Proposed GDPR processing provisions to be included as part of the Special Conditions of Contract in the LOGIC General Conditions of Contract for Services (On & Off-Shore, Edition 3 – March 2014)

1.1 Insert the following new sub-clauses in Clause 1 (DEFINITIONS):

[1.18] “CONTROLLER” (or data controller), “PROCESSOR” (or data processor), “DATA SUBJECT”, “INTERNATIONAL ORGANISATION”, “PERSONAL DATA” and “PROCESSING” all have the meanings given to those terms in DP LAWS (and related terms such as “PROCESS” shall have corresponding meanings).

[1.19] “DATA SUBJECT REQUEST” means a request made by a DATA SUBJECT to exercise any rights of DATA SUBJECTS under DP LAWS.

[1.20] “DPIA” means a Data Protection Impact Assessment, as defined in DP LAWS.

[1.21] “DP LAWS” means any applicable law relating to the processing, privacy, and use of PERSONAL DATA, as applicable to the COMPANY, the CONTRACTOR and/or the WORK, including:

(a) the Regulation of the European Parliament and of the Council 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 (General Data Protection Regulation) (“GDPR”), and/or any corresponding or equivalent national laws or regulations;

(b) [the UK Data Protection Act 1998, and any successor legislation which implements the GDPR in the UK]; and;

(c) any judicial or administrative interpretation of them, any guidance, guidelines, codes of practice, approved codes of conduct or approved certification mechanisms issued by any relevant SUPERVISORY AUTHORITY.

[1.22] “PRIVACY OFFICER” means the COMPANY’s Data Protection Officer (if applicable) or other person that the COMPANY notifies to the CONTRACTOR as being the COMPANY’s point of contact for data protection matters for the CONTRACT as set out in APPENDIX 1 TO SECTION 1 – FORM OF AGREEMENT. In the event that no person is specified in APPENDIX 1 TO SECTION 1 – FORM OF AGREEMENT, the PRIVACY OFFICER shall be the COMPANY REPRESENTATIVE.

[1.23] “PROTECTED DATA” means PERSONAL DATA received from or on behalf of the COMPANY, or otherwise obtained in connection with the performance of the CONTRACTOR’s obligations.

[1.24] “SUB-PROCESSOR” means another PROCESSOR engaged by the CONTRACTOR for carrying out PROCESSING activities in respect of the PROTECTED DATA on behalf of the COMPANY, and authorised by the COMPANY in accordance with Clause [34.7].

[1.25] “SUPERVISORY AUTHORITY” means any local, national or multinational agency, department, official, parliament, public or statutory person or any government or professional body, regulatory or supervisory authority, board or other body responsible for administering DP LAWS.

1.2 Insert a new clause [34] entitled “DATA PROTECTION”:

UK-608152740.4
The parties agree that, for PROTECTED DATA, the COMPANY shall be the CONTROLLER and the CONTRACTOR shall be the PROCESSOR.

Each party shall comply with DP LAWS and its relevant obligations under the CONTRACT. Without prejudice to clauses [8.2] (Subcontracting) and [34.7], the CONTRACTOR shall procure that any SUB-PROCESSOR that has access to PROTECTED DATA shall comply with the CONTRACTOR’s obligations under the CONTRACT.

The PROCESSING to be carried out by the CONTRACTOR under the CONTRACT is for the purpose and type described in APPENDIX 1 TO SECTION 1 – FORM OF AGREEMENT.

Where the CONTRACTOR PROCESSES PROTECTED DATA on behalf of the COMPANY, the CONTRACTOR shall (and shall procure that any person acting under its authority who has access to PROTECTED DATA shall):

(a) PROCESS the PROTECTED DATA only on and in accordance with the COMPANY’s documented instructions as set out in this clause [34], (“PROCESSING INSTRUCTIONS”); and

(b) immediately inform the COMPANY of any legal requirement under applicable law that would require the CONTRACTOR to PROCESS the PROTECTED DATA otherwise than only on and in accordance with the PROCESSING INSTRUCTIONS, or if any COMPANY instruction infringes DP LAWS.

