OPOL DATA PRIVACY POLICY

as at 25 May 2018

1. Introduction, Aims and Scope

1.1. The Offshore Pollution Liability Association Ltd ("OPOL") is committed to conducting its business in a manner that protects and values each individual's personal data, and processes said personal data fairly, lawfully, and ethically.

1.2. This policy (the "Policy") sets out OPOL's policy on data protection, and outlines an agreed set of standards by which OPOL, our employees, managers, agents and third parties contracting with OPOL, implement our commitment with regards to our processing personal data.

1.3. The explicit aim of this Policy is to support the management of data protection within OPOL by providing this agreed set of standards. All employees, managers, agents and contractors in the relevant territories and businesses should familiarise themselves with the processes and procedures set out herein and comply with them at all times.

1.4. This Policy applies when OPOL processes (whether electronically or otherwise) Personal or Special Category Personal Data or when Personal or Special Category Personal Data is processed on behalf of OPOL. Subject to Paragraph 1.5, OPOL shall treat data concerning a natural person as personal data, irrespective of their nationality, citizenship, or residence.

1.5. This Policy further applies when Personal or Special Category Personal Data is processed (whether electronically or otherwise) in:

1.5.1. The United Kingdom;

1.5.2. Any EEA country; or

1.5.2.1. Any country where the European Commission has made a finding of adequacy in accordance with Article 45 of the General Data Protection Regulation.

1.6. This Policy forms part of a framework governing OPOL's practices in relation to data privacy and should be read in conjunction with such other policies and

processes referenced within it. Linked policies and processes are identified at Paragraph 4 of this Policy ("Specific Policies").

1.7. This Policy shall apply subject to any Specific Policy, and in the event of direct conflict, the Specific Policy shall take precedence. In the event of ambiguity which falls short of conflict between this Policy and any Specific Policy, advice must be sought from OPOL's managing director (the "MD"), who will adjudicate on the ambiguity and update the policies and processes accordingly. The guiding principle in such cases, absent specific advice from the MD shall be to take the step that least infringes upon the data protection rights of the Data Subject, unless some other step is manifestly in their best interests.

1.8. For operational purposes, there may be occasions where deviations to this Policy or any linked Policies are required. Where this is necessary and justified, the deviations shall be provided in separate policy or policy documents.

2. Definitions

2.1. This Policy, unless indicated otherwise, adopts the definitions contained in the General Data Protection Regulation. Specifically, this Policy relies on the below definitions.

2.1.1. **Personal Data** means "*any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*."

2.1.2. **Special Category Personal Data** "*personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation*" and "*personal data relating to criminal convictions and offences or related security measures*."

2.1.3. **Processing** means "*any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.*"

2.1.4. **Data Controller** means "*the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.*"

2.1.5. **Data Processor** means "*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.*"

2.1.6. **Data Subject** means "*an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.*"

2.1.7. **Third Party** means "*a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.*"

2.1.8. **Consent** means "*any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.*"

2.2. In addition, the Policy relies on the following further definitions:

2.2.1. **General Data Protection Regulation** or **GDPR** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

2.2.2. **GDPR Enforcement Date** means 25 May 2018.

2.2.3. **Applicable Data Protection Law** means the General Data Protection Regulation and/or the Data Protection Act 2018 (if and insofar when enacted), orders and regulations made pursuant to the Data Protection Act 2018, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector, the Privacy and Electronic Communications (EC Directive) Regulations 2003, and any subsequent legal instrument which either amends or replaces Directive 2002/58/EC.

2.2.4. **Applicable Guidance** means guidance and/or codes of practice and/or outcomes of any enforcement action issued and/or published by the Information Commissioner's Office, the Article 29 Working Party and the European Data Protection Board, or any successor bodies to these organisations, as amended or updated by said organisations.

3. Our responsibilities and obligations under Applicable Data Protection Law

3.1. The Applicable Data Protection Law provides for a framework of rights and duties that OPOL is, subject to the qualifications outlined in Paragraphs 1.4 to 1.7 above, legally bound to comply. The foundation of the Applicable Data Protection Law is the General Data Protection Regulation. This is based on six principles, that form the foundations of OPOL's approach to data protection. These six principles are:

3.1.1. **Lawfulness, fairness and transparency**: Personal Data must be processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

3.1.2. **Purpose limitation**: Personal Data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

3.1.3. **Data minimisation**: Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

3.1.4. **Accuracy**: Personal Data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that Personal Data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

3.1.5. **Storage Limitation**: Personal Data must 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.

3.1.6. **Integrity and Confidentiality**: Personal Data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3.2. OPOL accepts the importance of the above six principles, and understands that OPOL is responsible for demonstrating compliance with the above six principles. This Policy, along with the linked policies outlined in paragraph 4 below, and most importantly, the processes underpinning these policies, outline the scope and nature of our compliance with the above six principles.

4. Policies and processes

4.1. In order to demonstrate our compliance with our responsibilities and obligations under the Applicable Data Protection Law, OPOL has a number of policy documents linked this Policy. These policy documents are as follows:

4.1.1. **OPOL Data Retention Policy**: this policy document outlines the nature and length of the time-frames by which OPOL retains personal data, and the legal bases for this retention.

