Data Processing Agreement

This Agreement ("**Agreement**") dated [●] is between:

(1) [The entity of Getlink[●] a company registered in [●] under company number [●] whose registered office is [●] (the "**Customer**")

and

(2) [Supplier Name] a company registered in [●] under company number [●] whose registered office is [●] (the "**Supplier**").

Whereas:

(A) This Agreement is supplemental to any other separate agreement entered into between the parties for the provision of [●] services (the "**Services**") and introduces further contractual provisions to ensure the protection and security of personal data processed by the Supplier in the course of providing the Services.

(B) This Agreement exists to ensure that the Customer and the Supplier comply with their respective obligations under applicable Data Protection Legislation (as defined below).

Definitions:

In this Agreement, including the recitals above and unless the context otherwise requires:

"**Brexit**" means the date on which the United Kingdom formally leaves the European Union and applies to each of the potential political and legal scenarios on which Brexit may be officially effected, which include but are not limited to the parties failing to reach an exit deal, the UK remaining in the European Union Customs Union or the UK retaining its membership of the European Economic Area.

"**Data Protection Legislation**" means European Directives 95/46/EC and 2002/58/EC and any legislation and/or regulation implementing or made pursuant to them, or which amends, replaces, re-enacts or consolidates any of them (including the General Data Protection Regulation), and all other applicable laws relating to processing of personal data and privacy that may exist in any relevant jurisdiction, including, where applicable, the guidance and codes of practice issued by supervisory authorities;

"**data controller**", "**data processor**", "**data subject**", "**personal data**", "**processing**" and "**appropriate technical and organisational measures**" shall be interpreted in accordance with applicable Data Protection Legislation; and

"**Security Breach**" means any accidental, unauthorised or unlawful destruction, loss, alteration, or disclosure of, or access to the personal data that the Supplier processes in the course of providing the Services.

1. General provisions

1.1 In consideration of the payment of [●] by the Customer to the Supplier (receipt of which the Supplier acknowledges), the Supplier agrees that the provisions of this clause 1 shall apply to the personal data the Supplier processes in the course of providing the Services.

1.2 The Supplier agrees that the Customer is the data controller and the Supplier is the data processor in relation to the personal data that the Supplier processes in the course of providing the Services.

1.3 The subject matter of the data processing is the performance of the Services and the processing will be carried out [please specify the duration]. Annex 2 of this Agreement provides a description of the processing activities.

2. Obligations of the Supplier

2.1 When the Supplier processes personal data in the course of providing the Services the Supplier will:

2.1.1 process the personal data only in accordance with written instructions from the Customer, (which may be specific instructions or instructions of a general nature as set out in the Agreement or as otherwise notified by the Customer to the Supplier from time to time). If the Supplier is required to process the personal data for any other purpose by European Union or Member State laws to which the Supplier is subject, the Supplier will inform the Customer of this requirement first, unless such law(s) prohibit this on important grounds of public interest;

2.1.2 notify the Customer immediately if, in the Supplier's opinion, an instruction for the processing of personal data given by the Customer infringes applicable Data Protection Legislation;

2.1.3 if it receives any complaint, notice or communication which relates directly or indirectly to the processing of the personal data or to any party's compliance with Data Protection Legislation, immediately notify the Customer and provide, at no cost, full co-operation and assistance in relation to any such complaint, notice or communication;

2.1.4 assist the Customer, taking into account the nature of the processing:

2.1.4.1 in ensuring compliance with the obligations pursuant to Articles 32 to 36 of the General Data Protection Regulation, taking into account the information available to the Supplier; and

2.1.4.2 by making available to the Customer all information which the Customer reasonably requests to allow the Customer to demonstrate that the obligations set out in Article 28 of the General Data Protection Regulation relating to the appointment of processors have been met.

The Supplier may not charge a fee for any such assistance, particularly where assistance was required directly as a result of the Supplier's own acts or omissions, in which case such assistance will be at the Supplier's expense;

2.1.5 implement and maintain appropriate technical and organisational measures to protect the personal data against unauthorised or unlawful processing and against accidental loss, destruction, damage, theft, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unlawful processing, accidental loss, destruction, damage or theft of the personal data and having regard to the nature of the personal data which is to be protected. As a minimum, these should include the requirements set out in Annex 1 to this Agreement;

2.1.6 at the Customer’s request, provide a copy of all personal data held by the Supplier in the format and on the media reasonably specified;

2.1.7 at the end of the Services, upon the Customer's request, amend, securely destroy or return the personal data to the Customer, and delete existing copies unless European Union or Member State laws requires storage of such personal data; and

2.2 In the event of a suspected Security Breach, the Supplier will:

2.2.1 take action immediately, at its own expense, to investigate the suspected Security Breach and to identify, prevent and mitigate the effects of the suspected Security Breach and to remedy the Security Breach;

2.2.2 notify the Customer immediately, as soon as it has reasonable cause to believe that a Security Breach has in fact occurred and provide the Customer with a detailed description of the Security Breach including:

2.2.2.1 the likely impact of the Security Breach;

2.2.2.2 the categories and approximate number of data subjects affected and their country of residence and the categories and approximate number of records affected;

2.2.2.3 and the risk posed by the Security Breach to individuals; and

2.2.2.4 the measures taken or proposed to be taken by the Supplier to address the Security Breach and to mitigate its adverse effects

and provide timely updates to this information and any other information the Customer may reasonably request relating to the Security Breach; and

2.2.3 not release or publish any filing, communication, notice, press release, or report concerning the Security Breach without the Customer's prior written approval (except where required to do so by law).

