OPOL SUBJECT RIGHTS POLICY

as at 25 May 2018

1. Introduction, Aims and Scope

1.1. The Offshore Pollution Liability Association Ltd ("OPOL") is committed to ensuring that Data Subjects are able to vindicate their rights, as provided for by Chapter 3 of the General Data Protection Regulation, and Article 8 of the EU Charter of Fundamental Rights.

1.2. This policy (the "Policy") sets out OPOL's policy on respecting the rights of Data Subjects, and outlines an agreed set of standards by which OPOL, our employees, managers, agents and third parties contracting with OPOL, respond to requests by aforementioned Data Subjects.

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 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 Personal Data or when Personal Data is processed on behalf of OPOL in the United Kingdom or elsewhere within the European Union.

1.5. Where data are used for statistical or analytical purposes, provided that the Data are subject to procedures to prevent that data being tracked back to an individual Data Subject, the continued retention and processing of that data is outside of the scope of this Policy. For clarity, appropriate procedures would include minimisation, anonymization, pseudonymisation and aggregation in such a way as to no longer permit the identification of Data Subjects.

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 13 of this Policy.

2. Definitions

2.1. The Policy, unless indicated otherwise, adopts the definitions contained in the General Data Protection Regulation and in the OPOL Data Privacy Policy.

3. Our responsibilities and obligations under the Applicable Data Protection Law in relation to Subject Rights

3.1. The General Data Protection Regulation provides a variety of rights to Data Subjects in Chapter III of the Regulation, Articles 12 to 23. In particular, the General Data Protection Regulation provides the following rights:

3.1.1. **The right to information**: affording the Data Subject the right to obtain certain information from a data controller, in particular:

3.1.1.1. Where Personal Data relating to a Data Subject have been collected from the Data Subject, the Data Controller shall, at the time when Personal Data are obtained, provide the Data Subject with the information outlined in Article 13(1) and 13(2) of the GDPR

3.1.1.2. Where Personal Data relating to a Data Subject have not been obtained from the Data Subject, the Data Controller shall provide the Data Subject with the information outlined in Article 14(1) and 14(2) of the GDPR.

3.1.2. **The right to access**: affording the Data Subject the right to obtain from the Data Controller confirmation as to whether or not Personal Data concerning him or her are being processed, and, where that is the case, access to the Personal Data and the information outlined in Article 15 of the General Data Protection Regulation.

3.1.3. **The right to rectification**: affording the Data Subject the right to obtain from the Data Controller without undue delay the rectification of inaccurate Personal Data concerning him or her.

3.1.4. **The right to erasure**: affording the Data Subject the right to obtain from the Data Controller the erasure of Personal Data concerning him or her without undue delay and the Data Controller shall have the obligation to erase Personal Data without undue delay, where one of the grounds outlined in Article 17 of the General Data Protection Regulation apply.

3.1.5. **The right to restriction of processing**: affording the Data Subject the right to obtain from the Data Controller restriction of processing where one of the grounds outlined in Article 18 of the General Data Protection Regulation apply.

3.1.6. **The right to data portability**: affording the Data Subject the right to receive the Personal Data concerning them, which they have provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the Data Controller to which the Personal Data have been

provided, where the grounds outlined in Article 19 of the General Data Protection Regulation apply.

3.1.7. **The right to object**: affording the Data Subject the right to object, on grounds relating to his or her particular situation, including profiling based on those provisions.

3.2. Generally, where a request to exercise any of these rights is made by a Data Subject, that request must be responded to within one month. Any request to exercise these rights must be made in writing (either electronic or hard copy) and must provide sufficient information and evidence to enable the Data Subject to be identified.

3.3. Where there is any concern as to the identity of the Data Subject, evidence of identity may be requested from the Data Subject. The one-month limit for provision of a response to the request does not start until such time as the Data Controller is satisfied of the identity of the Data Subject.

3.4. The Data Controller is entitled to extend the period for response to the request by up to two months over and above the initial month where necessary due to the complexity of the request. Where an extension is to be relied upon, the Data Subject must be advised of the extension within one month of the receipt of the request, accompanied by details of the reason for the delay.

3.5. The Data Controller may not charge any fee from the Data Subject in connection with the exercise of her rights unless the provisions of Paragraph 3.6 below apply.

3.6. Where the Data Subject makes either excessive or unfounded requests to exercise their rights, the Data Controller may either:

3.6.1. Charge the Data Subject a reasonable fee to cover the administration costs of responding to the request; or

3.6.2. Refuse to act on the request.

3.7. It is the responsibility of the Data Controller to demonstrate why and how the request is either unfounded or excessive in nature.

3.8. Where a request to exercise a right is received electronically, it should normally be responded to electronically unless this is unachievable.

