PROTECTION OF PERSONAL INFORMATION POLICY

Oceana Group Limited

Oceana House
25 Jan Smuts Street
Foreshore
8001

POLICY NAME	**PROTECTION OF PERSONAL INFORMATION POLICY**			**POLICY NO.**	1
EFFECTIVE DATE	1 JUNE 2021	**DATE OF LAST REVISION**	1 JUNE 2023	**VERSION NO.**	2

POLICY OWNER	Jayesh Jaga	**CONTACT INFORMATION**	Jayesh.jaga@oceana.co.za +27 21 410 1411

APPLIES TO					
BOARD MEMBERS	X	EXCO	X	PERMANENT EMPLOYEES	X
TEMPORARY EMPLOYEES	X	VISITORS	X	CONTRACTORS	X

SUMMARY OF CHANGES TO CURRENT REVISION:

NO.	DESCRIPTION OF CHANGES
1	**Change of information officer**

DOCUMENT APPROVAL LIST:

NAME	POSITION	SIGNATURE	DATE
Jayesh Jaga	**Chief ESG Officer and Information Officer**	Signed by:Jayesh Jaga Signed at:2023-07-20 18:35:21 +02:00 Reason:Witnessing Jayesh Jaga	20/07/23
Neville Brink	**CEO**	Signed by:Neville Donovan Brink Signed at:2023-07-21 08:32:42 +02:00 Reason:Witnessing Neville Donovan Brin	21/07/23
Karen-Dawn Koen	**Deputy Information Officer**	Signed by:Karen-Dawn Koen Signed at:2023-07-18 13:55:33 +02:00 Reason:Witnessing Karen-Dawn Koen	18/07/23

INTRODUCTION

Oceana has a long and proud tradition of conducting business with the highest level of integrity, in accordance with the highest ethical standards and in full compliance with all applicable laws, including the law known as the Protection of Personal Information Act, 4 of 2013, (POPIA), which regulates the Processing of Personal Information.

The Protection of Personal Information Policy has been developed at the direction of Oceana's Board of Directors in order to provide clear guidance to all directors, employees and those who Process Personal Information on behalf of Oceana on how they are to Process Personal Information, thereby ensuring that all Personal Information Processed by Oceana is done in a lawful, transparent and consistent manner and in full compliance with all and any applicable data protection laws which may from time to time apply to its operations, including POPIA and the General Data Protection Regulation 2016/679 (GDPR) applicable in the EU (hereinafter referred collectively as the "Data protection laws").

Oceana has adopted a zero-tolerance stance in relation to any non-compliance with its policies, including this Policy and any violation of this Policy will result in swift corrective action, including possible termination of employment, and criminal and civil action.

PURPOSE

The purpose of this Policy is to provide clear guidelines and directions to all Personnel on how they must Process Personal Information, thereby ensuring that Personal Information Processed by Oceana is done in a lawful, transparent and consistent manner and in full compliance with POPIA and where applicable the GDPR, and any other Data Processing laws which may from time to time apply to its operations; and establish uniform and suitable Personal Information Processing procedures and standards in respect of the Processing of Personal Information.

SCOPE

This Policy including any ancillary, associated or related rules and standards which seek to regulate the Processing of Personal Information Processed in South Africa, US or in any EU country, by Oceana, whether in an automated or non-automated manner, and regardless of how such information is stored or recorded, and regardless of when such record came into existence, applies to any persons who Process Personal Information on behalf of Oceana, including Oceana directors, employees and Operators, who will hereinafter be referred to collectively as "Personnel".

POLICY STATEMENT

The objective of this Policy is to ensure that Oceana and its Personnel comply with applicable laws, international legal standards and best practices which regulate the Processing of a Data Subject's Personal Information; protect the privacy of its Data Subjects in relation to their Personal Information; and mitigate the risks of unlawful Processing of Personal Information and avoid related data breaches.