The CONTRACTOR shall implement and maintain, at its cost and expense, appropriate technical and organisational measures in relation to the PROCESSING of PROTECTED DATA by the CONTRACTOR:

(a) such that the PROCESSING will meet the requirements of DP LAWS and ensure the protection of the rights of DATA SUBJECTS; and

(b) so as to ensure a level of security in respect of PROTECTED DATA PROCESSED by it that is appropriate to the risks that are presented by the PROCESSING, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to PROTECTED DATA transmitted, stored or otherwise PROCESSED.

Without prejudice to Clause [34.5(b)], the CONTRACTOR shall, in respect of all PROTECTED DATA PROCESSED by it under the CONTRACT comply with the requirements regarding security of PROCESSING set out in DP LAWS, all relevant COMPANY policies and in the CONTRACT.

The CONTRACTOR shall not engage another PROCESSOR to perform PROCESSING activities in respect of the PROTECTED DATA without the COMPANY’s prior written consent and, if the COMPANY gives its consent, the CONTRACTOR shall appoint the SUB-PROCESSOR under a binding written contract (“PROCESSOR CONTRACT”) which imposes the same data protection obligations as are contained in the CONTRACT on the SUB-PROCESSOR, in particular under Clause [34.5] and the conditions in this clause [34.7] for engaging another PROCESSOR. The CONTRACTOR shall immediately cease using any SUB-PROCESSOR upon receiving written notice from the COMPANY requesting that the SUB-PROCESSOR ceases PROCESSING PROTECTED DATA for security reasons or where the COMPANY has concerns about
the SUB-PROCESSOR’s compliance with DP LAWS or the PROCESSOR CONTRACT.

[34.8] THE CONTRACTOR shall ensure that CONTRACTOR personnel PROCESSING PROTECTED DATA have signed agreements requiring them to keep PROTECTED DATA confidential, and shall take all reasonable steps to ensure the reliability of the CONTRACTOR personnel PROCESSING PROTECTED DATA and to ensure that the CONTRACTOR personnel PROCESSING PROTECTED DATA receive adequate training on compliance with this clause [34] and the DP LAWS applicable to the PROCESSING.

[34.9] The CONTRACTOR shall implement and maintain appropriate technical and organisational measures to assist the COMPANY in the fulfilment of the COMPANY’s obligations to respond to DATA SUBJECT REQUESTS relating to PROTECTED DATA, including to ensure that all DATA SUBJECT REQUESTS it receives are recorded and then referred to the COMPANY within [three] days of receipt of the request.

[34.10] The CONTRACTOR shall provide reasonable assistance, information and cooperation to the COMPANY to ensure compliance with the COMPANY’s obligations under DP LAWS including with respect to: (i) security of PROCESSING; (ii) notification by the COMPANY of breaches to the SUPERVISORY AUTHORITY or DATA SUBJECTS; (iii) DPIAs and prior consultation with a SUPERVISORY AUTHORITY regarding high risk PROCESSING; and (iv) DATA SUBJECT REQUESTS.

[34.11] The CONTRACTOR shall not transfer any PROTECTED DATA to any country outside the European Economic Area (“EEA”) or to any INTERNATIONAL ORGANISATION (an “INTERNATIONAL RECIPIENT”) without the COMPANY’s prior written consent. If the COMPANY consents to the transfer of PROTECTED DATA to an INTERNATIONAL RECIPIENT, the CONTRACTOR shall ensure that such transfer (and any onward transfer): (i) is pursuant to a written contract including provisions relating to security and confidentiality of the PROTECTED DATA; (ii) is effected by way of a legally enforceable mechanism for transfers of PERSONAL DATA as may be permitted under DP LAWS from time to time (the form and content of which shall be subject to the COMPANY’s written approval); (iii) complies with Clause [34.4(a)]; and (iv) otherwise complies with DP LAWS.

[34.12] The CONTRACTOR shall maintain complete, accurate and up to date written records of all categories of PROCESSING activities carried out on behalf of the COMPANY containing such information as required under DP LAWS and any other information the COMPANY reasonably requires (“PROCESSING RECORDS”), and shall make available to the COMPANY on request in a timely manner such information (including the PROCESSING RECORDS) as is required by the COMPANY to demonstrate compliance by the CONTRACTOR with its obligations under DP LAWS and the CONTRACT, which the COMPANY may disclose to the COMPANY GROUP or to the SUPERVISORY AUTHORITY.