3.9. The United Kingdom Draft Data Protection Bill 2017 makes it a criminal offence to alter, deface, block, erase or conceal any Personal Data with the intention of preventing the disclosure of that information to the Data Subject. Both the Data Controller and any employee or representative of the Data Controller personally

can be convicted of this offence. It is therefore essential that data is not wilfully or intentionally.

3.10. Internally, this Policy should be read in conjunction with those documents identified in Paragraph 13.

4. Right to information

4.1. At any point where Personal Data is collected from a Data Subject by or on behalf of OPOL, OPOL must provide the following information:

4.1.1. The identity and contact details of the Data Controller and any representative (including, OPOL's managers, the Charles Taylor group, acting as "joint controllers" with OPOL);

4.1.2. The purposes and legal basis of the processing of the data;

4.1.3. If OPOL is relying on legitimate interests as it's reason for processing, details of what those legitimate interests are:

4.1.4. The recipients (or categories of recipient) of the data (including where any Data is transferred, shared or processed by any other part of OPOL);

4.1.5. Details of what safeguards are in place in the event that the data is to be transferred to any third country outside the EEA;

4.1.6. The period the data will be retained for (or the criteria used to calculate that period);

4.1.7. Details of the Data Subject's rights in relation to the data (specifically the right to access, rectify, have erased, restrict or object to processing and portability where these rights apply);

4.1.8. Where the legal basis for processing is based on consent, advice to the effect that the Data Subject has the right to withdraw that consent at any time;

4.1.9. The right to lodge a complaint with a supervisory authority (in most cases, the Information Commissioners' Office (known as the 'ICO'));

4.1.10. Whether the provision of the data is a statutory or contractual requirement and, if so, what the consequences of failure to provide the data are; and

4.1.11. Where automated decision making or profiling are engaged, details of the logic used by the processing and what the consequences of the processing are for the Data Subject.

4.2. This information is provided within the Privacy Notice which is accessible on the OPOL website. There is no requirement to provide the Privacy Notice itself at the point of collection provided that the Data Subject is given a link or an address where the Privacy Notice can be viewed.

4.3. Where data is to be obtained during the course of a telephone conversation, it is recommended (as well as providing the address at which the caller can access the Privacy Notice) that a recorded version of the Privacy Notice is made available to the Data Subject as a selectable option.

4.4. Where the Data Subject is not personally providing the data but it is coming from a third party, the information detailed in Paragraph 4.1 above must be provided within a reasonable period of receipt of the data and, in any event, within one month of having received the data. Again, this requirement may be met by providing a link to the address where the Privacy Notice can be viewed.

5. Right to Access

5.1. Where OPOL (or any other entity on OPOL's behalf) is processing data in relation to a Data Subject, that Data Subject has the right to access the data that is being processed. At the time the data is provided to the Data Subject, OPOL must also provide:

5.1.1. Details of the purposes for which the data is being processed;

5.1.2. Details of what categories of Personal Data are being processed;

5.1.3. Details of the recipients of any Personal Data (whether the Data has already been provided to the recipient or even where it is only intended that Data will be supplied or disclosed to any third parties);

5.1.4. Details of the period for which the data will be retained;

5.1.5. The existence of the Data Subjects right to request rectification or erasure of the data or to restrict or object to the continued processing of the data;

5.1.6. The existence of the right to lodge a complaint with the relevant supervisory authority;

5.1.7. Where the data has not been collected from the Data Subject, details of the source of the data; and

5.1.8. Where automated decision making or profiling are engaged, details of the logic used by the processing and what the consequences of the processing are for the Data Subject;

5.2. This information can be supplied in a covering letter that accompanies the data at the point it is provided to the data.

5.3. As a minimum, OPOL expects the following to take place upon receipt of a Subject Access Request:

5.3.1. Within 1 business day of the Access Request having been received by or on behalf of OPOL, the MD must be made aware of the request.

5.3.2. Within 3 days of the Access Request having been received, the MD has acknowledged receipt of the Access Request. Where necessary, this acknowledgement has been accompanied by appropriate questions to attempt to limit the scope of the Access Request and, where appropriate, has evidence to confirm the identity of the Data Subject. Where the Subject Access Request is a repeated request or where the scope of the request is unfeasibly large, leading the MD to believe that it is not reasonable to comply with the Subject Access Request at all, OPOL's board of directors must be consulted immediately, prior to the acknowledgement being sent.

5.3.3. Within 5 business days of the Access Request having been received, the MD has requested copies of relevant data held by the appropriate staff members of OPOL and of its managers, the Charles Taylor group

5.3.4. The request must be accompanied by a deadline for response no more than 20 days following receipt of the Access Request for return of the data. In the event that there is a genuine belief that it will not be possible to return the data to the MD within 20 days, the MD must be notified immediately. The MD must then notify the Data Subject that an extension of time to comply with the Request will be required and must give reasons for the extension. The notification to the Data Subject must provide a date by which the Subject Access Request will be responded to.