TERMS AND DEFINITIONS

TERM	DEFINITION
Consent	means in relation to POPIA, any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Information about them; and **Explicit Consent** means in relation to the GDPR, a higher standard of Consent that requires a very clear and specific statement rather than an action which is suggestive of Consent.
Data Privacy laws	means, for the purposes of this Policy, the European Union's General Data Protection Regulation ("GDPR") which applies in the EU, and the Protection of Personal Information Act, 14 of 2013 (POPIA) which applies in South Africa.
Data Subject	means, in relation to POPIA, any individual or legal entity, and means in relation to the GDPR, an individual. (Note - the GDPR does not apply to legal entities.)
Information Officer (IO)	means in relation to POPIA, a person who has been appointed as the organization's Information Officer, being the organisation's main representative on data protection and Processing matters, and Data Protection Officer (DPO) (GDPR) means in relation to the GDPR, a person who has been appointed as the organization's Data Protection Officer, being the organisation's main representative on data protection and Processing matters.
Operator	means, in relation to POPIA, any person who Processes Personal Information on behalf of a Responsible Party as a contractor or sub-contractor, in terms of a contract or mandate, without coming under the direct authority of the Responsible Party and **Processor** means, in relation to the GDPR, any person who Processes Personal Information on behalf of a Controller as a contractor or sub-contractor, in terms of a contract or mandate, without coming under the direct authority of the Controller.
Processing Notices	means a notice setting out the prescribed information that must be provided to Data Subjects before collecting his, her or its Personal Information, (also known as "section 18 notices", "privacy notices" or "data protection notices").
Personal Information	means Personal Information relating to any identifiable, living, natural person, in the case of POPIA and the GDPR and an identifiable, existing juristic person, in the case of POPIA, including, but not limited to: • name, address, contact details, date of birth, place of birth, identity number, passport number, • bank details, • qualifications, expertise, employment details, • tax number, • vehicle registration; • dietary preferences; • financial details including credit history; • next of kin / dependants;

	• education or employment history; and • **Special Personal Information**, being including race, gender, pregnancy, national, ethnic or social origin, colour, physical or mental health, disability, criminal history, including offences committed or alleged to have been committed, membership of a trade union and biometric information, such as images, fingerprints and voiceprints, blood typing, DNA analysis, retinal scanning and voice recognition.
Personnel	means Oceana directors, employees and any other person who may Process Personal Information on behalf of Oceana.
Processing, Process , Processed	means in relation to Personal Information, the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use; dissemination by means of transmission, distribution or making available in any other form; merging, linking, as well as restriction, degradation, erasure or destruction of information; or sharing with, transfer and further Processing, including physical, manual and automatic means.
Purpose	means the underlying reason why a Responsible Party or Controller needs to Process a Data Subject's Personal Information.
Responsible Party	means, in relation to POPIA, the person or legal entity who is Processing a Data Subject's Personal Information; and **Controller** means, in relation to the GDPR, the person or legal entity who is Processing the Data Subject's Personal Information;
Record	means any recorded information housing Personal Information Processed by Oceana, or its Personnel, regardless of form or medium, including any of the following: Writing on any material; information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored; label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means; book, map, plan, graph or drawing; photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced, in the possession or under the control of Oceana; whether or not it was created by Oceana and regardless of when it came into existence, and "Folder" for the purpose of this Policy includes any Folder, in paper or electronic format, that stores, houses or holds specific Records allocated thereto.

REQUIREMENTS

1. The Protection of Personal Information Act, 114 of 2013 (POPIA), came into operation on 1 July 2020.

POPIA governs the Processing of Personal Information with the central aim of upholding a person's right to privacy as provided for in the South African Constitution. POPIA achieves this by placing obligations on persons who request, collect, store, process and otherwise use Personal Information relating to another person, in order to protect such person from suffering potential damage or harm. More importantly POPIA seeks to achieve this by introducing penalties which will cater for instances of a breach of privacy of a person's Personal Information.

2. GDPR – UK AND EU

The General Data Protection Regulation ("GDPR") governs the processing of personal data belonging to individuals. The regulation was put into effect on May 25, 2018. The GDPR applies to any person or entity who Processes the personal data of EU citizens or residents, or who offer goods or services to EU citizens or residents regardless of whether the entity is situated in the EU.

3. PERSONAL INFORMATION PROCESSING PRICIPLES AND CONDITIONS

The GDPR and POPIA embrace and adopt a core set of universal Processing principles, (known as conditions under POPIA) which have to be met by any person who Processes another's Personal Information, which principles have informed Oceana's approach to Processing Personal Information.