[34.13] During the course of the PROCESSING and for a period ending two (2) years following termination or expiry of the CONTRACT, the COMPANY or its duly authorised representative shall have the right to audit or inspect the CONTRACTOR for the purpose of demonstrating the CONTRACTOR’s compliance with its obligations under DP LAWS and this clause [34], subject to the COMPANY giving the CONTRACTOR reasonable prior notice of such audit and/or inspection, and ensuring that any auditor is subject to
binding obligations of confidentiality and that such audit or inspection is undertaken so as to cause minimal disruption to the CONTRACTOR’s business and other customers. The CONTRACTOR shall co-operate fully with the COMPANY and/or its representatives in the carrying out of any audit or inspection required by the COMPANY.

[34.14] In respect of any personal data breach (actual or suspected) related to the WORK or the CONTRACT, the CONTRACTOR shall notify the PRIVACY OFFICER of the breach without undue delay (but in no event later than [twelve (12)] hours after becoming aware of the personal data breach) and provide the PRIVACY OFFICER without undue delay (wherever possible, within [twenty four (24)] hours of becoming aware of the breach) with such details relating to the breach as the PRIVACY OFFICER reasonably requires. Any notices provided under this clause [34.14] shall be subject to the requirements specified in APPENDIX 1 TO SECTION 1 – FORM OF AGREEMENT, and clause [29.6] of the CONTRACT shall not apply to this clause [34.14].

[34.15] The CONTRACTOR shall without delay, at the COMPANY’s written request, either securely delete or return all PROTECTED DATA to the COMPANY [in hardcopy or electronic form] after the end of the provision of the relevant WORK related to PROCESSING or, if earlier, as soon as PROCESSING by the CONTRACTOR of any PROTECTED DATA is no longer required for the CONTRACTOR’s performance of its obligations under the CONTRACT, and securely delete existing copies (unless storage of any data is required by applicable law, and if so the CONTRACTOR shall notify the COMPANY of this).
Amend the Guidance Notes to include a new “Guidance Note [2.19] – Clause [34] – Data Protection” as follows:

[2.19] Clause [34] – Data Protection

This optional clause should be used where the Company is engaging the Contractor to process any personal data as part of the work it is undertaking, so that both parties comply with their obligations under the EU General Data Protection Regulation (GDPR). “Personal data” is defined under the GDPR to mean any information relating to an identified or identifiable natural person. Examples of personal data include an individual’s name, email address and home address, but also may include employee/contractor numbers or other information that can identify the individual in combination with other information that an organisation holds about that individual.

The inclusion of this clause in the contract is only necessary where the Contractor will be processing personal data on behalf of the Company. In this context, the Company will be a “Data Controller” under the GDPR and the Contractor will be a “Data Processor”. “Processing” is broadly defined under the GDPR to mean any operation or set of operations performed on personal data (whether automated or not), including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, disclosure by transmission, restriction, erasure or destruction.

An example of processing that would require incorporation of these provisions is where the Company engages the Contractor to store personal data relating to the Company’s employees on IT infrastructure and makes that personal data available to the Company as part of the services it provides.

This clause will not however be necessary to the extent that both parties are collecting information about the other party’s personnel as an incidental part of their day to day performance of the contract (for example, each party recording the name and contact details of the other party’s contract representative, or the provision of details regarding contractor personnel to the Company as part of identifying who will perform the work under the contract).

As drafted, the provisions only cover the processing of Protected Data (i.e. the personal data that the Contractor receives from or on behalf of the Company or it otherwise obtains in performing its obligations) for which the Company is the Data Controller. If the Company requires the Contractor to process Protected Data that relates to other members of the Company Group, the definition for “Protected Data” should be amended to ensure it adequately covers personal data that relates to the other members of the Company Group. The Company may also wish to amend clause 32 (Contracts (Rights of Third Parties) Act) to ensure that those other members of the Company Group can rely on and enforce these provisions to the extent the Contractor is processing any Protected Data which relates to that company.

