POLARSTAR MANAGEMENT SEZC

PRIVACY POLICY – CAYMAN DATA PROTECTION

July 2023

POLARSTAR

Table of Contents

DOCUMENT CONTROL

VERSION #:	DATE:	CHANGES INCLUDE:
1	April 2019	Creation Date
2	Sept 2019	Updated
3	June 2020	Updated
4	30 June 2021	Inclusion of Privacy Statement
5	28 Sep 2021	Updated to include: cover the following: a) Key data privacy risks to PolarStar; b) Roles and responsibilities of the Board, Data Protection Officer, Chief Information Security Officer, Deputy Chief Information Security Officer, and Employees; c) Non-compliance with the Cayman Islands Data Protection Act; d) Security measures put in place; e) Data storage; f) Individual rights; g) Lawful basis for processing data; h) Employee training and acceptance of responsibilities; and I) Policy statements requiring that the policies and procedures are reviewed and updated on a periodic basis (i.e., at least on an annual basis), and/or when there are changes to its IT environment, legislations, processes, procedures and technologies.
6	December 2021	Inclusion of Appendix D – Undertaking
7	February 2023	Update the administrator information
8	July 2023	- Update address of the Cayman Islands Ombudsman; - Update the DPO.

1. INTRODUCTION

This Privacy Policy ("Privacy Policy" or "Policy") aims to describe the rules and processes in respect to data protection that are adopted and observed by PolarStar Management SEZC (the "Company" or "PolarStar"), a company based in the Cayman Islands.

The Data Protection Act (as defined below) applies to this Policy, and it is applied to the processing carried out by PolarStar, in its capacity as Data Controller or Data Processor of Personal Data, as applicable.

2. KEY TERMS

- **Biometric Data:** means any information relating to an individual's physical, physiological or behavioural characteristics of a natural person, which allows or confirms the unique identification of that natural person, such as facial images or fingerprints.
- **Consent:** concerning a Data Subject means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which the Data Subject, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to the said Data Subject.
- **Data Controller:** means the person who, alone, or jointly with others, determines the purposes, conditions and manner in which any personal data are, or are to be, processed.

- **Data Processor:** means any person who processes Personal Data on behalf of a Data Controller and does not itself determine why personal data should be processed. To a certain extent, a Data Processor may decide on how the personal data should be processed. Any person who processes Personal Data on behalf of a Data Controller, excluding employees of the Data Controller.
- **Data Protection Act** or **DPA:** means any applicable statute, regulation, order, or any other legal instrument which pertains to the protection of privacy and confidentiality personal information, including (i) the Data Protection Act (Law 33 of 2017 consolidated with Law 56 of 2021), as revised; (ii) the Data Protection Regulations, 2018 (SL 17 of 2019) and any other regulation promulgated under the DPA; (iii) any 'code of practice' promulgated under section 42 of DPA; and (iv) any binding decision of the courts and tribunals of the Cayman Islands that relate to the application or interpretation of any of the foregoing.
- **Data Protection Principles:** means the data protection principles (listed on the DPA) that relate to the Personal Data that the Data Controller processes. Data Controllers must observe and respect the principles.
- **Data Subject:** means an individual who is the subject of the Personal Data, meaning (i) an identified living individual; or (ii) a living individual who can be identified directly or indirectly by means reasonably likely to be used by the Data Controller or by any other person.
- **Inaccurate:** in relation to Personal Data, includes data that are misleading, incomplete, or out of date.
- **Ombudsman:** means the Cayman Islands' supervisory authority for data protection.
- **Personal Data:** means data relating to a Data Subject who can be identified.
- **Recipient:** in relation to Personal Data, includes a person to whom the data are disclosed, as well as any person (such as an employee or agent of the relevant Data Controller, a relevant Data Processor, or an employee or agent of a Data Processor) to whom they are disclosed in the course of processing the data for the Data Controller, but does not include a person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law;
- **Sensitive Personal Data:** includes data regarding the Data Subject's racial or ethnic origin, political opinions, religious beliefs, trade union membership, genetic, physical or mental health, medical data, sex life, commission or alleged commission of an offence (or information relating to any proceedings for any offence committed or alleged to have been committed).
- **Third Party:** in relation to Personal Data, means any person other than the Data Subject, the Data Controller, or any Data Processor or other person authorised to process data for the Data Controller or Data Processor.

3. DATA PROTECTION IN THE CAYMAN ISLANDS

The Cayman Islands Data Protection Act, as defined above, enacts a framework of rights and duties regarding data protection. The DPA is based on the same internationally recognised privacy principles that form the basis for other data protection laws, including the European Union (EU) General Data Protection Regulation (Regulation EU 2016/679).

Internationally active organisations will find many similarities between the data protection legislation of the Cayman Islands and of other jurisdictions where they are active. The DPA aims to reduce the administrative burden of operating internationally and cement the Cayman Islands as an attractive jurisdiction in line with international developments.

Importantly, the DPA provides a standard framework applied at PolarStar to manage the Personal Data Subjects used.

PolarStar aims to provide all individuals with a greater sense of comfort when it comes to how their Personal Data is managed and controlled. Where individuals feel that they are empowered to manage and control their Personal Data, they are more likely to share Personal Data.

4. OFFICE OF THE OMBUDSMAN OF THE CAYMAN ISLANDS

The Office of the Ombudsman is the Cayman Islands' supervisory authority for data protection. As part of this role, the Ombudsman:

- hears, investigates, and rules on complaints;
- monitors, investigates, and reports on compliance by Data Controllers;
- intervenes and delivers opinions and orders related to processing operations;
- gives orders on rectification, blocking, erasure, or destruction of data;
- imposes temporary and permanent bans on processing;
- makes recommendations for reform both generally and targeted at specific Data Controllers;
- engages in proceedings where there are violations, and refer violations to the appropriate authorities;
- co-operates with other supervisory authorities;
- publicises and promotes the requirements of the law and the rights of Data Subjects; and
- anything else that is conducive or incidental to the Office's functions.

The Office of the Ombudsman's approach to data protection is a practical one. PolarStar recognises and respects the fundamental right to privacy. At the same time, PolarStar understands that fair and lawful processing of Personal Data is essential to the modern service economy.

The DPA implemented throughout PolarStar is modelled on European data protection legislation. Supervisory authorities and court decisions in the European Union are an important reference resource for PolarStar and the Ombudsman in Cayman when interpreting and applying the DPA.

5. WHAT IS PROCESSING OF PERSONAL DATA?

The DPA defines processing very broadly, covering any conceivable use of data. In fact, any activity which affects Personal Data in any way constitutes processing; mere storage or retention will constitute processing as well.

In relation to Personal Data, "processing" is: obtaining, recording, or holding data, or carrying out any operation or set of operations on Personal Data, including:

- organising, adapting, or altering the Personal Data;
- retrieving, consulting, or using the Personal Data;
- disclosing the Personal Data by transmission, dissemination or otherwise making it available; or
- aligning, combining, blocking, erasing, or destroying the Personal Data.

6. LEGAL BASIS FOR PROCESSING

Schedule 2 of the DPA specifies the legal basis for processing Personal Data. PolarStar ensures that at least one of the below is applied when processing Personal Data:

- Consent:

Clear Consent is provided by Data Subjects for processing of their data.