These principles are as follows:

- **Lawfulness, fairness and transparency:** Personal Information must be Processed lawfully, fairly and in a transparent manner.
- Purpose limitation: Personal Information must be collected for specified, explicit and legitimate purposes and not further Processed in a manner that is incompatible with those purposes.
- **Data minimization:** The Processing of Personal Information must be limited to what is needed for the purpose, and to this end must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.
- **Accuracy:** Personal Information Processed must be accurate and, where necessary, kept up to date; and every reasonable step must be taken to ensure that inaccurate Personal Information, having regard to the purposes for which it is Processed, is erased or rectified without delay.
- **Storage limitation:** Personal Information must be kept for no longer than is necessary for the purposes for which the Personal Information was Processed and may not be stored for longer periods unless there are reasons for such longer storage.

- **Integrity and confidentiality and security:** Personal Information must be Processed in a manner that ensures appropriate security of the Personal Information, including protection against unauthorised or unlawful Processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. Furthermore Personal Information shall not be transferred to another country unless the person transferring the Personal Information ensures that the Data Subject is provided with the same rights and level of protection in relation to the Processing of its Personal Information in the receiving country as provided for and received under POPIA or the GDPR.
- **Accountability:** The person who is Processing the Personal Information, known as the Responsible Party, (POPIA) or Controller (GDPR) is responsible for compliance with the Data Processing laws and the principles and conditions for Processing, and such Responsible Party or Controller must be able to demonstrate compliance with the Data Processing laws including POPIA or the GDPR and these principles.

4. AREAS WHERE OCEANA PROCESSES PERSONAL INFORMATION

- Oceana is a fishing and commercial cold storage company which, inter alia, harvests and distributes a diverse range of marine resources in South Africa and overseas.
- Oceana in order to carry out its business and realise its objectives, does and will continue to make use of Personal Information which belongs to individuals and public and private entities, including employees and directors, service providers, customers and other third parties.
- The Processing of this Personal Information mostly takes place in South Africa.
- There will however be occasions where certain Oceana Processing activities take place in countries situated in the US and EU.
- In light of these Processing activities, Oceana as a law-abiding entity is obligated and will ensure that it and its Personnel, comply with POPIA, and where applicable with the GDPR, and the applicable Processing principles and conditions when carrying out is business.

5. LAWFUL BASIS FOR PROCESSING

- In terms of POPIA, and where applicable the GDPR, where Personal Information is Processed such Processing must be done lawfully and in a reasonable manner that does not infringe on the privacy of the Data Subject.
- In order to discharge the above obligations, Personnel must comply with the Processing guides, rules and procedures set our below.

6. CONSENT

- A Data Subject does not have to Consent to the Processing of his, her or its Personal Information where there is a lawful basis for such Processing.
- A lawful basis for Processing in terms of the Data Processing laws, is where:
    - the Processing is necessary to conclude a contract to which the Data Subject is a party and to perform contractual obligations or give effect to contractual rights;
    - the Processing is necessary in order to comply with a law or to comply with certain legal obligations imposed by a law;
    - the Processing is necessary to protect Oceana's legitimate interests or rights,
    - the Data Subject's legitimate interests or rights or a third party's legitimate interests or rights, unless there is a good reason to protect the Data Subject's Personal Information which overrides those legitimate interests;
    - the Processing is necessary in order to perform a public duty or to perform tasks carried out in the public interest or the exercise of official authority.

