POLARSTAR MANAGEMENT SEZC

DATA PROTECTION LAW, 2017 (THE "DPL")

June 2020

POLARSTAR

DATA PROTECTION LAW, 2017 (the "DPL")

The DPL aligns the Cayman Islands with other major jurisdictions around the world, notably the European Union, and thereby facilitates the free flow of data – a pre-requisite for the Cayman Islands being an equal and competitive participant in today's globalized economy.
The DPL provides a standard framework applied at PolarStar in the management of the personal data subjects used. PolarStar aims to best align the data protection law of the Cayman Islands with all other jurisdictions where we are active. The DPL incorporated at PolarStar is intended to reduce the administrative burden of operating internationally and cement the Cayman Islands as an attractive jurisdiction in line with international developments.

At PolarStar, the DPL implemented provides assurance to individuals whose personal data is being processed. PolarStar aims to provide all individuals with a greater sense of comfort when it comes to how we manage and control their personal data.

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;
- publicizes 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 recognizes 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 DPL 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 for the Ombudsman in Cayman when interpreting and applying the DPL.

Introduction & Key Terms:

The DPL applies to processing carried out by PolarStar Management (based in the Cayman Islands). The DPL applies to personal data processed by 'data controllers' and 'data processors'.

- A 'data controller' determines why and how personal data is processed.
- A 'data processor' processes personal data on behalf of a data controller and does not itself determine why personal data should be processed. A data processor may, to a certain extent, decide on how the personal data should be processed.
- A data controller who engages a data processor must ensure that the engagement is based on a written contract which contains certain prescribed assurances regarding the processing of personal data.

What is processing of personal data?

The DPL 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:

- organizing, 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.

Data controller vs Data Processor

The DPL defines a "data controller" as: 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 and includes a local representative.

As a data controller, one is responsible for applying the requirements of the DPL, applying the data protection principles to the personal data which is processed (or which is processed by someone else on your behalf), and cooperating with investigations of the Ombudsman.

As a data controller one is also responsible for ensuring that the data protection principles are complied with in relation to personal data being processed on your behalf (by a data processor).

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.

As a data controller, one may decide together with another organization about how and why personal data is processed, they will be a joint data controller together with the other organization. This means that both entities are jointly responsible for complying with their obligations under the DPL. While not explicitly mentioned in the DPL, it is best practice for joint 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.

The DPL 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).

PolarStar Management is established in the Cayman Islands with an office presence.
Sanne Fund Services Malta Limited (administrator) is the third-party administrator meaning that they are a separate legal entity from PolarStar, and they are based in Malta. Sanne uses the client's personal data to perform its own anti-money laundering checks to comply with legal requirements.

Data Processor is commonly a natural or legal person that processes personal data in accordance with the data controller's instructions & the terms of a written agreement (i.e. data processing agreement) on behalf of the controller.

- Data Processors should:
- maintain records of processing activities;
- cooperate with the SA (where necessary)
- implement appropriate security measures;
- inform the controller in the event of a data breach; and
- comply with the requirements of the DLR regarding cross-border data transfers
- A processor will be considered a joint controller in the event that it processes personal data other than in accordance with the instructions of the controller
- Outsourcing of data processing activities by a controller to a processor is governed by a written 'data processing agreement'.

The data controller/data processor is required to implement policies and procedures to ensure compliance and has the following direct responsibilities:

- Maintain internal records of data processing activities
- Implement robust information security measures
- Conduct Data Privacy/Legitimate Impact Assessments
- Only make use of a sub-processor with the prior written authorization of PolarStar;
- Co-operate with the Office of the Ombudsman;
- Ensure the security of its processing;
- Document the processing activities; and
- Notify any personal data breaches to PolarStar, data subjects and the Ombudsman without delay.

If a data processor/controller fails to meet any of these obligations, then it may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures.

PolarStar Management as Investment Manager and the funds that it manages are out of scope as there are no Cayman data subjects. The data controller role also fulfils the data processor role. The impact of DPL for PolarStar Management refers to all Cayman based employees and third-party Cayman relationships that the Investment Manager has.