- Contract:

Processing is necessary for the performance of investing in the PolarStar funds requested by the Data Subjects.

- Legal Obligation:

Processing is necessary for PolarStar to comply with the law (excluding contractual obligations).

- Vital Interests:

Processing is necessary to protect the individual's life.

- Public Functions:

Processing is necessary for PolarStar to perform a public function, or a function of a public nature exercised in the public interest.

- Legitimate Interests:

Processing is necessary for legitimate interests pursued by the Data Controller/Processor, except where it is unwarranted because of prejudicing the individual's rights and freedoms or legitimate interests.

7. DATA CONTROLLER VS DATA PROCESSOR

Data Controller is the person who, alone or jointly with others, determines the purposes, conditions, and manner in which any Personal Data are, or are to be, processed.

The DPA applies to a Data Controller if they are:

- established in the Cayman Islands, and the Personal Data is processed in the context of that establishment; or
- not established in the Cayman Islands, but the data is being processed in the Cayman Islands (otherwise than for transit purposes).

As a Data Controller established in the Cayman Islands and processing Personal Data in the context of that establishment, PolarStar is responsible for applying the requirements of the DPA, applying the Data Protection Principles to the Personal Data which we process, and to co-operate with investigations of the Ombudsman.

As a Data Controller, PolarStar is also responsible for ensuring that the Data Protection Principles are complied with in relation to Personal Data being processed on our behalf (by a Data Processor). Therefore, whenever PolarStar acts as a Data Processor, the same Data Protection Principles will be observed.

Information regarding the information collected by PolarStar through its website (www.polarstarfunds.com) is detailed in Appendix C to this Policy.

PolarStar may be a Data Controller of certain Personal Data jointly with another Data Controller[1]. In that case, PolarStar will decide with the other Data Controller on how and why Personal Data is being processed. Both, PolarStar and the other Data Controller will be jointly responsible for complying with their obligations under the DPA. While not explicitly mentioned in the DPA, it is best practice for joint Data Controllers to enter into a joint controllership agreement, which will lay out the parties' respective responsibilities. It should be noted that the information requirements under the first Data Protection Principle (fair and lawful processing) will mean that the essence of the joint controllership agreement should be communicated to the individual.

Apex Group Administration Services Ireland Ltd. (administrator), a company based in Ireland ("Apex"), is the third-party administrator of the funds managed by PolarStar. Apex is a separate legal entity from PolarStar and uses the client's Personal Data to perform its own anti-money laundering checks to comply with legal requirements. Therefore, in the above context, PolarStar and Apex are joint Data Controllers of the client's Personal Data.

Data Processor is commonly a natural or legal person that processes Personal Data following the Data Controller's instructions & the terms of a written agreement (i.e., data processing agreement) on behalf of the Data Controller.

The Data Controller shall instruct the Data Processors to:

- maintain records of processing activities;
- co-operate with the Ombudsman (where necessary);
- implement appropriate security measures;
- inform the Data Controller in the event of a data breach; and
- comply with the requirements of the DPA regarding cross-border data transfers, if applicable.

A Data Processor will be considered a joint Data Controller in the event that it processes Personal Data other than under the instructions of the Data Controller.

Outsourcing Personal Data processing activities by a Data Controller to a Data Processor shall be governed by a written 'data processing agreement'.

Both the Data Controller and the Data Processor are required to implement policies and procedures to ensure compliance with the DPA and has the following direct responsibilities:

- maintain internal records of Personal Data processing activities;
- implement robust information security measures;
- conduct assessments on the procedures adopted regarding data protection;
- only make use of a sub-processor with the prior written authorisation of PolarStar;
- co-operate with the Office of the Ombudsman;
- notify any Personal Data breaches to PolarStar, Data Subjects and the Ombudsman without delay.

A Data Controller or a Data Processor that fails to meet any of these obligations may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures.

PolarStar as Investment Manager has various Data Subjects. The data controller role also fulfils the Data Processor role.

8. LOCAL CAYMAN REPRESENTATIVE

The DPA establishes that a local representative in the Cayman Islands shall be nominated if the Data Controller is not established on the Island. PolarStar does not require a local Cayman representative as it has a Cayman presence with a fully staffed office. However, an entity based outside of Cayman would have an obligation to appoint a representative in Cayman.

[1] A Data Controller can be any legal person, i.e., an individual, corporation, either aggregate or sole, or any club, society, association, public authority, or other body, of one or more persons.

9. WHAT INFORMATION DOES THE DPA APPLY TO?

9.1. PERSONAL DATA

The DPA applies to 'personal data' meaning any information relating to a living individual who can be directly or indirectly identified. Several different factors may identify an individual, including a name or number, as well as online identifiers such as an IP address or other factors. The DPA applies to the processing of Personal Data, regardless of its format or storage medium.

9.2. SENSITIVE PERSONAL DATA

The processing of some types of Personal Data presents a higher risk to that person's rights and interests. The DPA explicitly recognises certain types of data as being 'Sensitive Personal Data'; however, the processing of types of Personal Data not defined as sensitive under the DPA may, depending on the overall context, also pose a higher risk to a person's rights and interests and warrant an extra level of care.

As a defined term under the DPA, Sensitive Personal Data is Personal Data consisting of:

- the racial or ethnic origin of the Data Subject;
- the political opinions of the Data Subject;
- the Data Subject's religious beliefs or other beliefs of a similar nature;
- whether the Data Subject is a member of a trade union;
- genetic data of the Data Subject;
- the Data Subject's physical or mental health or condition;
- medical data;
- the Data Subject's sex life;
- the Data Subject's commission, or alleged commission, of an offence; or any proceedings for any offence committed, or alleged, to have been committed, by the Data Subject, the disposal of any such proceedings or any sentence of a court in the Islands or elsewhere.

Even though Biometric Data is not defined as Sensitive Personal Data, PolarStar treats it as such.

PolarStar does retain Sensitive Personal Data.

10. THE EIGHT (8) DATA PROTECTION PRINCIPLES

The DPA is a powerful piece of legislation. It introduces globally recognised principles about the use of Personal Data to the Cayman Islands. All the Eighth Data Protection Principals are observed by PolarStar, as described below.

I. FAIR AND LAWFUL USE

PolarStar endeavours to manage Personal Data in a fair way. This means processing the data in a way that is unduly detrimental, unexpected, or misleading to the individuals concerned. PolarStar remains transparent, honest, and open with all clients from relationship inception and after termination about how we handle their Personal Data. PolarStar aims at offering the upmost fairness, lawfulness, and transparency around data handling.

PolarStar understands that for a Data Controller to process Personal Data fairly (i.e., to comply with the first Data Protection Principle), the identity of the Data Controller and the purpose for processing the Personal Data must be disclosed. In addition, one of the following preconditions must be fulfilled:

(i) the Data Subject has given consent to the processing;
(ii) the processing is necessary for administration of justice or exercise of statutory, governmental or public functions; or
(iii.a) the processing is necessary for legal compliance (other than contractual compliance);

(iii.b) the processing is necessary for the performance of a contract to which the Data Subject is a party or taking steps at the request of the Data Subject with a view to entering into a contract;

(iii.c) the processing is necessary for the purposes of legitimate interests pursued by the Data Controller or the Third Party to whom the data is disclosed, except if the processing is unwarranted by reason of prejudice to the rights and freedoms or legitimate interests of the Data Subject;
(iii.d) the processing is necessary to protect the Data Subject's life.