These provisions do not address each party’s liability in relation to compliance with these provisions or DP Laws (which includes the GDPR). The parties should therefore consider what amendments, if any, they require as part of their review of clause 30 (Limitations of Liability).

Clause [34.3] requires the parties to describe (in Appendix 1 to Section I – Form of Agreement) the purpose and type of processing that will be undertaken by the Contractor. This is a key requirement under Article 28(3) of the GDPR. Examples of the kind of processing which may be undertaken, and which may be relevant to the oil & gas industry are set out in the appendix to this document.
Note that these are examples only, and the Company and Contractor should ensure that the details that are specified in Appendix 1 to Section 1 accurately reflect the purpose and type of processing that will be undertaken by the Contractor.

Care should be taken in relation to clauses [34.2] and [34.7], and how they relate to clause 8.2 (Subcontracting). Under Article 28(2), a Data Processor is required to obtain prior authorisation from the Data Controller before engaging another processor (i.e. a sub-processor) to process any personal data. It is therefore important to ensure that any variation to the contract that might allow the Contractor to sub-contract without the Company’s consent does not override the requirement in clause [34.7] for the Contractor to obtain the Company’s consent to any sub-processing.

In relation to clauses [34.9], [34.10] and [34.13], it is assumed that the Contractor will be responsible for any costs it incurs complying with these obligations unless the parties otherwise agree in Section III - Remuneration. This is consistent with the general position under clause 14.2.

Note that Article 12(3) of the GDPR requires Data Controllers to respond to Data Subject Requests without undue delay and in any event within one month of receipt of the request (subject to a right to extend the timeframe for two further months where necessary, taking into account the complexity or number of requests). The Company may therefore wish to consider amending clauses [34.9] and [34.10] to incorporate timeframes for the Contractor to respond to any requests for assistance or information when responding to a Data Subject Request.

In order to comply with Article 28(3)(h) of the GDPR, clause [34.13] includes a right for the Company or its authorised representative to conduct audits or inspections in relation to the Contractor’s compliance with DP Laws and clause [34]. As drafted, the Company is entitled to exercise this right during the course of the Processing and for a period ending two years following termination or expiry of the Contract. Whilst the GDPR does not stipulate any timeframe beyond the term of the processing contract for this right to continue, the approach adopted for this clause ensures that there is a reasonable period following termination/expiry for the Company to exercise this right. This can however be amended provided that the Company retains, at a minimum, the right to audit/inspect for the duration of the Processing undertaken by the Contractor.

Under clause [34.14], the timeframes for the Contractor to notify the Company of any personal data breach are to be agreed between the parties. It is important however for the Company to ensure that it receives notification from the Contractor in sufficient time for it to meet any obligation it has to notify the Supervisory Authority (being the Information Commissioner in the UK) and/or any affected Data Subjects. In certain circumstances under Articles 33 and 34 of the GDPR, a Data Controller has an obligation to notify the applicable Supervisory Authority without undue delay, and no later than 72 hours after having become aware of a personal data breach (where feasible), and also notify Data Subjects without undue delay. The notification obligation under this clause should therefore provide the Company sufficient time to assess the personal data breach following notification from the Contractor and determine whether it is required to notify either the Supervisory Authority and/or the Data Subjects.