- Where there is no lawful basis for the Processing, then the Data Subject,
    - has to Consent to the Processing, where the Processing is done in South Africa, which must be freely and genuinely given; or
    - has to provide Explicit Consent to the Processing, where the Processing is done in the UK or a country falling within the EU, which must be freely and genuinely given.
    - Personnel must ensure that prior to Processing a Data Subject's Personal Information, that there is either a lawful reason for the Processing, or alternatively that the Data Subject has Consented to such Processing, which lawful reason will be described under the specific and informative Oceana Processing notice, or in the absence of a lawful reason, will call for the Data Subject's consent.
    - A Data Subject may withdraw his, her it its Consent or Explicit Consent to Processing so long as it provides Oceana with a "withdrawal of consent notice", which notice is available on the Oceana website, which request will be handled and actioned directly by the Oceana Information Officer, which outcome in turn, will be relayed to the respective Personnel who has been Processing such Personal Information.
    - A Data Subject may not with withdraw Consent where no Consent (POPIA) or Explicit Consent (GDPR) is required, i.e. where Oceana can show that there is a lawful basis for the Processing. In such a case the Data Subject may only object to such Processing, provided that an "Objection notice" is sent to Oceana, which notice is available on the Oceana website, which request will be handled and actioned directly by the Oceana Information Officer and which outcome will be relayed to the respective Personnel who has been Processing such Personal Information.
    - Where a Data Subject withdraws Consent or Explicit Consent or objects to the Processing, in such case Oceana and the respective Personnel who has been Processing the impacted Personal Information, will have to stop Processing the Personal Information, unless Oceana can show compelling legitimate grounds for the Processing which overrides the interests, rights and freedoms of the Data Subject, or the Processing is necessary for the establishment, exercise or defence of legal claims.
    - The Information Officer will at the time of the withdrawal or objection referred to under 11.5 and 11.6, explain to the Data Subject the effects and consequences of any withdrawal or objection.

7. PURPOSE SPECIFIC

- Personal Information may only be collected for a specified, explicit and legitimate purpose; must only be used for the purpose for which it was collected and for no other purpose, unless the Data Subject has been informed of the other purposes; may not be further Processed or used

for any subsequent purpose, unless that Personal Information is required for a similar purpose; and such Processing is compatible with the initial purpose.

- Oceana for the purposes of carrying out its business and related objectives Processes Personal Information belonging to a vast range of Data Subjects, including employees and staff, prospective employees and job applicants, students and interns, service providers and contractors, vendors, clients, customers, and other third parties, which Processing is required for a variety of business related purposes - managing employees - employment.
- Personnel must ensure that before Personal Information is Processed, there is a valid and legitimate reason for such Processing; advise all Data Subjects why the Personal Information is required, i.e. the purpose for the Processing, which purpose will be described under the specific and informative Oceana Processing notice, housed on the Oceana website; direct the Data Subject to the applicable area of the Oceana website where the specific and informative Oceana Processing notice is housed.

8. ACCURACY

- All Personal Information Processed by Oceana must be accurate and, where necessary, kept up to date.
- Personnel in order to ensure that Personal Information is accurate, and is up to date, must:
  - take all and every reasonable step to ensure that all Personal Information which they Process is accurate, having regard to the purposes for which it is Processed, and where it is found to be inaccurate, that it is where possible, updated and rectified without delay;
  - implement procedures allowing Data Subjects to update their Personal Information;
  - send out regular communications to Data Subject requesting "updates to details" which if responded to, should be acted on immediately by the relevant or responsible department;
  - where appropriate, and possible, ensure that any inaccurate or out-of-date records are updated and the redundant information deleted or destroyed;
  - take note of the rights of the Data Subject in relation to updates and rectifications of Personal Information, housed under the Oceana Processing Notices and give effect to any update request, when such request has been communicated through to it by the Information officer.

9. DATA MINIMISATION

- Oceana may not Process Personal Information which is not necessary for the Purpose for which the Personal Information is Processed.
- Personnel must ensure that when they processes Personal Information on behalf of Oceana, that it is adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed; and revisit all pre-populated questionnaires and forms which are currently used to collect or house Personal Information and consider the purpose or reason for the collection and thereafter analyse the types of Personal Information which is request or collected and where of the view that certain Personal Information is not needed for the defined purpose, then such information should no longer be called for, collected and / or recorded and the relevant areas where this information is housed or asked for should be deleted.

10. TRANSPARENCY AND PROCESSING NOTICES

- Oceana has a duty to show that it has dealt with a Data Subject in a transparent manner.
- In order to demonstrate transparency, Oceana must provide all Data Subjects, with a specific and informed Processing notice, at the time when Oceana collects and Processes a Data Subject's Personal Information or within a reasonable period thereafter, which Processing notice must set out:
  - the types of Personal Information Processed, and the purpose or reason for the Processing;
  - the lawful basis relied upon for such Processing or whether Consent or Explicit Consent is required for the Processing;
  - the period for which the Personal Information will be retained;
  - who the Personal Information will be shared with, including external or cross border transfers and the mechanism(s) relied upon for such transfer;
  - the security measures which are in place to protect the Personal Information, including where the Personal Information is sent to parties' cross border and the mechanism(s) relied upon for such protection; and
  - the respective rights of the Data Subject and how these rights may be exercised.

