OPOL DATA RETENTION POLICY

as at 25 May 2018

1. Introduction, Aims and Scope

Introduction and aims

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 that personal data fairly, lawfully, and ethically. This includes not only the obtaining and use of such personal data, but also the retention of such personal data for no longer than is necessary.

1.2. This policy (the "Policy") sets out policy for OPOL on data retention, 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 should familiarise themselves with the processes and procedures set out herein and comply with them at all times. All employment contracts will, from 25 May 2018 if not before, include binding contractual terms requiring employees to follow this Policy and the other specific data protection policies cited in this document.

1.4. 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.

1.5. For operational purposes, there may be occasions where exceptions to, or deviations from, this Policy are required. Where this in necessary and justified, these must be justified by reference to specific policies.

Scope

1.6. This Policy applies to when OPOL (or any other person on its behalf) process personal data in the United Kingdom or elsewhere within the European Union.

1.7. This Policy applies to data contained in both electronic and hard copy records held by OPOL, provided such records are held in an organised filing system. For

the avoidance of doubt, this includes all electronic copy records held by or on behalf of OPOL.

1.8. Where personal data are used for statistical or analytical purposes, provided that the personal 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.

2. Definitions

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

2.1.1. **Filing system** means "*any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.*"

2.1.2. **Archiving** means the removal of data from active systems and placing the data into secure storage (whether hard copy or electronic) where the data is still capable of being accessed by arrangement.

3. Regulatory Framework

3.1. The GDPR provides that data shall be kept in a form which permits the identification of Data Subjects for no longer than is necessary for the purposes for which the data are processed (Art. 5(1)(e)).

3.2. Recital 65 expands on the Article by making it clear that a Data Subject should have the right to have his or her data erased and no longer processed where the data are no longer necessary in relation to the purposes for which they were collected, where consent to process is withdrawn or where the processing does not otherwise comply with the GDPR.

3.3. The recital provides an exemption enabling the continued lawful retention of data where necessary to comply with legal and regulatory obligations or for the establishment, exercise or defence of legal claims.

3.4. The starting point therefore for any data retention policy is that data should be destroyed as soon as the reason for processing that data has come to an end. In the normal course of business this would be the conclusion of a contract or ending of any ongoing legal relationship between OPOL and the Data Subject.

3.5. The exemption referred to in Rec. 65 provides that data can be retained to protect OPOL against legal claims brought against it once the legal relationship between the Subject and OPOL has come to an end. Time limits for claimants to

bring legal action against OPOL are prescribed (in the United Kingdom) by the Limitation Act 1980 which provides that, for actions founded on either tort or contract, such action shall not be brought after the expiration of six years from the date on which the cause of action accrued. Where actions are founded on deed, the action shall not be brought after the expiration of a period of 12 years from the date on which the cause of action accrued.

3.6. Exemptions to the general limitation provisions exist where a case is brought on behalf of a minor where the limitation period will not begin to run until the minor has reached their 18th birthday. Exemptions also exist in the case of claimants who are affected by a relevant disability.

3.7. Any subcontracting arrangement needs to be back to back with any Data Processing Agreements mentioned in Paragraph 3.8 if the subcontractor is dealing with any data relating to that agreement.

3.8. Where OPOL instructs a third-party Processor or outsources any processing activity to a third party Processor, those instructions must be governed by a Data Processing Agreement between OPOL and the Processor. Any Data Processing Agreement must contain provisions relating to retention and return/destruction of data that are in accordance with this Policy.

3.9. Internally, this Policy should be read in conjunction with those documents identified in Paragraph 9.

4. Electronic Retention

4.1. Any electronic document containing data must be saved to the appropriate file and stored on the recognised system within each division as soon as possible following receipt or creation. Documents containing data must not be retained in outlook folders, inboxes, sent items folders or personal drives.

4.2. Where, for legitimate business reasons, documents containing data are required to be locally accessible in environments where access to recognised networked systems is not possible, such documents may be temporarily saved to external media (USB sticks, external Hard Drives etc) subject to the following observations:

4.2.1. Data must not be transferred from any approved external device onto a secondary device at any time.

4.2.2. Wherever possible, principles of data minimisation should be adopted to ensure that the least amount of data necessary to complete the legitimate business function is stored on external media at any time.

4.2.3. As soon as the legitimate business reason for using an external media device has come to an end (for example, by returning to the office), any document containing data must be transferred to the recognised

networked system and permanently erased from the external media device.

4.2.4. Reasonable personal security measures must be taken in relation to external media devices that contain data. Specifically, devices should be retained on the person when not in use, must not be left connected when not in use, and must not be connected to personal equipment that has not been supplied by OPOL.

4.2.5. In the event an external media device containing data is stolen, lost or otherwise damaged, this must be raised with the MD. Loss of Data in this way may constitute a Personal Data Incident which may trigger onward notification to both the Data Subject and the Information Commissioners' Office.

4.3. At the termination of OPOL membership or at the conclusion of any matter (whether as a result of the expiry or termination of the contractual relationship or following the settlement of a claim whichever is the latter) all data relating thereto should be transferred from the recognised system into archive storage as detailed in Paragraph 6 below.