4.1.2. **OPOL Subject Rights Policy**: this policy document outlines our processes and procedures used when responding to requests from Data Subjects pursuant to their rights as a Data Subject (where OPOL is acting as a Data Controller).

4.1.3. **OPOL Data Incident Management Plan**: this plan outlines the way in which OPOL (and its managers, Charles Taylor group) will report and respond to suspected data incidents, including breaches of the Applicable Data Protection Law and any other incidents where there is a material risk of the unauthorised or unlawful processing of personal data.

4.2. In addition, a number of further exercises have been undertaken, or are in the process of being undertaken, in order to comply with our responsibilities and obligations:

4.2.1. **OPOL Data Inventory**: OPOL has undertaken work to map and audit the data used by OPOL, in particular:

4.2.1.1. whether this data is Personal Data and/or Special Category Personal Data;

4.2.1.2. in what manner is this data is processed by OPOL;

4.2.1.3. where jurisdictionally such data is held; and

4.2.1.4. under what legal bases such data is processed.

4.2.2. **Gap Analyses**: OPOL has undertaken gap analyses into order to assess the level at which OPOL is compliant with the Applicable Data Protection Law and Applicable guidance.

4.2.3. **Data Protection Impact Assessments and Privacy Impact Assessments**: these assessments have been undertaken or are in the process of being undertaken by OPOL.

4.3. The above policy documents and exercises will be reviewed and updated regularly/annually, and in particular, Data Protection Impact Assessments and Privacy Impact Assessments will be undertaken when OPOL concludes that a new method of processing is likely to lead to a high risk to Data Subjects' data protection and/or privacy rights.

5. Governance Arrangements

5.1. In order to demonstrate such compliance with the Applicable Data Protection Law, the Applicable Guidance, and the above policies, the below governance arrangements have been put in place.

5.1.1. This Policy is directed by the MD who also maintains data privacy principles on behalf of OPOL, along with policies, processes and tools. The MD will also keep copies of all data protection documentation, including data inventories, lawful bases of processing, and all registration documentation so as to provide the Information Commissioner with a single point of contact for all data protection related queries.

5.1.2. The MD, in conjunction with its managers, the Charles Taylor group, acting as "joint controllers" of any Personal Data held and/or processed by or on behalf of OPOL, helps to facilitate implementation of privacy matters within OPOL and coordinates responses to Data Subjects. The MD is also the nominated point of contact for data protection authorities.

5.1.3. The MD is also responsible for responding to requests from Data Subjects to exercise their rights, conducting initial Privacy Impact Assessments and escalating matters to OPOL's board of directors as and when required and shall ensure that:

5.1.3.1. a record of Processing operations conducted by OPOL which shall record the legal basis upon which processing operations are undertaken is duly maintained.

5.1.3.2. notice is provided to Data Subjects detailing how their data is to be processed and who their data may be shared with at all points of data collection. The MD shall further maintain a record of all privacy notices in use accompanied by copies of any historic privacy notices that have been either amended or withdrawn.

5.1.3.3. an inventory detailing the various data sets held within OPOL and the legal basis under which data is processed is duly maintained.

5.1.3.4. employees, managers, agents and contractors are made aware of this Policy and the other policies outlined in Appendix 1 below, and that the employees, managers, agents and contractors working receive suitable training in order to comply with aforementioned policies.

5.1.3.5. the Data Inventory is up to date at all times and shall ensure that where new processes or systems are introduced that involve the processing of Personal Data, details of those systems are added to the Data Inventory.

6. The role of Employees, managers, agents and contractors

6.1. All of OPOL's employees are required, as a part of their contract of employment, to confirm that they have read, understood and will comply with this Policy along with any associated policies and subsequent revisions. Any failure to comply with this Policy may constitute an act of misconduct which, following investigation, may result in termination of the employee contract.

6.2. All of OPOL's managers (including, the Charles Taylor group), agents and contractors are required, as a part of their service agreements, to confirm that they have read, understood and will comply with this Policy along with any associated policies and subsequent revisions. Any failure to comply with this Policy may constitute breach of contract which may result in termination of their service agreements.

6.3. All employees, managers, agents and contractors are required, on receipt of a request from a Data Subject exercising their rights to immediately notify the MD.

7. Processing, storage, retention and destruction of data

7.1. OPOL processes Personal and may have to process Special Category Personal Data for the following broad purposes: the administration of the OPOL Agreement.

Collection and use of Special Category Data

7.2. OPOL may collect and process Special Category Personal Data from time to time.

7.3. Records of the processing of Special Category Personal Data shall be retained by the MD.

Consent

7.4. Where OPOL relies upon consent as a valid basis for processing, OPOL will ensure that systems are set up that allow OPOL to:

7.4.1. demonstrate that a Data Subject has consented to processing of their personal data, via documenting the date, method and content of the disclosures made.