II. PURPOSE LIMITATION

PolarStar ensures that Personal Data is only processed for the purpose it was collected for by:

- Clearly identifying our purpose for processing;
- Regularly reviewing our processing & updating our documentation around privacy for information for individuals.

III. DATA MINIMISATION

PolarStar ensures that the processing of Personal Data is adequate and relevant to fulfil the stated purpose.

IV. DATA ACCURACY

PolarStar actions all reasonable steps to ensure that Personal Data is not incorrect or misleading.

V. STORAGE LIMITATION

PolarStar ensures that Personal Data are:

- kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data are processed.
- stored for longer periods insofar as the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to the implementation of the appropriate technical and organisational measures required in order to safeguard the rights and freedoms of the Data Subject.

VI. RESPECT FOR THE INDIVIDUAL'S RIGHTS

PolarStar endeavours to ensure that Personal Data is processed in accordance with the rights of the individual in mind. The obligation lies with PolarStar to respect the rights of the individuals.

VII. SECURITY – INTEGRITY & CONFIDENTIALITY

PolarStar ensures that Personal Data is kept safe. PolarStar holds integrity and confidentiality as core values throughout the business. These values are applied to Personal Data that must be kept secure not just from malicious attacks but from inadvertent damage too.

VIII. INTERNATIONAL TRANSFERS

The eighth Data Protection Principle of the DPA prohibits the international transfer of Personal Data where the jurisdiction does not present an adequate level of right protection of Data Subjects in relation to the processing of Personal Data. This does not mean that Personal Data cannot be transferred internationally. However, any such transfers need to be assessed against the DPA.

Personal Data may be transferred outside the Cayman Islands where it is adequately protected. As described above, Apex makes use of client Personal Data to perform its own anti-money laundering checks to comply with legal requirements in Ireland. Apex fulfils the role of both the Data Controller and Data Processor.

The Ombudsman considers the following countries and territories as ensuring an adequate level of protection:

- member States of the European Economic Area (EEA) (that is, the European Union plus Lichtenstein, Norway, and Iceland) where Regulation (EU) 2016/679 (the General Data Protection Regulation or "GDPR") is applicable;
- any country or territory in respect of which an adequacy decision has been adopted by the European Commission pursuant to Article 45(3) GDPR or remains in force pursuant to Article 45(9) GDPR.

PolarStar acknowledges that Malta lies within the EEA and therefore provides an adequate level of protection for the rights and freedoms of Data Subjects in relation to the processing of Personal Data.

11. INDIVIDUAL RIGHTS

The DPA establishes the rights of Data Subjects. These rights are not absolute as they may be restricted in certain specified circumstances. Exemptions may also apply, whereby specified rights or other provisions of the DPA do not apply. PolarStar observes and respects the Data Subject rights, as described below:

I. THE RIGHT TO BE INFORMED:

A person is entitled to be informed by a Data Controller whether the Personal Data of which the person is the Data Subject is being processed by or on behalf of that Data Controller. This is a key transparency requirement under the DPA.

Following this right, PolarStar must provide individuals with information including:

- who the Data Controller is;
- the purpose of processing.
-

PolarStar may also decide to provide additional information, such as:

- PolarStar contact details;
- the legal basis of processing (including statutory requirements if applicable);
- the legitimate interests of processing (if applicable);
- the categories of data obtained;
- the source of the data;
- the Recipients or categories of Recipients of the data;
- the details of any international transfers;
- the retention period of the data;
- the rights available to individuals;
- the right and contact details to make a complaint to the Ombudsman;
- the details of any automated decision making.

The information described above is known as 'privacy information' and is usually communicated in a 'privacy notice'. PolarStar must provide privacy information to individuals "as soon as reasonably practicable", which generally means at the time when their Personal Data is collected from them.
If PolarStar obtains Personal Data from other sources, PolarStar must provide individuals with privacy information within a reasonable period of obtaining the data, either directly or indirectly through a public notice, depending on the processing activity and the ability to directly notify the individuals.
PolarStar regularly reviews, and where necessary, updates privacy information. PolarStar brings any new uses of an individual's Personal Data to the attention of the individuals before processing their data. Getting the right to be informed correctly aids PolarStar in complying with other aspects of the DPA and builds trust with people.

When collecting Personal Data from individuals, PolarStar will not need to provide them with any information that we already have.

There are circumstances when PolarStar is not obliged to provide the privacy information. The DPA recognises the following exemptions from the right to be informed:

- the data is processed for crime prevention, detection or investigation, the apprehension or prosecution of any person suspected of having committed an offence, or the assessment or collection of any fees or duty;
- the data is processed for monitoring, inspection or a regulatory function, to the extent that applying it would be likely to prejudice the discharge of the function;
- the data is processed for statistical purposes or for the purposes of historical or scientific research.
- the data consists of information you are obliged by the Act to make available to the public;
- the data is processed for purposes of conferring any honour or dignity by the Crown or the Premier;
- the data is processed for purposes of corporate finance and the application of the provision could affect the price of a financial instrument, or for the purpose of safeguarding an important economic or financial interest of the Cayman Islands;
- the data consists of intentions in regard to any negotiations with the individual which would be prejudiced by the processing;
- the processed data consists of information in respect of which legal professional privilege applies and in respect of trusts and wills;
- the notification could reasonably cause mental or physical harm to any person;

- to the extent that the notification would be likely to prejudice the carrying out of social work because of serious harm to the physical or mental health or condition of any person.

II. THE RIGHT OF ACCESS

Individuals have the right to access their own Personal Data. This is commonly referred to as subject access. To do so, individuals must make a subject access request ("SAR") in writing. PolarStar will respond the request within thirty days. If PolarStar requires further information from the requestor, the period of time for PolarStar's response can be extended by the Regulations. PolarStar will not apply any fee to deal with a request except in exceptional circumstances.

What is an individual entitled to?

Following the DPA provisions, PolarStar will provide the following to the Data Subject:

- confirmation that PolarStar is processing their Personal Data;
- a copy of their Personal Data;
- other supplementary information – this includes the information that PolarStar should provide in a privacy notice, but also additional information.

In addition to a copy of their Personal Data, PolarStar must provide individuals with the following information:

- the purposes of our processing;
- the categories of Personal Data concerned;
- the Recipients or classes of Recipient disclosed, or may disclose, the Personal Data to;
- any countries or territories outside the Cayman Islands to which PolarStar does, or intends to, transfers the Personal Data;
- the general measures taken to ensure the security of the personal data (i.e., to comply with the seventh Data Protection Principle);
- any information available as to the source of the Personal Data;
- the reasons for any automated decision made in relation to the individual, including the individual's performance at work, creditworthiness, reliability or conduct;
- the right to make a complaint to the Ombudsman.

PolarStar may have already provided some of this information in the privacy notice.

A Data Subject access request does not need to be for all the types of information listed above. However, PolarStar will clarify to the requestor that they are entitled to the types of information listed above.

III. THE RIGHT TO RECTIFICATION

PolarStar ensures that Personal Data is accurate and, where necessary, up to date. The individuals have the right to have Inaccurate Personal Data rectified or completed if it is incomplete, insofar as the Data Controller is convinced of the validity of the request.