5. Hard Copy Retention

5.1. Wherever possible, OPOL should rely on electronic retention as opposed to hard copy retention. Quite apart from the security challenges posed by hard copy data, it is also significantly more difficult to ensure compliance with Data Subject rights when hard copy data is used. Where, for legitimate business reasons, hard copy retention is required, it must be undertaken in accordance with the remainder of this section.

5.2. Hard copy documents containing data must be stored in lockable filing cabinets when not actively in use. Filing cabinets must be located in secure environments where access is only permitted to employees of OPOL or managers, agents, contractors appointed on behalf of OPOL. Documents containing data must not be stored in personal drawer units or left on unattended desks. Filing cabinets must be kept locked outside of normal business hours and keys stored in a secure location.

5.3. Where there is no requirement to retain hard copy data (for example, where the data has been provided in both hard copy and electronic format, or where the data has been subsequently converted to an electronic format), hard copy data must be disposed of securely. Hard copy data must not be disposed of in general waste.

5.4. From time to time, there may be a legitimate business reason for hard copy data to be removed from the office. Due to the increased security risk posed by hard copy data, removal from the office is subject to the following observations:

5.4.1. Hard copy data must be retained on the person at all times. Under no circumstances should hard copy data be left overnight in a car or similar insecure environment.

5.4.2. Extra care must be taken when using hard copy data outside of the office. Consideration must be given to any factors that may cause a third party to have access to the data including (but not limited to) surroundings, proximity of third parties and lines of sight/hearing.

5.4.3. In the event hard copy data is lost, stolen or permanently damaged or defaced, the MD must be notified at the earliest possible opportunity. Loss of Data in this way may constitute a Personal Data Incident which may trigger onward notification to both the Data Subject and the Information Commissioners' Office.

5.5. At the conclusion of any matter (whether as a result of the expiry or termination of the contractual relationship or following the settlement of a claim whichever is the latter), where possible, all hard copy data in relation to that matter should be converted into electronic format prior to transfer to archive storage in accordance with Paragraph 6 below. Once converted into electronic format, all hard copy data should be securely destroyed in accordance with Paragraph 5.3 above. If it is necessary to retain hard copy data beyond the conclusion of any matter, this data must be retained in accordance with Paragraphs 6.3 to 6.7 below.

6. Archive Retention

Electronic Records – hosted by the Managers

6.1. OPOL is currently managed by the Charles Taylor group pursuant to a management agreement. The managers are considered as "joint controllers" under GDPR. The managers will comply with OPOL's specific archiving arrangements and when the Charles Taylor group ceases to act as managers of OPOL, the Charles Taylor group will return all data to OPOL and will securely delete any back-up copies held. OPOL will then retain the data in accordance with the provisions of Paragraphs 6.1 to 6.5.

6.2. Where Processing Agreements provide that the Data Processor shall retain archive records, these arrangements must be reflected in any notice provided to the Data Subject, accompanied by the identity of the Processor concerned, the type of data retained and details of contact arrangements should the Data Subject wish to exercise their rights against the Data Processor.

Hard Copy Records

6.3. Where there is a requirement to retain Hard Copy Records following the conclusion of a matter, these must be retained in a secure manner.

6.4. As a minimum, OPOL must retain a record of what Hard Copy data has been archived, where that data has been archived, when the data has been archived, when the data is scheduled for destruction and how the data can be retrieved in the event that this is necessary for a legitimate business purpose.

6.5. Prior to transferring any hard copy data to archive, OPOL must ensure that only that data which may be required at a later date for legitimate business purposes is transferred to archive. Excessive, unnecessary or duplicated data should be securely destroyed prior to archiving.

6.6. Unless expressly provided otherwise, all archived hard copy data must be securely destroyed on the destruction date provided in accordance with Paragraph 7 below.

7. Destruction

7.1. Destruction dates shall be calculated from the last action on a particular live matter, whether that be the termination of a contract, the conclusion of a claim or other specific action that results in the matter no longer being "live".

7.2. Where the matter is based on a contractual relationship, the destruction date shall be 7 years after the event referred to in Paragraph 7.1 above.

7.3. Where the matter is based on a Deed, the destruction date shall be 12 years after the event referred to in Paragraph 7.1 above.

7.4. In the event that a matter becomes "live" again following archive (for example, where a claim is filed against OPOL) and the archived Data is recovered, the original destruction date shall be disregarded. A new destruction date shall be set in accordance with Paragraphs 7.2 or 7.3 above relying on the date on which the reactivated matter ceases to be live.

8. Audit and Review

8.1. OPOL shall conduct ad-hoc audit of the implementation of this Policy.

8.2. 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):

8.2.1. *Do you maintain a data destruction policy that defines acceptable methods for the secure destruction of personal data regardless of whether that personal data is in an electronic or paper format?*

8.2.2. *Do you maintain a data retention policy which has been made available to all relevant parties?*

8.2.3. *Do you maintain or review data retention schedules stating how long personal data may be retained in line with relevant laws and regulations?*

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

8.4. 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.

9. Linked Policies and Policies

9.1. This Policy should be read in conjunction with the following internal policy documents (all documents are accessible through the Data Privacy Intranet site):

9.1.1. OPOL Data Privacy Policy.

9.1.2. OPOL Subject Rights Policy.

9.1.3. OPOL Data Incident Management Plan.