- In order to meet its obligations under 10.2 above, Oceana has developed and placed on its websites the following informed and specific Processing notices which apply to the different Data Subject categories who it deals with:
  - an **HR Processing Notice**, which applies to all employees – perspective and actual, all bursary or learnership beneficiaries- perspective or actual;
  - a **Procurement Processing Notice**, which applies to all participants in the Oceana supply chain, including persons who provide goods and services to Oceana (service providers), persons or entities who purchase goods or services from Oceana (Customers), and / or other parties who Oceana may engage with and who make up the Oceana Procurement and supply chain, including Regulators;
  - a **Corporate Social Investment (CSI) Processing Notic**e, which applies to CSI beneficiaries, perspective or actual who Oceana may engage with;
  - a **Company Secretarial Processing Notice**, which applies to directors, trustees, executives, committee members, shareholders and stakeholders who Oceana may engage with;
  - **OET Processing Notice**, which applies to all Oceana Empowerment Trust Beneficiaries who Oceana may engage with;
  - Security Processing Notice, which applies to any persons who come onto the Oceana sites, facilities and offices who Oceana may engage with;

- In order to give effect to the above transparency requirement, Personnel:
  - must all understand the provisions of the Data Processing laws;
  - familiarise themselves with the above-mentioned Oceana Processing Notices and any others which Oceana may implement from time to time, and any changes made thereto;
  - familiarise themselves with, where applicable, Oceana's standard binding corporate rules, its standard Personal Information transfer agreement and / or its Operator agreement;
  - ensure that all Oceana documents, forms or other records (Records) which house or call for Personal Information contain the following Data Processing details:
    "Please note that in order for Oceana to engage with you, it will have to Process certain Personal Information which belongs to you, which Processing is described and explained under the specific and informative Oceana Processing Notices, housed for ease of reference on the Oceana website. By providing us with the required Personal Information, such act will be taken as an indication that you have read and agree with the provisions described under the Processing Notice."
  - at the time of Processing, direct the Data Subjects who they deal with to the applicable area of the Oceana website where the specific and informative Oceana Processing notice is housed.

11. GENERAL DUTIES: CONFIDENTIALITY, INTEGRITY AND SECURITY OF PERSONAL INFORMATION

- In order to safeguard, secure and ensure the confidentiality and integrity of all Personal Information held by or under the control of Oceana, Oceana must:
  - identify all reasonably foreseeable internal and external risks to Personal Information in its possession or under its control;
  - document the identified risks;
  - establish, in response to the identified risks, reasonable technical and organisational measures across all areas where Personal Information is held or stored, including electronic and physical mediums;
  - implement and maintain all approved and required measures across all areas where Personal Information is held or stored, including electronic and physical measures, all which are designed to minimise the risk of loss, damage, unauthorised destruction and / or unlawful access of Personal Information;
  - regularly verify that these measures are effectively implemented; and ensure that the measures are continually updated in response to new risks or deficiencies in previously implemented measures and safeguards, which measures include, where appropriate, among others, the following: the pseudonymisation and encryption of Personal Information; ongoing efforts to ensure the long-term confidentiality, integrity, availability and resilience of Personal Information housed within the Oceana environment; applications and processes which have the ability to rapidly restore the availability of and access to Personal Information in the event of a tangible or technical incident; and procedures for the regular review, assessment and evaluation of the effectiveness of the technical and organizational measures taken to ensure the security of Processing, including regular IT Security Audits.
- The duty to ensure data privacy, confidentiality and integrity of Personal Information starts when Oceana initially interacts with a Data Subject and will continue throughout the relationship, until the purpose for the Processing of the Personal Information comes to an end.
- In order to give effect to the above, all Personnel must:
  - keep all Personal Information, safe, secure and confidential and ensure that the confidentiality and security of Personal Information is maintained at all times;
  - identify all reasonably foreseeable internal and external risks to Personal Information which is in their possession or under their control;
  - establish and maintain appropriate safeguards against the risks identified;
  - regularly verify that the safeguards are effectively implemented;
  - ensure that the safeguards are continually updated in response to new risks or deficiencies in previously implemented safeguards;
  - not attempt to circumvent any administrative, physical or technical measures which Oceana has implemented in order to minimise, in relation to Personal Information, the risk of loss, damage, unauthorised destruction and / or unlawful access thereto;
  - ensure that prescribed security measures and controls are implemented or where instructed followed to prevent all and any unauthorised access to Personal Information, the accidental deletion of Personal Information or the exposure of Personal Information to malicious hacking attempts.