The DPA does not specify how to make a request for rectification. An individual can make a request for rectification verbally or in writing. It can also be made to any part of PolarStar and does not have to be to a specific person or contact point. A request to rectify Personal Data does not need to mention the phrase' request for rectification' or the fourth Data Protection Principle of the DPA to be a valid request. As long as the individual has challenged the accuracy of their data and has asked you to correct it or has asked that you take steps to complete data held about them that is incomplete, this will be a valid request. PolarStar will provide training to its employees so they can identify a request.

If PolarStar receives a request for rectification, the reasonable steps to satisfy whether the data is accurate and to rectify or update the data, if necessary, should be taken. What steps are reasonable will depend, in particular, on the nature of the Personal Data and what it will be used for. The more important it is that the Personal Data is accurate, the greater the effort required in checking its accuracy and, if necessary, taking steps to rectify it.

An individual can complain to the Ombudsman, who may issue an order for rectification, blocking, erasure or destruction of the data in question where the complaint is upheld. The same approach described above will be practiced while the complaint is under investigation by the Ombudsman, until the conclusion of the matter.

PolarStar is not obligated to correct Inaccurate Personal Data, unless ordered to do so by the Ombudsman. However, we understand it makes sense to do so when possible.

IV. THE RIGHT TO STOP/RESTRICT PROCESSING

Individuals have the right to require that processing stop, or not begin, or cease processing for a specified purpose or in a specified way. This is not an absolute right and does not apply in certain circumstances. PolarStar does not have to comply with a request to stop or restrict the processing if:

- the processing is necessary for the performance of a contract to which the individual is a party (or taking steps at the request of the individual towards entering into a contract.
- the processing is necessary under a legal obligation to which the Data Controller is subject.
- the processing is necessary to protect the vital interests of the individual.
- PolarStar has requested and received the approval of the Ombudsman.

An individual must make a request to stop processing in writing. PolarStar has one twenty-one days to respond to a request or apply to the Ombudsman not to comply with the request. This right has close links to other rights, including the right to rectification (the fourth Data Protection Principle) and the right to object to direct marketing.

PolarStar has internal processes to restrict Personal Data processing. Depending on the nature of the restriction the individual requested, PolarStar will not process the data at all, and it will be erased. This is the case unless:

- the individual has not demanded PolarStar to stop processing their data outright, but PolarStar ceases processing their Personal Data for a specified purpose or in a specified way only.
- the data is being processed in the context of a contract, a legal obligation or to protect the vital interests of the individual.
- an exemption applies to the processing you undertake.

PolarStar has the right to apply to the Ombudsman for permission not to comply with a request to stop or restrict processing. If so, PolarStar will do so within twenty-one days from the date of the request and will inform the individual that we have applied to the Ombudsman.

If the Ombudsman issues an order to block, erase or destroy data, it may order PolarStar to notify Third Parties to whom the data may have been disclosed of the blocking, erasure or destruction. In any event, PolarStar will let any Third Parties to whom the Personal Data was disclosed know of the fact that we stopped or restricted processing.

V. THE RIGHT TO STOP DIRECT MARKETING

The DPA gives individuals an absolute right to stop the processing of their Personal Data for direct marketing purposes. An individual must notify PolarStar in writing. When notified, PolarStar should cease, or not begin processing for the purpose of direct marketing without undue delay within a reasonable period of time.

An individual may complain to the Ombudsman if PolarStar does not comply with their request.

VI. THE RIGHTS IN RELATION TO AUTOMATED DECISION MAKING

The DPA has provisions on solely automated individual decision-making (making a decision exclusively by automated means without any human involvement). An individual may at any time give PolarStar a notice in writing requiring that a decision which affects them significantly is not solely based on processing by automated means. If PolarStar makes decisions that significantly affect individuals solely by automated means, PolarStar must notify the individual that the decision was taken on that basis. The individual may then notify PolarStar within twenty-one days that PolarStar needs to reconsider the decision on a different basis (not solely based on automated means). PolarStar must then, within twenty-one days inform the individual explaining what steps they intend to take to comply with the notice.

This right is not absolute and does not apply if one each of the following listings of conditions is met:

- the decision is taken in the course of:

(a) considering whether to enter into a contract with the individual.

(b) entering into such a contract.

(c) performing such a contract.

- the decision grants a request from the individual.
- steps have been taken to safeguard the legitimate interests of the individual including allowing the individual to make representations.

If PolarStar receives a notice relating to the right in relation to automated decision making, PolarStar will:

- provide meaningful information about the logic involved in the decision-making process, as well as the significance and the envisaged consequences for the individual.
- use appropriate mathematical or statistical procedures.
- ensure that individuals can: obtain human intervention, express their point of view, and obtain an explanation of the decision and challenge it.
- put appropriate technical and organisational measures in place, so that you can correct inaccuracies and minimise the risk of errors.
- secure Personal Data in a way that is proportionate to the risk to the interests and rights of the individual, and that prevents discriminatory effects.

VII. THE RIGHT TO COMPLAIN/SEEK COMPENSATION

An individual has the right to complain to the Ombudsman about any perceived violation of the DPA. The Ombudsman may also investigate matters under the DPA on its own motion. An individual that suffers damage due to a contravention of the DPA by a Data Controller may seek compensation in the courts. A complaint must relate to Personal Data processing that has not been or is not being carried out in compliance with the DPA, or anything done pursuant to the DPA.

12. PERSONAL DATA BREACHES

DPA defines a Personal Data breach ("Personal Data Breach") as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or, access to, Personal Data transmitted, stored or otherwise processed.

Breaches can be the result of both accidental and deliberate causes. It also means that a breach is more than just about losing Personal Data.

Personal data breaches can include:

- access by an unauthorised Third Party.
- deliberate or accidental action (or inaction) by a controller or processor.
- sending Personal Data to an incorrect Recipient.
- computing devices containing Personal Data being lost or stolen.
- alteration of Personal Data without permission.
- loss of availability of Personal Data.

PolarStar is aware of the Company's Data Privacy Risks, as described further in Appendix A.

PolarStar adopts internal procedures and contracts technological systems and tools to protect the Company from cyber-attacks, internal sabotage, and malware infestations that may result in a Personal Data Breach. Among the procedures adopted, PolarStar conducts training to its employees, clients, and Third Parties, as well as tests to confirm if the measures adopted seems to be sufficient for the Company's goals in terms of cyber security and technology, as approved and determined in accordance with the Company's governance. Further information may be found on PolarStar's Cyber Security Policy and in Appendix A to this Policy.

As part of the procedures adopted, PolarStar has established the following procedures to recognise and respond to a Personal Data Breach:

13. PREPARING FOR A PERSONAL DATA BREACH

- PolarStar's employees are constantly trained to recognise a Personal Data Breach.
- PolarStar understands that a Personal Data Breach is not only about loss or theft of personal data.
- PolarStar has a response plan in place for addressing any Personal Data Breaches that occur.
- PolarStar has allocated responsibility for the governance bodies of the Company to manage data breached (further information may be found below).
- PolarStar employees are constantly trained to understand how to escalate a security incident internally so the correct procedures can be applied.

13.1. RESPONDING TO A PERSONAL DATA BREACH

PolarStar has a process in place to assess the likely risks to individuals as a result of a Personal Breach.

