OPOL DATA INCIDENT MANAGEMENT PLAN
as at 25 May 2018

1.1. This data incident management plan ("Plan") applies to The Offshore Pollution Liability Association Limited ("OPOL").

1.2. OPOL is committed to conducting its businesses in a manner that protects and values each individual's personal data, and processes said personal data fairly, lawfully, and ethically.

1.3. This Plan sets out the way in which OPOL (and its managers, Charles Taylor Insurance Services Limited) 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. "Data Incident" means any event, occurrence or happening whereby it appears to an employee, manager, agent or contractor of OPOL that there are objective grounds to suspect a Data Breach, or where any such suspicions are reported to the Privacy Office.

1.4. This Plan is part of OPOL's framework governing the processing of personal data by or on behalf OPOL. The other data privacy documentation applicable within OPOL is as follows:

1.4.1. OPOL Data Privacy Policy;
1.4.2. OPOL Data Retention Policy; and
1.4.3. OPOL Subject Rights Policy;

1.5. The aim of these policies is to support the management of data protection within OPOL by providing this agreed set of standards. All of OPOL's employees, managers, agents and contractors must familiarise themselves with the processes and procedures set out herein and comply with them at all times.

Definitions

1.6. This Plan, unless indicated otherwise below, adopts the definitions contained in Article 4 GDPR and in the OPOL Data Privacy Policy.

2. The Principles underpinning this Plan

2.1. It is integral to information security that there are simple processes for capturing and monitoring all events and occurrences which might suggest unauthorised processing of personal data. All staff must have the ability to easily report such instances.

2.2. All reports of Data Incidents shall be reviewed by the MD and all that require notification to third parties (including the Information Commissioner's Office and/or to Data Subjects) shall be reviewed by OPOL's board of directors.

2.3. No person working for (or processing on behalf of) OPOL, whether staff, or manager, agents or contractors, shall process personal data except on the general or specific instructions of OPOL acting as data controller, unless required by law. OPOL shall take such steps as are necessary to ensure the integrity of all OPOL employees, managers, agents and contractors insofar as they have access to personal data processed by or on behalf of OPOL.

3. General Process in Outline

3.1. There are 5 stages to the process for assessing & responding to Data Incidents:

3.1.1. Report or capture of the Data Incident;
3.1.2. Initial triage;
3.1.3. Identification and Notification of data controllers;
3.1.4. Investigation of Data Incident;
3.1.5. Notification of Data Subjects and/or the Information Commissioner.

3.2. STAGE 1: Report or capture of Data Incidents

3.2.1. OPOL (and its managers) shall ensure that any of their staff, whether employees

or contractors:

3.2.1.1. Shall be trained in the importance of reporting any and all Data Incidents, irrespective of seriousness;

3.2.1.2. Have access to a Data Incident Form, a template for which is provided at **Appendix A** to this Plan.

3.2.2. Reports of a Data Incident, whether as a result of an employee reporting through a standard form or otherwise, shall be sent to an email account operated by the MD. All staff shall have access to the MD's contact details for the purposes of reporting such incidents.

3.2.3. It is the obligation of every staff member, whether employee or contractor of OPOL and/or its managers, to report any Data Incident to the MD immediately, and in any event within 2 hours of encountering it. Details which must be reported shall include:

3.2.3.1. The date and time of the report;

3.2.3.2. The date and time that the Data Incident was discovered, or that a reasonable suspicion arose that a Data Incident had occurred;

3.2.3.3. If known, the date and time that the Data Incident (first) occurred;

3.2.3.4. The nature of the Data Incident;

3.2.3.5. Whether there are grounds to believe that the Data Incident may have resulted by reason of a person acting maliciously;

3.2.3.6. The nature of the Personal Data potentially affected in the Data Incident;

3.2.3.7. Whether the Data Incident includes Special Category Personal Data;

3.2.3.8. The number of Data Subjects known and/or suspected to be affected; and

3.2.3.9. Any other information that might assist investigation of the Data Incident.

3.2.4. OPOL, in cooperation with its managers, shall keep a complete register of all Data Incident reports, and shall review the register with the MD at least quarterly with a view to maintaining a taxonomy of Data Incidents for reporting purposes.