12. OPERATORS

- Where Oceana makes use of an Operator or a GDPR Processor it must ensure that a written agreement is concluded between Oceana and the Operator, which sets out the rules which the Operator will have to follow when Processing Personal Information on behalf of Oceana.
- Oceana has developed a standard Operator Agreement for this purpose, which agreement is housed on its website.
- All Personnel must:
  - familiarise themselves with the standard Oceana Operator agreement;
  - ascertain who they use as Operators, now and in the future, include such details under an Operator register, and ensure that all such Operators sign the standard Oceana Operator agreement or a similar one which has been approved and signed off by the Oceana Legal Department;
  - ensure that Operator agreement is followed by an Operator;
  - where an Operator agreement is breached, bring this to the attention of one's line manager and the Information Officer and following a decision reached by these parties, carry out the planned course of action, which ultimately must aim to protect and secure the Personal Information which is the subject matter of that Operator agreement.

13. SHARING PERSONAL INFORMATION

- Oceana may not share Personal Information with third parties, unless:
  - there is a legitimate business need to share the Personal Information; or
  - the Data Subject has been made aware that his, her or its Personal Information will be shared with others and has, where required, given consent to such sharing; and
  - the person receiving the Personal Information has either agreed to keep the Personal Information confidential and to use it only for the purpose for which it was shared under the standard Oceana Personal Information transfer agreement, which is housed on the Oceana website or where acting as an operator or a GDPR Processor, has concluded an Operator agreement with Oceana, before receipt of the Personal Information.
- In order to ensure that the above takes place, Personnel must ensure:
  - that where Personal Information is shared externally with a third party, on a need to know basis, that the standard Oceana Personal Information transfer agreement is concluded with the recipient, before receipt of the information;
  - that where Personal Information is shared with an Operator, that the standard Oceana Operator agreement is concluded with the Operator before receipt of the Personal Information;
  - that any requested deviations for the standard Oceana Personal Information transfer agreement or the Operator agreement is vetted and approved by the Oceana Legal Department;
  - when sending emails which contain Personal Information, that they are marked "confidential", do not contain the Personal Information in the body of the email, whether sent or received, but rather placed in an attachment, which email is then encrypted before being transferred electronically;
  - that Personal Information is not transferred or sent to any entity not authorised directly to receive it;
  - that where Personal Information is to be sent by facsimile transmission, that the recipient has been informed in advance of the transmission and that he or she is waiting by the fax machine to receive the data;
  - that where Personal Information is transferred physically, whether in hardcopy form or on removable electronic media that it is passed directly to the recipient or sent using recorded deliver services and housed in a suitable container marked "confidential";
  - that where Personal Information is shared internally, that adequate measures are put in place to protect the confidentiality and integrity of such information.
- The standard Oceana Data transfer agreement and Operator agreement can be accessed by using these hyperlinks.