In case of a Personal Data Breach is confirmed, PolarStar will notify the Ombudsman and the affected Data Subjects of a breach within 5 days (unless the breach is unlikely to prejudice their rights and freedoms), even if all the details are not yet known.

PolarStar knows what information must be provided to the Ombudsman and the Data Subjects about a breach, including advice to assist them in protecting themselves from its effects.

In case a Personal Data Breach occurs, PolarStar will investigate whether the Data Breach resulted from human error or a systemic issue and take corrective action to ensure that recurrences are prevented. In addition, PolarStar will document and maintain in its files all Data Breaches.

13.2. FAILURE TO NOTIFY THE OMBUDSMAN AND THE DATA SUBJECTS OF BREACHES

Failure to notify the Ombudsman and Data Subjects timeously may cause additional damages to the Data Subject's whose Personal Data has been breached. PolarStar will adopt all the measures and procedures to prevent this from occurring. PolarStar is aware that failure to notify a breach when required to do so is an offence under the DPA and can result in a conviction and a monetary penalty imposed by the Ombudsman. Also, this tarnishes the reputability of PolarStar and undermines the trust Data Subjects have in PolarStar.

14. CAYMAN ISLANDS OMBUDSMAN CONTACT

The details to contact Ombudsman can be found below:

Address: 5th Floor, Anderson Square, 64 Shedden Road, George Town, Grand Cayman

Mail: PO Box 2252, Grand Cayman KY1-1107, CAYMAN ISLANDS

Email: info@ombudsman.ky

Phone: +1 345 946 6283

Hours: Monday to Friday 8:30am to 4:30pm

To make a request under the Freedom of Information Law for access to records from the Ombudsman office their information manager should be contacted: rene.lynch@ombudsman.ky and the FOI Request Form should be submitted (more information can be found on the website of Ombudsman at https://ombudsman.ky/get-in-touch).

15. GOVERNANCE

PolarStar has roles and responsibilities for the directors, managers and employees, as described further in Appendix B.

16. PRIVACY & DATA SECURITY TRAINING

PolarStar conducts training in-house via resources and outsourced service providers.

Training is mandatory for all workforce members (from the Board to senior management to all employees) with access to the information the organisation desires to safeguard. Interns and other non-traditional categories of workers are also included in the training.

Basic privacy and security training is provided before an individual obtains access to confidential or personal information. At PolarStar, this is prior to being hired and provided access to the PolarStar systems. At a minimum, training is conducted annually. Training may be needed after changes in policies; following increases in levels of access or sensitivity of information; to react to changes in technology; and following a security incident and other situations.

Training may be delivered via consistent messaging about data security throughout an organisation. This includes policies, notices, newsletters, in-person sessions, online courses, videos, testing, tabletop exercises, employee resource groups or a combination of these. The ability for participants to interact and ask questions can be critically important to their understanding their responsibilities as they relate to the business.

Training is documented and logged. This enables PolarStar to defend its data privacy and security practices by maintaining comprehensive training programs. This allows PolarStar to tracks the materials covered in the training and those who attended or received the information.

The substance of the training will depend on the data at issue, the audience and other factors. In general, training should cover some basic issues, such as what is confidential or personal information or what is a Data Breach. However, training programs can be significantly enhanced when they use real situations that participants in the program can relate to and apply in their jobs.

Additionally, all the employees are required to read this Police and sign the acknowledgement form which's template can be found on Appendix D to this Police.

17. NON-COMPLIANCE WITH DPA

PolarStar is aware that a director, manager, secretary or other company officer may be guilty of an offence in addition to the Company if the offence is proved to have been committed with their Consent or connivance or attributable to their neglect.

Offences under the Law include:

- unlawfully obtaining or disclosing Personal Data;
- unlawful sale of Personal Data;
- failing to comply with an enforcement notice or an information notice.

Fines under the DPA could be as high as CI $100,000 (US $122,000) and certain offences are punishable by imprisonment. Under the DPA the Ombudsman also has the right to serve a Data Controller with a monetary penalty order if the Ombudsman is satisfied on a balance of probabilities that there has been a serious contravention of this Act by the Data Controller and the contravention was of a kind likely to cause substantial damage or substantial distress to the Data Subject. Monetary penalty orders could be as high as CI $250,000 ($305,000).

18. POLICY STATEMENT REGARDING REVIEW & UPDATE PROCEDURES

Aside from at least an annual review of the Policy, there will be times when the Privacy Policy needs to be updated to ensure that it remains in line with the way PolarStar operates and complies with all current laws and legislation. Other events that may result in a policy change may include changes to the IT environment, legislations, processes, procedures and technologies. PolarStar will inform all employees when material changes to the Policy are made. Material changes include changes to the type of data PolarStar collects or the way we process data.

19. APPENDICES

The Appendices to this Policy, as listed below, are an integral part of this Policy.

- Appendix A – PolarStar Data Privacy Risks & Implemented Measures
- Appendix B – PolarStar Roles & Responsibilities Regarding Data Protection
- Appendix C – PolarStar Data Protection/Privacy Statement
- Appendix D – Undertaking

APPENDIX A – POLARSTAR DATA PRIVACY RISKS & IMPLEMENTED MEASURES

KEY DATA PRIVACY RISKS FOR POLARSTAR

Privacy and data security concerns are among the most critical issues facing investment funds and managers alike. The privacy and data security challenges confronting PolarStar, include the increased focus on the privacy and security of sensitive information by authorities. With daily attacks by hackers on corporate networks, PolarStar aims to develop and implement effective strategies to protect the organisation from privacy and security threats.

Investment managers have always been highly attractive targets for cyber criminals because of the extremely sensitive information that is possessed. While the security of personal and financial information has garnered most of the attention over the last ten years. PolarStar places great attention on the protection of non-public information of potential transactions, as failure to secure such information could place such transactions in jeopardy. A security breach resulting in the disclosure of such sensitive information may cost extortionate amounts in remediation and litigation costs, not to mention the reputational harm of such a breach.

Data security is a top action item for many organisations today. Here are the top reasons.

Data breaches

A data breach, or data leak, is a security event when critical data is accessed by or disclosed to unauthorised viewers. Data breaches can happen due to:

- Cyberattacks in which hackers bypass your security technologies and get into your important software or your security platform.
- Theft or loss of devices containing protected information.
- Data theft by employees or other internal users, such as contractors or partners.
- Human errors such as accidentally sending sensitive data to someone unauthorised to see it.

Data breaches can have a significant financial impact. It can interrupt business operations, which may impact company revenue. A breach may also involve legal costs, and if it involves a violation of a compliance or industry mandate, the regulatory body can impose fines or other consequences. In addition, PolarStar may suffer lasting damage to its reputation and customer trust.

Compliance

Compliance requirements also drive data security. In particular, data privacy regulations like the EU's General Data Protection Regulation (GDPR) and the Cayman Islands DPA strictly regulate how companies collect, store and use personally identifiable information (PII). Compliance failures can be expensive; for example, DPA fines can reach 4% of a company's global annual turnover for the preceding financial year. In addition, authorities can issue warnings and reprimands, and, in extreme cases, ban the organisation from processing Personal Data.

Meeting compliance requirements is necessary for a successful data security strategy but checking the boxes during compliance audits is not sufficient. Regulations typically focus only on specific aspects of data security (such as data privacy), and real-world security threats evolve faster than legislation. Protecting sensitive data should be viewed as a long-term, ongoing commitment.