5.3.5. Upon receipt of the data, the MD must review the data to ensure that there is nothing that should be redacted prior to the data being sent out. Company confidential material, material that is not strictly Personal Data and any material data that identifies third parties should be redacted as a matter of course. Care must be taken when redacting data (particularly where the redaction is being undertaken electronically) to ensure that it is not possible to "resurrect" the redacted data once it has been passed to the Data Subject.

5.3.6. No later than 26 days following receipt of a Subject Access Request, the MD must send a copy of the data, accompanied by a document fulfilling the requirements of Paragraph 5.1 above to the Data Subject either electronically (if the request was received electronically) or by post. An electronic copy of all information sent as part of a Subject Access Request must be retained on the appropriate system.

6. Right to Rectification

6.1. Where a Data Subject establishes that data held by the Data Controller is either inaccurate or incomplete, the Data Controller must either rectify or complete the data record within a reasonable period.

6.2. As a minimum, OPOL's expectation is that legitimate requests to rectify data will be completed within 5 business days of receipt. Where the data has been provided by a third-party Data Controller, good practice dictates that OPOL should notify the Data Controller of the request to have data rectified.

7. Right to Erasure

7.1. Any Data Subject has the right to ask a Data Controller to delete Personal Data held in relation to him or her under the following circumstances:

7.1.1. The Personal Data is no longer required for the purposes for which it was obtained/processed;

7.1.2. The Data Subject has withdrawn their consent to process the Personal Data where there is no other lawful basis under which the data is being processed;

7.1.3. The Data Subject objects to the processing and there are no overriding legitimate reasons for continuing to process the data; or

7.1.4. The data has been unlawfully processed;

7.2. The Data Controller is not required to honour the request to delete Personal Data in the following circumstances:

7.2.1. The data is being processed in order to enable the Data Controller to comply with a legal obligation for which the Data Controller is required to continue to process the data;

7.2.2. The Data Controller is processing the data pursuant to a task carried out in the public interest;

7.2.3. The Data Controller requires the Personal Data for the establishment, exercise or defence of any legal claim.

7.3. In the event that the Data Controller determines it is not required to delete the data for one of the reasons expressed in Paragraph 7.2 above, the Data

Controller must advise the Data Subject of that refusal, with reasons, within one month of receipt of the request.

7.4. As a minimum, OPOL expects the following in the event of a request to erase data:

7.4.1. Within 3 business days of receipt of the request to erase data, the MD must be notified that a request has been received.

7.4.2. Within 7 days of receipt of the request to erase data, the MD has considered the request and determined whether the requirements of Paragraph 7.1 above have been met and whether any of the exemptions provided in Paragraph 7.2 above apply.

7.4.3. No later than 21 days following receipt of the request to erase data, the MD has provided confirmation to the Data Subject that request has been complied with or refused accompanied with the reasons for such refusal.

8. Right to Restriction of Processing

8.1. Any Data Subject has the right to request that processing of their Personal Data is restricted in the following circumstances:

8.1.1. Where the accuracy of the Personal Data is contested by the Data Subject;

8.1.2. Where the processing of the Personal Data is unlawful but the Data Subject does not wish their data to be erased;

8.1.3. Where the Data Controller no longer requires the data for the purposes for which it was obtained, but the data is retained for the establishment, exercise of or defence of legal claims; or

8.1.4. Where the Data Subject is challenging the assertion that the legitimate interests of the Data Controller in processing the data outweigh the legitimate interests of the Data Subject.

8.2. Where a request to restrict processing is made by a Data Subject, the Data Controller may continue to store the data but must not undertake any other processing activity with the data without the explicit consent of the Data Subject unless that further processing is undertaken for the establishment, exercise of or defence of legal claims.

8.3. Where processing activities are restricted, prior to the restriction being lifted (for example, where any accuracy issues are corrected or where a legitimate interests challenge is resolved) the Data Controller must notify the Data Subject of the intention to lift the restriction. This notification need not be in writing

provided that it can be demonstrated that the Data Subject was given prior notification.

8.4. As a minimum, OPOL has the same expectations as in Paragraph 7.4 with respect to responding to a request to restrict processing.

9. Right to Portability

9.1. Where data is provided by the Data Subject to the Data Controller, the Data Subject has the right to receive that data in a structured, commonly used and machine-readable format and has the right to have that data sent to another Data Controller without hindrance. This right applies **only** where:

9.1.1. The processing of the data is undertaken in accordance with consent provided by the Data Subject or pursuant to a contract to which the Data Subject is a party; and

9.1.2. The processing of the data is carried out by automated means.

10. Right to Object

10.1. Where processing activity is undertaken, the Data Subject has the right to object to continued processing of the data.