14. CROSS BORDER TRANSFERS OF PERSONAL INFORMATION

- Oceana may not transfer Personal Information to another party who is situated outside South Africa, or outside any territories falling within the EU, unless
  - the Data Subject Consents (POPIA) or Explicitly Consents (GDPR) to such Processing; or
  - the transfer is necessary in order to perform a contract between Oceana and a Data Subject, or for reasons of public interest, or to establish, exercise or defend legal claims or to protect the vital or legitimate interests of the Data Subject in circumstances where the Data Subject is incapable of giving Consent; or
  - the country where the Personal Information is being transferred to provides the same level of protection for the Data Subject (s) as housed under the data processing laws applicable in South Africa, or in the EU; or alternatively,
  - Oceana has concluded an agreement with the recipient of the Personal Information, either in the form of a standard binding corporate rule, or an Operator agreement or a Personal Information transfer agreement, which sets out the rules which apply to the receipt and subsequent Processing of that Persona Information.
- In order to ensure that the above is followed, Personnel may not transfer Personal Information to areas outside South Africa, or to areas outside territories within the EU, unless one of the following controls and safeguards are in place:
  - the European Commission or the South African Data Privacy Regulator has issued an "adequacy decision" confirming that the territory or country where Oceana proposes transferring the Personal Information to, has adequate Data Protection laws in place which will afford the Data Subject with the same level of protection as that under POPIA or the GDPR, as the case may be;
  - a standard binding corporate rule is in place, which covers the recipient of the Personal Information;
  - the standard Oceana Personal Information data transfer agreement or Operator agreement has been concluded with recipient of the Personal Information;
  - Oceana has an approved code of conduct in place which has been approved by the Information Regulators which allows such transfers;
  - the Data Subject has given Consent (POPIA) or Explicit Consent (GDPR) to the proposed transfer, having been fully informed of any potential risks;
  - the transfer is necessary in order to perform a contract between Oceana and a Data Subject, for reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject in circumstances where the Data Subject is incapable of giving Consent (POPIA),or Explicit Consent (GDPR).

15. DIRECT MARKETING

- Direct marketing, including unsolicited direct electronic marketing is prohibited unless the Data Subject has consented to the receipt of this marketing material.
- In order to ensure that direct marketing is sent out in a lawful manner, all Personnel must ensure that:
  - all Oceana customers, when approached or dealt with for the first time, are given the opportunity in an informal manner to agree or disagree to the receipt of any Oceana direct marketing material;
  - before direct marketing is sent to a non-customer that such person provides his, her, or its consent thereto, which will be in the form of the prescribed "opt in" notice, available on the Oceana website;
    when marketing material is sent to Data Subjects, that the material houses an "opt out" form, allowing the Data Subject to opt out of any further marketing material; and

- when a Data Subject exercises his, her or its right to object to receiving direct marketing, in the form of an opt out, that such opt out is recorded and given effect to, and that no further direct marketing is sent to the opted out customer.
- The Oceana marketing opt in and opt out forms are available on its website.

16. REPORTING PERSONAL INFORMATION BREACHES

- In the event of a Personal Information breach, Oceana has a duty to give notice of such breach to:
  - the Information Control Officer (ICO) in the case of a breach in the EU;
  - to the Information Regulator in the case of a breach in South Africa, and
  - to the affected Data Subjects in the case of a breach in South Africa or the EU.
- Oceana has put in place appropriate procedures to deal with any Personal Information breach and will notify the ICO / Information Regulator and / or the Data Subjects, as the case may be when it is legally required to do so.
- Personnel have a duty to:
  - immediately report through to the Information Officer, any suspected or known Personal Information breach; in the prescribed Oceana data breach report, which report must contain the following details: categories and approximate number of Data Subjects concerned; categories and approximate number of Personal Information records concerned; the likely cause of and the consequences of the breach; details of the measures taken, or proposed to be taken, to address the breach including, where appropriate, measures to mitigate its possible adverse effects;
  - keep such information strictly private and confidential;
  - not to deal with any persons in relation to the Personal Information breach, including any officials to investigators, noting that only the Information Officer with the approval of the Organization's Board has the right to report any Personal Information or security breach to the ICO / Information Regulator and / or the affected Data Subjects, as the case may be.
  - The Oceana data breach report is available on its website.

MANAGEMENT ROUTINES

Information Officers, Data Protection Officers and deputies

- Oceana has appointed in South Africa, in respect of all Personal Information Processed in South Africa, the following Information Officer:
  Jayesh Jaga
  Chief ESG Officer

- Oceana has appointed, in respect of all Personal Information Processed in the UK and the EU the following Data Protection Officer:
  Jayesh Jaga
  Chief ESG Officer

- The Information Officer and the Data Protection Officer have the right to appoint and to delegate certain activities to deputy Information Officers, or Data Protection Officers.