Cloud security

PolarStar has been using cloud solutions since 2015. During the COVID-19 pandemic, cloud data security became a significant priority for PolarStar and many other industries, as employees increasingly had the capability to transition between the office and their homes.

Data protection strategies generally focused on keeping malicious intruders out of systems where sensitive data is stored but with cloud computing, data is stored in systems that are outside the traditional perimeter and can flow freely everywhere. Therefore, PolarStar has required a data-centric security strategy that prioritises the most sensitive information.

SECURITY MEASURES IMPLEMENTED AT POLARSTAR

Building a solid data security strategy:

Organisations do not need to build a data protection strategy from scratch. Instead, they can take advantage of established tools like the NIST Cybersecurity Framework, which can help PolarStar to:

- understand the applicable security risks,
- prioritise the security efforts, and
- measure the ROI of cybersecurity investments.

The NIST framework comprises five major functions:

1. Identify — Understand and document the cybersecurity risks to systems, people, assets, data and capabilities.
2. Protect — Implement appropriate security controls and other measures to protect the most critical assets against cyber threats.
3. Detect — Ensure you can quickly spot actions and events that could pose a risk to data security.
4. Respond — Have tested procedures ready to enable prompt response to cybersecurity incidents.
5. Recover — Implement strategies for ensuring the ability to quickly restore data and services impacted by a security incident.

Technologies which strength data protection capabilities:

Modern data security methods involve implementing a comprehensive set of protective measures. NIST CSF and other frameworks provide detailed catalogs of controls for defending against threats.

Data discovery and classification —

Data discovery technology scans data repositories and reports on the findings, avoiding storing sensitive data in unsecured locations where it is more likely to be compromised. Data classification is the process of labelling sensitive data with tags in order to protect data in accordance with its value or applicable regulatory requirements.

Data encryption —

Encoding critical information making it unreadable and useless for malicious actors. Software-based data encryption is performed by a software solution to secure the digital data before it is written to the SSD. In hardware-based encryption, a separate processor is dedicated to encryption and decryption for safeguarding sensitive data on a portable device, such as a laptop or USB drive.

Dynamic data masking (DDM) —

This data security technique involves real-time masking of sensitive data to prevent exposure to non-privileged users while not changing the original data.

User and entity behaviour analytics (UEBA) —

UEBA technology is designed to spot deviations from normal activity that could indicate a threat. It is particularly helpful for detecting insider threats and hacked accounts.

Change management and auditing —

Improper changes to IT systems, whether accidental or malicious, can lead to downtime and breaches. Establishing formal change management procedures and auditing actual changes assist in detecting misconfigurations promptly.

Identity and access management (IAM) —

IAM helps organisations manage both regular and privileged user accounts and control user access to critical information.

Backup and recovery —

Organisations need to be able to restore data and operations promptly, whether a user has accidentally deleted a single file that they now urgently need, or a natural disaster or targeted attack has brought down the entire network. The PolarStar disaster recovery plan is laid out with a clear set of steps for retrieving lost data and managing incident response.

Effective data security at PolarStar, requires more than just technical measures; they need to be implemented as part of a well-managed, holistic data protection program.

APPENDIX B – POLARSTAR ROLES & RESPONSIBILITIES REGARDING DATA PROTECTION

ROLES & RESPONSIBILITIES

Role	Responsibility
Board of Directors	Given the statutory and fiduciary duties of the Board, the directors of PolarStar have the unique responsibility and legal duty to ensure that the organisation has appropriate privacy compliance programs in place to mitigate these risks. In particular, PolarStar's Board of directors is responsible for managing the business affairs of the organisation and directors are required to act honestly and in good faith with a view to the best interests of the organisation and to exercise the care, diligence and skill of a reasonable person in comparable circumstances. When it comes to privacy, this means that directors are responsible for ensuring that PolarStar is compliant with the DPA and that PolarStar takes appropriate steps to mitigate privacy and related risks (including cybersecurity). PolarStar's failure to have appropriate privacy compliance programs in place can result in significant financial and reputational consequences. Directors may also be held personally liable in cases where they do not provide appropriate oversight to mitigate the risks of these consequences. Directors can manage their responsibilities and mitigate their liabilities by taking certain key steps and ensuring that appropriate privacy compliance programs are in place. It is thus critical for directors to be properly trained and informed on the requirements of the Cayman Islands DPA.
Data Protection Officer (DPO): • Vivian Bandler Deputy DPO: • Allannah Scott-Bowles Fulfils the DPO roles in the event that the existing DPO is unable to.	The primary role of the DPO is to ensure that the organisation processes the Personal Data of its staff, customers, providers or any other individuals (also referred to as Data Subjects) in compliance with the applicable data protection rules. In the Cayman Islands, the DPA requires the appointment of the DPO. The DPO is an integral part of the organisation, making them ideally placed to ensure compliance. The DPO must be able to perform duties independently. There must not be a conflict of interest between the duties of the individual as a DPO and their other duties, if any. The PolarStar DPO • is not a controller of processing activities (i.e., he/she is not head of Human resources); • is not an employee on a short or fixed term contract • has responsibility for managing his/her own budget. • has the authority to investigate. The DPO has immediate access to all Personal Data and data processing operations; those in charge are also required to provide information in reply to questions from the DPO. Tasks of the DPO include: • ensuring that the DPA is respected in cooperation with the data protection authority; • Ensuring that controllers and Data Subjects are informed about their data protection rights, obligations and responsibilities and raise awareness about them; • Giving advice and recommendations to PolarStar about

	the interpretation or application of the data protection rules; • Creating a register of processing operations within PolarStar and notifying the Board of present specific risks; • Ensuring data protection compliance within PolarStar; • Handling queries or complaints on request by PolarStar, the controller, other person(s), or on own initiative; • Co-operating with the Board or regulatory bodies (responding to requests about investigations, complaint handling, inspections conducted etc.); • Highlighting PolarStar of any failures to comply with the applicable DPA.
Chief Information Security Officer (CISO): • Duncan Greenwood **Deputy CISO:** • Allannah Scott-Bowles Fulfils the CISO roles in the event that the existing CISO is unable to.	The CISO function reports directly to a high-level company official (Board). To ensure independence, the CISO should be given sufficient authority that is clearly promoted by executive leadership across the Company. To merit such independence, of course, the CISO must bring to the role the knowledge, background, and training to perform the tasks involved. Typical day-to-day CISO responsibilities include the following: **Information security governance** • Making sure that security initiatives and the overall information security strategic plan are run smoothly and adequately funded, with regular reporting to business management leadership and the Board. **Information security operations** • Analysing threats in real-time, using a variety of security tools along with the review of additional security reports at different intervals; • Implementing or deploying the incident response plan when there is a possible incident **Cybersecurity Intelligence** • Keeping up to date with emerging security threats; • Communicating with business management leadership regarding any potential security issues that might arise; • Informing management of any security risks (e.g., known vulnerabilities) for new systems/applications regardless of the business potential. **Training/data loss and fraud prevention** • Educating staff on information security awareness activities including how and who to report to, if they believe that there is a possible breach of security. **Information security architecture** • Advising and working closely with the IT provider on the planning, selection, and implementation of security hardware and software; • Working with IT and/or Third Parties with access to or hosting the Company's data to make sure that the network and access points are designed with security best practices where possible; • Reviewing firewall and intrusion detection/prevention. **Identity and access management** • Authorising and reviewing user access (including administrator and vendor access) to the Company's data and systems;