3.2.5. In the event that a Data Incident is reported to OPOL or its managers from an external source, the staff-member first alerted by that external source shall be under an obligation to file a Data Incident report.

3.3. STAGE 2: Initial Triage

3.3.1. Within 24 hours of receiving a Data Incident report, the MD shall determine to which of the following three categories it should be allocated:

3.3.1.1. A Data Incident likely to be a Data Breach necessitating notification to either the Information Commissioner's Office ("ICO") or to the Data Subject(s) affected by the Data Breach ("a Tier 3 Incident"). Any Data Incident which arises out of unauthorised external access to the manager's computer systems, or unauthorised processing of the personal data of multiple Data Subjects will usually be considered a Tier 3 Incident until proven otherwise;

3.3.1.2. A Data Incident which, if a Data Breach, would not require notification to the ICO or to the Data Subject(s) affected, but which nonetheless requires notification to contractual counterparties, including those who are Data Controllers ("a Tier 2 Incident");

3.3.1.3. A Data Incident which is either unlikely to be a Data Breach, or if it were a Data Breach would not require notification, whether to the ICO or Data Subject(s) affected, or contractual counterparties (other than the data co-controller in respect of that personal data) and which need only be investigated internally ("a Tier 1 Incident").

3.4. STAGE 3: Identification & Notification of the Data Controllers

3.4.1. Within 24 hours of receiving a Data Incident report, the MD shall identify if there are other relevant Data Controllers (if any) in respect of the affected Personal Data, (e.g. parties to the OPOL Agreement).

3.4.2. Any data co-controllers directly affected by a Tier 1 or Tier 2 or Tier 3 Data

Incident shall be notified by the MD in writing pursuant to the contractual arrangement between them and OPOL and Article 33(2) GDPR, but in any event no later than 48 hours from the Data Incident having been reported. Such notification shall, at the minimum, provide:

3.4.2.1. The nature of the suspected personal data breach, including the categories of personal data affected, and the approximate number of Data Subjects and personal data records which are involved;

3.4.2.2. The likely consequences of the suspected data breach;

3.4.2.3. The measures taken or proposed to be taken by OPOL and by the data controller, including acts to mitigate the suspected data breach; and

3.4.2.4. The name and contact details of the MD.

3.4.3. Such other data co-controllers, who are not directly affected by the Data Incident, may also be notified of Tier 2 and Tier 3 Data Incidents at the same time insofar as their contractual arrangements with OPOL require it.

3.5. STAGE 4: Investigation of the Data Incident

3.5.1. The MD may delegate investigation of Tier 1 Incidents to the managers, but shall report to the OPOL's board of directors immediately if upon investigation, a Tier 1 Incident requires reallocation to a Tier 2 or Tier 3 Incident.

3.5.2. The MD shall investigate a Tier 2 Incident, in liaison with the managers, and shall report to OPOL's board of directors immediately if upon investigation, a Tier 2 Incident requires reallocation to Tier 3.

3.5.3. The MD shall investigate a Tier 3 Incident personally, in liaison with the appropriate information security staff under the supervision of the Chief Information Security Officer at Charles Taylor Insuretec Limited.

3.5.4. The Investigation shall be proportionate to the anticipated seriousness of the Data Incident, and shall at the earliest possible opportunity, but (in the case of a Tier 2 or Tier 3 incident) in any event within 72 hours:

3.5.4.1. Identify whether the Data Incident is in fact a Data Breach;

3.5.4.2. Identify how many Data Subjects are affected, and the nature of the Personal Data (including Special Category Personal Data) involved;

3.5.4.3. Take all reasonable steps to prevent further unauthorised processing;

3.5.4.4. Prepare a report to present to the board of directors of OPOL.

3.5.5. All Investigations and their outcomes shall be recorded on the Data Incident register kept by the MD.

4. STAGE 5: Notification of Data Subjects and/or the Information Commissioner

4.1. If a Tier 3 or Tier 2 Data Incident is, after Investigation, confirmed as a Data Breach, the MD shall be responsible for:

.