EXCEPTIONS

None

RELATED POLICIES AND OTHER REFERENCES

1. Oceana Document Management Policy
2. Records Management and Retention Standard Operating Procedure
3. PAIA Manual
4. IT End User Agreement

Where any of the above-mentioned Policies conflict with this Policy, then in so far as the conflicting provision (s) provide for and apply to the Processing of Personal Information, then the provisions housed under this Policy will prevail.

ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
Information Officer and Deputy Information officer	1. developing, constructing and once prepared, implementing and overseeing an enterprise wide Personal Information Processing framework and related roadmap;

2. developing, constructing and once prepared, implementing and overseeing the various Personal Information Processing policies and procedures, including this Policy;

3. monitoring compliance with this Policy, the various Personal Information Processing policies, procedures and the Data Processing laws;

4. providing all Personnel with the necessary and required Personal Information Processing training;

5. providing on - going guidance and advice on Personal Information Processing;

6. conducting Personal Information impact assessments when required, including base line risk assessments of all the Organization's Personal Information Processing activities;

7. ensuring that all operational and technological Personal Information and data protection standards are in place and are complied with;

8. working closely with IT in order to ensure that appropriate technological and operational measures have been implemented in order to ensure the safety and security of all electronically stored Personal Information;

9. receiving and considering reports from IT about compliance with all technological and operational data protection standards and protocols;

10. be entitled and have authorisation in conjunction with the Oceana HR function, to initiate disciplinary proceedings against Personnel who breach any technological and / or organisational and / or operational data protection standard, rule, custom, instruction, policy, practice and / or protocol (verbal, in writing or otherwise), including this Policy;

11. review and approve any contracts or agreements which deviate from the standard Oceana Processing documentation;

12. attend to requests and queries from Data Subjects, including requests for access to their Personal Information;

13. liaising with and / or co-operating with any regulators or investigators or officials who may be investigating a Personal Information or data privacy matter.

14. All queries and concerns in relation to the Processing of Personal Information within the Oceana operations or concerning Oceana activities, must be taken up with the Information Officer.

CONTACTS

List contacts in the table.

SUBJECT	CONTACT	PHONE	EMAIL
Information Officer	Karen-Dawn Koen	021 410 1475 082 044 5400	Karendawn.Koen@oceana.co.za
Deputy Information Officer	Jayesh Jaga	021 410 1411 082 495 4225	Jayesh.Jaga@oceana.co.za

VERSION HISTORY

VERSION	APPROVED BY	REVISION DATE	DESCRIPTION OF CHANGE	AUTHOR
1	Jillian Marais	June 2021	New Policy	Nabeelah Edwards
2	Jayesh Jaga	June 2023	New Information Officer	Nabeelah Sawant

LEGAL COMMENTS

NON-COMPLIANCE

- Compliance with this Policy and any related procedures and policies, including those detailed under 27, is mandatory.
- Any transgression of this Policy, and any related procedures and policies, will be investigated and may lead to disciplinary, civil and criminal action being taken against the offender.

- Further information on the Data protection laws, the Oceana Processing of Personal Information procedures and issues, including specific practical guidance on issues of particular relevance to Oceana staff, can be found on Oceana website, under the following URL.

NON-COMPLIANCE PENALTIES

- Failure to comply with the Data Processing laws may have severe consequences for Oceana, including criminal sanctions, civil claims, damages and potential administrative fines of up to R10 000 000 (ten million rand) in the case of Processing activities in South Africa, and up to €20 million (twenty million euro) or 4% of Oceana's total worldwide annual turnover, whichever is higher, in the case of Processing activities in the EU.
- In light of these high penalties, any violation or breach of this Policy will result in swift corrective action, including, possible termination of employment, and criminal and civil action.

ADDITIONAL NOTES

TRAINING

Oceana will conduct regular training sessions covering the contents of the data privacy laws and Oceana's related Personal Information Processing policies and procedures, which will be available to all Personnel.

Personnel must:

- attend the scheduled and offered training;
- do all that is necessary in order to understand the data privacy laws and how they may impact on Oceana's Personal Information Processing activities;
- familiarise themselves Oceana's Personal Information Processing policies, procedures and prescribed forms;
- ensure that they Process Personal Information in accordance with the Data Processing laws, this Policy, the training, the related policies and procedures and / or any guidelines issued by Oceana from time to time.