	• Overseeing the user access review process. Information security program management • Performing security risk assessments; • Overseeing social engineering exercises, penetration testing, and vulnerability scanning; • Overseeing and reporting on mitigation of information security issues; • Annual reporting to the Board; • Bi-annual reporting of key risk indicators to senior management. Incident investigations and forensic review • Incident response table-top testing; • Deploying the incident response plan if there is a possible security breach; • Coordinating with an external forensic service if warranted and requested by senior management. Regulatory • Ensuring compliance with all information security regulatory requirements; • Representing the Company in information security examinations with regulators.
Cybersecurity Officer (CO) (the CISO fills this role)	New security threats occur all the time, and the CO/CISO needs to stay up to date with the latest tactics that hackers are employing in the field. In addition to the high-level responsibilities mentioned above, some specific duties the CO/CISO conduct, include: • Setting and implementing user access controls and identity and access management systems; • Monitoring application performance to identify any irregular activity • Performing regular audits to ensure security practices are compliant; • Deploying endpoint detection and prevention tools to thwart malicious hacks; • Ensure that patch management systems are in place and are updating applications automatically; • Implementing comprehensive vulnerability management systems across all assets in the cloud; • Working with all employees to set up and share disaster recovery/business continuity plan; • Educating employees on how to identify suspicious activity.
Technical security manager (the CISO fills this role)	In charge of security systems, such as firewalls, data protection controls, patching, encryption, vulnerability scanning, pen testing, and so on. Managing the team or outsourced service provider that oversees the proper deployment, configuration, and functioning of these systems.
Program security manager (the CISO fills this role)	This is a more strategic role engaging in the world of risk management and mitigation. Typically, this individual is involved in evaluating vendor risk, examining vendor contracts or terms of service, helping different teams around the organisation understand third-party risk and data privacy issues, and more.
Data owner (Employees)	A Data Owner is an individual or group or people who have been officially designated as accountable for specific data that is

	transmitted, used, and stored on a system or systems within a department. Each employee at PolarStar is a data owner. The role of the data owner is to provide direct authority and control over the management and use of specific information. Data Owners: • Must ensure compliance with IT polices and all regulatory requirements; • Are responsible for having an understanding of legal and contractual obligations surrounding information assets within their functional areas; • Must determine appropriate criteria for obtaining access to sensitive information assets; • Must understand how information assets are stored, processed, and transmitted; • Must document and disseminate administrative and operational procedures to ensure consistent storage, processing and transmission of information assets; • Must understand and report security risks and how they impact the confidentiality, integrity and availability of information assets.

APPENDIX C – POLARSTAR DATA PROTECTION/PRIVACY STATEMENT

PolarStar strongly believes in protecting the privacy of Internet users who visit our website, located at www.polarstarfunds.com ("the **Site**"). This Privacy statement is intended to inform you of the ways in which this Site collects personal information, the uses to which that information will be put, and the ways in which we will protect any personal information you choose to provide us with. Generally, personal information is information that can be used to identify you or your activities on the Site or through services offered on the Site.

This Privacy statement applies solely to data collected via the Site. There may be additional personal (and other) information that we have or collect about you or your Company pursuant to other relationships which is subject to other agreements and rules.

Exclusion of Liability
The access and/or use of any information or materials contained in this Site are at your sole risk. Under no circumstances shall PolarStar officers or employees be liable for any losses, damages, costs, and expenses whatsoever (whether direct, indirect, consequential, incidental, special or economic including loss of profits) whether in an action in contract, negligence or tort arising out of or in connection with:

- the access or use, inability to access or use, or incomplete, delayed, or interrupted access or use of this Site or any other website linked to this Site;
- the reliance on information contained on this Site or on any other website linked to this Site;
- the failure of performance, error, omission or defect of any network, line or server system or the transmission to any computer hardware or software used in accessing this website of any computer virus or other corrupting or destructive codes, programs, macros, or elements of any kind; or
- the access by any unauthorised person to any information transmitted by you to PolarStar or vice versa through this Site.

This website may contain links to external websites and external websites may link to this Site. We are not responsible for the content or operation of any such external sites.

What Data Do We Collect?
The information collected by PolarStar through the Site falls into two categories: (1) information voluntarily supplied by visitors to our Site and (2) information gathered via automated means as visitors navigate through our Site.

Information Voluntarily Provided by You:
In the course of using the Site, you may choose to provide us with information to help us serve your needs. For example, you may provide us your email address to request information, or you may send us your mailing address so we may send you the material you have requested. Any personal information you send us will be used only for the purpose indicated on the Site or in this statement.

Information Collected by Automated Means:
We use various tools to enhance the Site user experience and track users of the Site, including cookies. Cookies are small pieces of text that a website places on your computer to help remember information about your visit. Cookies cannot read data off your computer's hard drive or collect your personal information. We use information collected from cookies to improve your experience and the overall quality of our services. We may also use cookies to collect information from Third Parties (such as Google) to analyse the effectiveness of our marketing or the performance of our Site. Our cookies may also come from third-party service providers who have permission to place such tools on our Site. You can refuse to accept and delete cookies by adjusting your browser settings. Please note that refusing or deleting cookies may impact your browsing experience on the Site or prevent you from using some of its services, and it may result in the deletion of any preferences you may have set. For more information on how to reject or delete cookies, you should consult with your browser's or device's help documentation. PolarStar does not use technology that recognises or tracks signals from your browser. You can also opt out of Internet-based advertising by installing a browser plugin from the Third Party where available.

In addition, in the course of ensuring network security and consistent service for all users, PolarStar employs software programs to do such things as monitor network traffic, identify unauthorised access or access to non-

public information, detect computer viruses and other software that might damage PolarStar computers or the network, and monitor and fine-tune the performance of PolarStar's Site. In the course of such monitoring, these programs may detect additional information from your computer such as your IP address, addresses from network packets, and other technical information. Any such information is used only for the purpose of maintaining the security and performance of PolarStar's networks and computer systems.

How Do We Use the Data We Collect?
We will use the information provided by you in order to serve your needs. This may include things such as sending you electronic or written materials or, for example, if you supply us with your telephone number, you may receive telephone contact from us in response to your request.

Do We Share Your Data?
We will not sell, exchange, or otherwise distribute your personal information without your consent, except to the extent required by law, in accordance with your instructions, or as identified in this Privacy statement:

- Affiliates: Our affiliates to enable them to provide services to you and to enable them to contact you regarding additional products and services in which you have expressed an interest.
- Agents and Service Providers: We sometimes contract with other companies and individuals to perform functions or services for us or on our behalf, such as hosting this Site, sending email messages, and making phone calls. They may have access to personal information, such as addresses, needed to perform their functions, but are contractually restricted from using it for purposes other than providing services for PolarStar or on our behalf.
- Legal Matters: PolarStar may preserve, and has the right to disclose, any information about you or your use of this Site without your prior permission if PolarStar has a good faith belief that such action is necessary to: (a) protect and defend the rights, property, or safety of PolarStar, other users of this Site, or the public; (b) enforce the terms and conditions that apply to the use of this Site; (c) respond to claims that any content violates the rights of Third Parties; (d) respond to claims of suspected or actual illegal activity; (e) respond to an audit or investigate a complaint or security threat; or (f) comply with applicable law, regulation, legal process, or governmental requests.