The Company should also confirm how it wishes to receive notification of any personal data breaches under clause [34.14]. Given the importance of receiving notification as quickly as possible, it would be advisable to specify at least two means of notification (for example email address and mobile telephone number). These details should be specified in Appendix 1 to Section 1 – Form of Agreement.
Clause [34.15] requires the Contractor to delete or return all Protected Data to the Company on written request after completion of the Work or the processing (if sooner), except where the Contractor is legally required to keep any personal data. This provision is required under Article 28(3)(g) of the GDPR, and it is important to note that there is no exception that would permit the Contractor to retain any personal data retained in backups to its systems. Contractors should therefore ensure that they have procedures in place to comply with this obligation.
<table>
<thead>
<tr>
<th>Example</th>
<th>The subject matter and duration of the processing</th>
<th>The nature and purpose of the processing</th>
<th>The type of personal data being processed</th>
<th>The categories of data subjects</th>
</tr>
</thead>
<tbody>
<tr>
<td>IT outsourcing provider (HR system)</td>
<td>The processing relates to the provision of [the IT services] being provided to the Company. As part of the services, the Contractor will process personal data on its IT systems for the duration of the Contract.</td>
<td>The processing forms part of the hosting of a HR system that incorporates personal data relating to the data subjects. This data is stored and accessed by Company personnel as part of the Company’s day-to-day business practices.</td>
<td>Name, contact details, date of birth, health information (sickness records)</td>
<td>Employees and contractor personnel of the Company</td>
</tr>
<tr>
<td>Medical provider</td>
<td>The processing relates to the provision of medical checks undertaken by the Contractor on data subjects to ensure they are fit and healthy to travel to one of the Company’s assets. The processing shall be conducted for the duration of the contract.</td>
<td>The processing involves the collection of personal data relating to data subjects who are undergoing medical checks. The data is used by the Contractor to assess each data subject’s fitness to work, and a limited amount of this personal data will be reported back to the Company so that the Company can confirm whether the data subject can travel to the asset.</td>
<td>Name, contact details, date of birth, health information relating to the tests.</td>
<td>Employees and contractor personnel of the Company</td>
</tr>
<tr>
<td>Example</td>
<td>The subject matter and duration of the processing</td>
<td>The nature and purpose of the processing</td>
<td>The type of personal data being processed</td>
<td>The categories of data subjects</td>
</tr>
<tr>
<td>----------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Transport Operator</td>
<td>The processing relates to the transporting of data subjects by the Contractor to one of the Company’s assets. The personal data shall only be processed as part of booking and operating the flight, and shall be retained for a period of [TBC] following completion of the applicable flight.</td>
<td>The processing involves the identification of data subjects who will be booked on the Contractor’s flights in order to manage the operation of those flights and the identification of the data subjects prior to, and during, operation of the flight.</td>
<td>Name, age, medical information, training information.</td>
<td>Employees and contractor personnel of the Company</td>
</tr>
<tr>
<td>Security contractor</td>
<td>The processing relates to the monitoring of data subjects entering and leaving the Company’s premises. The personal data shall only be processed for as long as is required for the Contractor to perform its duties under the Contract, unless otherwise specified in the Contract.</td>
<td>The processing involves the monitoring and identification of data subjects who are entering and leaving the Company’s premises in order to maintain security and safeguard the Company’s assets and confidential information and other data subjects.</td>
<td>Name, entry and exit information, vehicle registration numbers (where applicable), CCTV footage.</td>
<td>Employees, contractor personnel, third party visitors, members of public (where they have entered on to Company premises)</td>
</tr>
<tr>
<td>Recruitment provider</td>
<td>The processing relates to the assessment by the Contractor of each data subject’s suitability for employment by the Company.</td>
<td>The processing involves the identification and assessment of the data subject’s experience and suitability for employment by the Company.</td>
<td>Name, address, employment history, education history, references.</td>
<td>Candidates, referees</td>
</tr>
<tr>
<td>Example</td>
<td>The subject matter and duration of the processing</td>
<td>The nature and purpose of the processing</td>
<td>The type of personal data being processed</td>
<td>The categories of data subjects</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>Payroll</td>
<td>The processing relates to the payment of salaries to data subjects on behalf of the Company. The processing shall only be conducted for as long as is required in order to process payment.</td>
<td>The processing involves the payment of salaries to data subjects in accordance with the Company’s instructions and requires the Contractor to process payments to each data subject’s nominated bank account.</td>
<td>Name, address, NI number, tax code, bank account details, salary information, nationality (where required for tax purposes)</td>
<td>Employees of the Company</td>
</tr>
<tr>
<td>Training provider</td>
<td>The processing relates to the operation of training services for the data subjects. The personal data shall only be processed in order to conduct the training and retain a record of the training that has been undertaken.</td>
<td>The processing involves the use of personal data relating to the data subject to book and undertake training sessions, and report the outcomes of those sessions to the data subject and the Company.</td>
<td>Name, address, education history</td>
<td>Employees of the Company</td>
</tr>
</tbody>
</table>