7.4.2. demonstrate that OPOL's requests for consent are presented in a manner which is clearly distinguishable from any other matters, is made in an intelligible and easily accessible form, and uses clear and plain language.

7.5. To ensure that OPOL's processing is compliant with the Applicable Data Protection Law, Personal and Special Category Personal Data will not be retained by OPOL for longer than necessary in relation to the purposes for which it was originally collected, or for which it was further processed.

Maintenance of Data Quality

7.6. OPOL recognises the importance of keeping data up to date and accurate at all times. All employees are required to ensure that the Data they are processing is accurate, free from errors and updated as and when required or where expressly requested by the Data Subject.

Automated Processing

7.7. OPOL will only engage in automatic processing activities, including profiling, where:

7.7.1. it is necessary for entering into, or performance of, a contract between the Data Subject and a Data Controller;

7.7.2. it is authorised by Union or Member State law to which the Data Controller is subject and which also lays down suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests; or

7.7.3. it is based on the Data Subject's explicit consent.

7.8. In relation to such processing, OPOL shall implement suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the Data Controller, to express his or her point of view and to contest the decision.

Retention and Destruction

7.9. The storage, retention and destruction of Personal and Special Category Personal Data is governed by a separate, specific policy, as set out in Appendix 1 below.

8. Subject Rights

8.1. OPOL will respect the rights of Data Subjects as provided for in Chapter 3 of the General Data Protection Regulation, and Article 8 of the EU Charter of Fundamental Rights.

8.2. This is governed by a separate, specific policy, as outlined in Appendix 1, which deals, in particular, with the suite of rights provided for by the General Data Protection Regulation.

9. Incident Management

9.1. OPOL is responsible for the creation and maintenance of an Incident Management Plan detailing what steps must be taken in the event of a Data Incident taking place within OPOL.

9.2. The majority of Data Incidents shall be handled by the MD, in cooperation with OPOL's managers, the Charles Taylor group, acting as "joint-controller" with OPOL. Where an incident is particularly serious or may require notification to either the Regulator or to the Data Subject, the MD must notify OPOL's board of directors without delay.

9.3. All involvement with the Regulator shall be undertaken by the MD.

9.4. The MD will maintain a register of all Data Incidents that have taken place within OPOL. Metrics relating to Data Incidents shall be reported to OPOL's board of directors on a regular basis.

9.5. The MD is responsible for arranging periodic testing of OPOL's Incident Management Plan and proposing any amendments to the plan from time to time.

10. Data Transfer

10.1. Where possible, OPOL shall rely on adequacy decisions made by the European Commission to legitimise transfers to third parties in other jurisdictions. Notwithstanding the reliance on adequacy decisions, OPOL shall still enter into Data Processing or Data Sharing Agreements in relation to the passage of Personal Data.

10.2. Where it is not possible to rely on an adequacy decision, the MD is responsible for ensuring that, in the event data is, or may be, transferred to another jurisdiction, any processing or sharing agreement shall be approved by the board of directors of OPOL.

10.3. The MD shall retain records of transfer activity that is taking place within OPOL or by or to OPOL.

11. Security

11.1. OPOL will adopt physical, technical, and organisational measures to ensure the appropriate security of processing in relation to Personal Data, and that unauthorised or unlawful processing does not occur. Please find below a non-exhaustive list of security measures:

11.1.1. ensuring the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

11.1.2. restoring the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and

11.1.3. implementing a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

11.2. In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Personal Data transmitted, stored or otherwise processed.

12. Third Party Risk

Data Processing and Sharing Agreements

12.1. Wherever Personal Data is shared with third parties or provided to third parties for processing, this shall occur in accordance with terms provided in either a Data Processing Agreement or a Data Sharing Agreement.

12.2. The MD retains a record of all Processing and Sharing Agreements that are in force.

13. Complying with Law Enforcement

13.1. In certain circumstances, OPOL is able to share a Data Subject's Personal Data without the knowledge or consent of the Data Subject, in particular where:

13.1.1. The disclosure is required by law.

13.1.2. The disclosure is required in order to assist in the prevention or detection of crime.

13.1.3. The disclosure is required in order to assist in the apprehension or prosecution of offenders.

13.1.4. The disclosure is required in order to assist in the assessment or collection of any tax or duty or of any imposition of a similar nature.

13.2. Any processing of Personal Data relating to criminal convictions and offences or related security measures shall be carried out only under the control of official authority or when the processing is authorised by Union or Member State law providing for appropriate safeguards for the rights and freedoms of Data Subjects.

14. Audit and Review

14.1. The MD shall engage in ad hoc assessments of compliance with this Policy and the policies sitting under it from time to time to ensure that best practice is being maintained and that employees, managers, agents and contractors are complying with their obligations in relation to data privacy. Details of ad hoc assessments that have been conducted are reported to OPOL's board of directors on a periodic basis.

14.2. This Policy shall be periodically reviewed on an annual basis. Earlier review or amendment may take place in the event of changes to Regulation or Legislation or following any incident.

Appendix 1

1. OPOL Data Retention Policy

2. OPOL Subject Rights Policy

3. OPOL Data Incident Management Plan