10.2. In the event a Right to Object is exercised by the Data Subject, the Data Controller must not further process the data unless it can demonstrate that the legitimate interests of the Data Controller in continued processing outweigh the legitimate interests of the Data Subject or where the processing is necessary for the establishment, exercise of or defence of legal claims. Until the Data Controller can so demonstrate, the Data Controller must not further process any data concerning the Data Subject.

10.3. Where data is processed and a decision made regarding the Data Subject that is based solely on automated means (i.e. without any human involvement or consideration) the Data Subject has the right to object to such a decision unless:

10.3.1. The decision is necessary for the purposes of entering into or performance of a contract between the Data Subject and the Data Controller; or

10.3.2. The automated processing is based on the Data Subject's explicit consent.

10.4. Where a Data Subject objects to any form of automated processing, the Data Controller must provide a means for the decision to be reviewed by a human being and a means to have the representations of the Data Subject taken into account.

11. Satisfying Data Subject Rights

11.1. Wherever a request to exercise a Data Subject's rights is received by or on behalf of OPOL, details of the request must be passed without delay to the MD for that request to be recorded and compliance with the statutory timescale monitored.

11.2. When a request is received for access to Personal Data, appropriate searches will need to be carried out in both electronic and hard copy filings systems of OPOL. This search should include:

11.2.1. Live systems;

11.2.2. Shared Drive folders;

11.2.3. Exchange folders; and

11.2.4. Archive folders.

11.3. It is reasonable, in the case of a Subject Access Request to liaise with the Data Subject to try to limit the scope of the search for data to specific topics, subject areas or periods. However, it is the right of the Data Subject to have access to all their data held by the Data Controller and the Data Controller may not insist on limiting the scope of the search. This would include opinions that have been recorded about a Data Subject as well as purely factual information.

11.4. When responding to a Subject Access request, care must be taken to ensure that the rights of any third parties are not violated by responding to the request. It is therefore necessary to ensure that any Personal Data relating to someone other than the Data Subject that is contained within the information that is to be released to the Data Subject is deleted prior to the information being provided. This is known as redaction. In a similar vein, commercially sensitive information must be redacted prior to the information being released to the Data Subject. When redacting documents, care must be taken to ensure that the information that has been redacted is not capable of being restored by the Data Subject – this is particularly relevant when releasing documents electronically, although also consider whether a Data Subject can read redacted wording on hard copy documents by lighting the document from behind.

11.5. It is good practice to retain a copy of the information provided to the Data Subject (along with the covering letter as detailed above) in the event that there is a need to refer to the released Data downtime. It should be remembered that, particularly in the case of Subject Access, a request for release of information is often a precursor to other "action" such as litigation, grievance or complaint. This does not provide a reason to refuse to release information requested by a Data Subject.

12. Audit and Review

12.1. A timely response to Data Subject rights issues are a matter of interest to OPOL's board of directors as they present both a resourcing issue but also carry a significant financial penalty in the event that they are not properly undertaken. Therefore, all data subject rights requests must be brought to the attention of the MD to enable metrics to be monitored and reported. The following fields must be provided in all instances:

12.1.1. Date of receipt of Rights request.

12.1.2. Nature of Rights request (e.g. Access, Erasure, Amendment etc).

12.1.3. Due date for completion of Rights request.

12.1.4. Actual date of completion of Rights request.

12.1.5. Date extension brought to the attention of Data Subject (if applicable).

12.1.6. If Rights request refused, date of refusal and reason for refusal.

12.2. As part of its continuing data privacy and accountability requirements, OPOL shall complete an annual review of data privacy arrangements and the MD shall be required to respond to the following (with evidence):

12.2.1. *Have you reviewed the Privacy Notice for alignment with legal requirements and confirmed that the description of data processing activities is accurate and complete?*

12.2.2. *Do you routinely review all subject access requests to ensure that data is provided in accordance with this Policy.*

12.2.3. *Do you routinely review all requests to be forgotten or have data erased?*

12.3. As part of its continuing data privacy and accountability requirements, OPOL shall complete an annual review of data privacy arrangements.

12.4. This Policy shall be periodically reviewed on an annual basis. Earlier review or amendment may take place in the event of changes to Regulation, Legislation, working practices or following any Personal Data Incident.

13. Linked Policies

13.1. This Policy should be read in conjunction with the following internal policy documents:

13.1.1. OPOL Data Privacy Policy

13.1.2. OPOL Data Retention Policy

13.1.3. OPOL Data Incident Management Plan