4.1.1. notifying the managers, as joint Data Controllers, so that they can indicate whether they or OPOL shall notify the ICO or any other relevant supervisory authority under Article 33(1) GDPR.

4.2. When OPOL is required to notify the ICO, the required notification shall include at a minimum:

4.2.1. A description of the nature of the personal data breach, including the categories and approximate number of Data Subjects concerned and the number of personal data records affected;

4.2.2. The name and contact details of the MD and the managers;

4.2.3. The likely consequences of the Personal Data Breach;

4.2.4. The measures taken or proposed to be taken by OPOL, its managers, and/or any other Data Controller, in response to the Data Breach, including any acts of mitigation.

4.3. The MD shall be responsible for notifying any Data Subject affected by a Data Breach, according to the criteria in Article 34 GDPR, unless notification of the Data Subject is exempted in the particular case pursuant to Article 23(1) GDPR, and a provision of Applicable Data Protection Law. If non-notification of the Data Subject is justified under this paragraph, then a specific written record of such justification shall be made by the

MD, and appended to the relevant Data Incident record in the relevant register of Data Incidents.

5. Audit and Review

5.1. On a quarterly basis, or more often, the MD in co-operation with the managers, shall conduct an audit of the Data Incident Register and the investigations and Data Breaches recorded therein, with a view to making recommendations that will ensure OPOL's continued compliance with the security requirements of GDPR and other Applicable Data Protection Law.

5.2. The Audit conducted by the MD, in cooperation with the managers shall consider at a minimum:

5.2.1. a sample of 20 Tier 1 Incidents, or if fewer than 20 then all Tier 1 incidents;

5.2.2. all Tier 2 and Tier 3 Incidents and resulting investigations.

5.3. This Plan shall be periodically revised on an annual basis. Earlier review or amendment may take place in the event of changes to Regulation or Legislation or following a Data Incident.

Appendix A: Data Incident Reporting Form

YOUR DETAILS

Name:

Job title:

Direct Line:

Work Mobile:

Email:

Line Manager name:

Line Manager direct line:

Line Manager email:

DATA INCIDENT DETAILS

Data Breach means: "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed*."

Data Incident means: "*any event, occurrence or happening whereby it appears to an employee, manager, agent or contractor of OPOL that there are objective grounds to suspect a Data Breach, or where any such suspicions are reported to the Privacy Office.*"

When did <u>you discover</u> (or first suspect) that a Data Incident had occurred?	Day: Date: Time (approximately):
If earlier, when did you think the Data Incident <u>first occurred</u>?	Day: Date: Time (approximately):

Please describe the Data Incident in your own words, giving as much detail as possible.	
Please describe how you became aware of the incident, including the names and contact details of anyone who brought it to your attention?	

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*."

Do you suspect that the Data Incident involves Personal Data?	Yes ☐ No ☐
What <u>types</u> of Personal Data do you think may be involved? Please tick as many as are appropriate.	Names: ☐ Contact Details: ☐ Dates of Birth: ☐ Policy details: ☐ Documents: ☐ Emails/Correspondence: ☐ Financial information: ☐ Other (please describe in your own words): ☐ _____ _____ _____

Special Category Data means: "*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.*."

Does any of the Personal Data you think may be involved include Special Category Personal Data?	Health: ☐ Genetic and biometric: ☐ Racial or ethic origin: ☐ Sex or sexual orientation: ☐ Political, religious, trade union: ☐
How many individuals' Personal Data do you think might have been affected by this Data Incident?	
Do you have any other information that might assist investigation of the Data Incident?	
	Name: Signature: Date of report: Time of report:

Please send this form immediately to admin@opol.co.uk