Local Cayman Representative

PolarStar Management does not require a local Cayman representative as it has a Cayman presence with a fully staffed office. An entity based outside of Cayman would have an obligation to appoint a representative in Cayman.

What information does the DPL apply to?

Personal data

The DPL applies to 'personal data' meaning any information relating to a living individual who can be directly or indirectly identified. A number of 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 DPL applies to the processing of personal data, regardless of its format or storage medium.

Sensitive personal data

The processing of some types of personal data presents a higher risk to that person's rights and interests. The DPL explicitly recognizes certain types of data as being "sensitive personal data"; however, the processing of types of personal data not defined as sensitive under the DPL 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 DPL, 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.

PolarStar does not retain any sensitive personal data.

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 minimization*

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. *Storage limitation*

As a rule, PolarStar retains records for a period of 5 years and no longer.

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. *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.

8. *International transfers*

The eighth data protection principle of the Data Protection Law, 2017 (DPL) 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 DPL.

Personal data may be transferred outside the Cayman Islands where it is adequately protected. Sanne Fund Services Malta Limited (fund administrator based in Malta) makes use of client personal data to perform its own anti-money laundering checks to comply with legal requirements in Malta. Sanne 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.

Legal Basis for Processing

Schedule 2 of the DPL specifies the legal basis for processing personal data. At least one of the below should apply:

- ***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 rights and freedoms or legitimate interests of the individual.

Personal Data Breaches

The DPL introduces a duty on all data controllers/processors to report personal data breaches to the Ombudsman and the individual(s) whose data was breached, unless the breach is unlikely to prejudice their rights and freedoms. This is required to be done within 5 days. The Ombudsman and the individual(s) will need to be provided with certain information, including measures PolarStar has taken, and measures PolarStar recommends that the individual take. PolarStar ensures that there are robust breach detection, investigation and internal reporting procedures in place. This facilitates the communications with the Ombudsman and the data subjects.

CHECKLIST

Preparing for a personal data breach

- We know how to recognize a personal data breach.
- We understand that a personal data breach is not only about loss or theft of personal data.
- We have prepared a response plan for addressing any personal data breaches that occur.
- We have allocated responsibility for managing breaches to a dedicated person or team.
- PolarStar staff knows how to escalate a security incident to the appropriate person or team in our organization to determine whether a breach has occurred.

Responding to a personal data breach

- We have in place a process to assess the likely risks to individuals as a result of a breach.
- We know the Ombudsman is the relevant supervisory authority for our processing activities.
- We have a process to notify the Ombudsman and the affected data subjects of a breach within 5 days, even if we do not have all the details yet.
- We know what information we must give the Ombudsman and the data subjects about a breach.

- We know what information about a breach we must provide to the Ombudsman and affected data subjects, including advice to help them protect themselves from its effects.

It is best practice to record all breaches.

As with any security incident, PolarStar investigates whether the breach was a result of human error or a systemic issue and takes corrective action to ensure that recurrences are prevented – whether this is through better processes, further training or other corrective steps.

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 data has been breached. This tarnishes the reputability of PolarStar and undermines the trust data subjects have in PolarStar. Furthermore, failure to notify a breach when required to do so is an offence under the DPL and can result in a conviction and a monetary penalty imposed by the Ombudsman under section 55 of the DPL.

Notifying the Cayman Islands Ombudsman

Contact Us

The Regulatory Authority is the Cayman Ombudsman. No planned auditing as yet but should auditing commence:

- PolarStar Management would have 5 days to complete an internal risk assessment & report the issue to the Ombudsman.

Visit: 3rd Floor, Anderson Square, 64 Shedden Road, George Town, Grand Cayman
Mail: PO Box 2252, Grand Cayman KY1-1107, CAYMAN ISLANDS
Email: info@ombudsman.ky
Call: +1 345 946 6283

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

Access to Information

If you would like to make a request under the Freedom of Information Law for access to records from our office please contact our Information Manager, rene.lynch@ombudsman.ky and complete the FOI Request Form.