What Steps Do We Take to Protect Your Information?
This Site and all information that you submit through this Site is collected, stored, and processed in the Cayman Islands within Company-controlled databases. We restrict access to your personal information to those employees of ours, and our affiliates, and to those service providers who need to use it to provide this Site and our products or services. We have implemented physical, administrative, and technical safeguards to protect your personal information from unauthorised access. However, as effective as our security measures are, no security system is impenetrable. We cannot guarantee the security of our systems, nor can we guarantee that information you supply will not be intercepted while being transmitted to us over the Internet.

Some Other Matters
Accessing and Correcting Your Information:
Keeping your information accurate and up-to-date is very important. Inaccurate or incomplete information could impact our ability to deliver relevant services to you. Please let us know about any changes that may be required to your personal information via our "contact us" form.

External Links:
This Site may include links to other sites. If you access another organisation's website using a link provided, the other organisation may collect information from you. PolarStar is not responsible for the content or privacy practices of linked websites or their use. Once you have left this Site via such a link (you can tell where you are by checking the URL in the location bar on your browser), you should refer to those websites' privacy policies, terms of use, and practices to determine how they will handle any information they collect from you.

Applicability of This Privacy Statement to International Users:
This Privacy statement is provided in accordance with and subject to the Cayman Islands law, specifically the Data Protection Act ("DPA") of the Cayman Islands. If you access this site from a location outside of the Cayman Islands, you agree that your use of this Site is subject to the terms of this Privacy statement and the Terms of Use.

Children:
This Site it not intended for children, and we do not knowingly collect, use, or disclose information of children under the age of thirteen (13) without the consent of their parents or legal guardians. In an instance where such information was collected, it would be purely accidental and unintentional.

The key principles that PolarStar applies when processing personal information of those individuals within the scope of the DPA is as follows:

THE EIGHT (8) DATA PROTECTION PRINCIPLES:

1. *Fair and lawful use*

PolarStar endeavours to manage personal data in a way that is fair. This means processing the data in a way that is unduly detrimental, unexpected, or misleading to the individuals concerned. PolarStar remains clear, honest, and open with all clients from relationship inception and after termination about how we handle their personal data. PolarStar aims at offering the upmost fairness, lawfulness, and transparency around data handling.

2. *Purpose limitation*

PolarStar ensures that personal data is only processed for the purpose it was collected for by:

- Clearly identifying our purpose for processing;
- Regularly reviewing our processing & updating our documentation around privacy for information for individuals.

3. *Data minimisation*

PolarStar ensures that processing of personal data is adequate and relevant to fulfil the stated purpose.

4. *Data accuracy*

PolarStar actions all reasonable steps to ensure that personal data is not incorrect or misleading.

5. *Retention/Storage limitation*

personal data:

- shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required in order to safeguard the rights and freedoms of the data subject.

6. *Respect for the individual's rights*

PolarStar endeavours to ensure that personal data is processed in accordance with the rights of the individual in mind. The obligation lies with PolarStar respect the rights of the individuals.

7. *Data Security & Protection – Integrity & Confidentiality*

PolarStar ensures that personal data is kept safe. PolarStar holds integrity and confidentiality as core values throughout the business. These values are applied to personal data that must be kept secure not just from malicious attacks but from inadvertent damage too. PolarStar implements technical and organisational measures to ensure an appropriate level of data security and protection. Such measures provide for the prevention of any unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to that data.

8. *Protection for International transfers*

The eighth data protection principle of the DPA prohibits the international transfer of personal data where the jurisdiction does not present an adequate level of right protection of data subjects in relation to the processing of personal data. This does not mean that personal data cannot be transferred internationally. However, any such transfers need to be assessed against the DPA.

personal data may be transferred outside the Cayman Islands where it is adequately protected. Apex Group Administration Services Ireland Ltd. (fund administrator based in Ireland) makes use of client personal data to perform its own anti-money laundering checks to comply with legal requirements in Ireland. Apex fulfils the role of both the Data Controller and Data Processor.

The Ombudsman considers the following countries and territories as ensuring an adequate level of protection:

- Member States of the European Economic Area (EEA) (that is, the European Union plus Lichtenstein, Norway, and Iceland) where Regulation (EU) 2016/679 (the General Data Protection Regulation or "GDPR") is applicable;
- any country or territory in respect of which an adequacy decision has been adopted by the European Commission pursuant to Article 45(3) GDPR or remains in force pursuant to Article 45(9) GDPR.

PolarStar acknowledges that Ireland lies within the EEA and therefore provides an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

If you have any questions or concerns about your personal information in respect of this section, please contact us at info@polarstarfunds.com. If you consider that your personal data has not been handled correctly, or you are not satisfied with the response to any requests you have made regarding the use of your personal data, you have the right to complain to the Cayman Islands' Ombudsman. The Ombudsman can be contacted by called: + 1 345 946-6283 or by email at info@ombudsman.ky.

Changes to Privacy Statement:
The Privacy statement is subject to change at any time. It was last changed on 28th of September 2021. If we make changes to this Privacy statement, we will update the date it was last changed. Any changes we make to this Privacy statement become effective immediately when we post the revised Privacy statement on this Site. We recommend that you review this Privacy statement regularly for changes.

APPENDIX D – UNDERTAKING

To: Management of PolarStar Management SEZC (the "Company").

Re: Privacy Policy

1. I confirm that:

- I have received the Privacy Policy — Cayman Data Protection of the Company, and I have been advised of the requirements of the current version of the relevant laws, regulations, and guidance as of the date of this undertaking, in particular, any applicable statute, regulation, order, or any other legal instrument which pertains to the protection of privacy and confidentiality personal information, including (i) the Data Protection Act (Law 33 of 2017 consolidated with Law 56 of 2021), as revised; (ii) the Data Protection Regulations, 2018 (SL 17 of 2019) and any other regulation promulgated under the DPA; (iii) any 'code of practice' promulgated under section 42 of DPA; and (iv) any binding decision of the courts and tribunals of the Cayman Islands that relate to the application or interpretation of any of the foregoing;
- I have been made aware of the Cayman Islands laws and regulations relating to data protection;
- I have or will be provided with training regarding data protection and regarding the recognition and handling of Personal Data Breaches;
- I understand that, as an employee of the Company, I am a Data Owner and, consequently, I have Data Owner responsibilities;
- I understand that breaches to the data protection rules and regulations may result in fines and penalties that may be applied to the Company and the directors, managers, secretaries, or officers if the offence is proved to have been committed with their Consent or connivance or attributable to their neglect.
- I understand that any Capitalised term on this statement will have the same meaning as established in the Company's Privacy Policy.

2. I agree that this undertaking extends to any further amendment, or replacement of, the Legislation, Regulations or Guidance that the Company may, from time to time, set out in any notice.

3. I agree that the undertaking shall form part of my contract of employment. Any breach of this undertaking may result in offences, fines and penalties to the Company and myself, as established by the laws and regulations.

Signature: _____

Name: _____

Date: _____