2.3 The Supplier shall further:

2.3.1 not give access to or transfer any personal data to any third party (including any affiliates, group companies or sub-contractors) without the prior written consent of the Customer. Where the Customer does consent to the Supplier engaging a third party to carry out any part of the Services, the Supplier must include in any contract with the third party provisions in favour of the Customer which are equivalent to those in these terms and as are required by applicable Data Protection Legislation. For the avoidance of doubt, where a third party fails to fulfil its obligations under any sub-processing agreement or any applicable Data Protection Legislation, the Supplier will remain fully liable to the Customer for the fulfilment of the Supplier's obligations under these terms;

2.3.2 ensure that access to the personal data is limited to employees, agents or sub-contractors who need access to the data to meet the Supplier's obligations under this Agreement;

2.3.3 ensure that personnel required to access the personal data are made aware of their obligations with regard to the security and protection of the personal data and require that they enter into binding obligations with the Supplier, including a binding duty of confidentiality, in respect of the personal data in order to maintain the levels of security and protection provided for in this Agreement; and

2.3.4 not divulge the personal data, whether directly or indirectly, to any person, firm or company unless (i) required by law or (ii) directed in writing to do so by the Customer except to those of its employees, agents and sub-contractors who are engaged in the processing of the personal data and are subject to the binding obligations referred to in clause 2.3.3.

3. **Audit Rights of the Customer**

3.1 The Customer and its respective auditors or authorised agents are entitled to conduct audits or inspections on reasonable notice during the term of the Agreement and for 12 months thereafter, which will include allowing inspection of and providing access to the premises, equipment, documents, electronic data and personnel of the Supplier and sub-contractors used in connection with the provision of the Services, and the Supplier shall provide all reasonable assistance in order to assist the Customer in exercising its audit rights under this paragraph. The purposes of an audit pursuant to this clause include verifying that the Supplier is processing personal data in accordance with the Supplier's obligations under these terms.

3.2 The requirement under clause 3.1 to give notice will not apply if the Customer believes that the Supplier is in breach of any of its obligations under this Agreement.

4. **Transfer Mechanisms**

4.1 The Supplier shall not transfer the personal data outside the European Economic Area, or to a country in respect of which a valid adequacy decision has not been issued by the European Commission, except with the prior written consent of the Customer.

5. **Warranties**

5.1 The Supplier warrants that it shall:

5.1.1 process the personal data in compliance with all applicable laws, enactments, regulations, orders, standards and other similar instruments, including but not limited to the Data Protection Legislation; and

5.1.2 use its best endeavours to safeguard the personal data from unauthorised or unlawful processing or accidental loss, destruction or damage and acknowledges that it has implemented the technical and organisational measures specified in Annex 1 to prevent unauthorised or unlawful processing or accidental loss or destruction of the personal data.

6. **Liability**

6.1 The Supplier shall be liable for and shall indemnify (and keep indemnified) the Customer against each and every action, proceeding, liability, cost, claim, loss, expense and demand incurred by the Customer which arises directly or in connection with the Supplier's data processing activities under this Agreement, including without limitation those arising out of any third-party demand, claim or action, or any breach of contract, negligence, fraud, wilful misconduct, breach of statutory duty or non-compliance with Data Protection Legislation by the Supplier or its employees, agents or sub-contractors.

6.2 The Supplier's liability referred to in clause 6(1) shall not exceed £10 million or the upper limit of the Supplier's insurance coverage, whichever is the higher. For the avoidance of doubt, the limits of liability referred to in this clause 6(2) shall apply per event rather than in the aggregate.

7. **Jurisdiction**

7.1 These terms and any dispute or claims (including non-contractual disputes or claims) arising out of or in connection with the subject matter or formation of this Agreement shall be governed by and interpreted in accordance with the law of England and Wales.

7.2 The Supplier and the Customer irrevocably agree that the courts of England and Wales have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) that arises out of, or in connection with, the Agreement or its subject matter or formation.

8. **Brexit**

8.1 In the event that Brexit takes effect during the term of this Agreement, the Supplier agrees that it will discuss in good faith and agree to any amendments to this Agreement that are reasonably requested by the Customer as a result of Brexit. The Customer reserves the right to terminate the Agreement in the event that negotiation is unsuccessful.

Signed for and on behalf of [Getlink entity] Name: Position: Date: Signature:	Signed for and on behalf of [Insert Name] Name: Position: Date: Signature:

Annex 1

Security Measures

1. Access control to premises and facilities

Measures must be taken to prevent unauthorized physical access to premises and facilities holding personal data. Measures shall include:

- Access control system
- ID reader, magnetic card, chip card
- (Issue of) keys
- Door locking (electric door openers etc.)
- Surveillance facilities
- Alarm system, video/CCTV monitor
- Logging of facility exits/entries

2. Access control to systems

Measures must be taken to prevent unauthorized access to IT systems. These must include the following technical and organizational measures for user identification and authentication:

- Password procedures (incl. special characters, minimum length, forced change of password)
- No access for guest users or anonymous accounts
- Central management of system access
- Access to IT systems subject to approval from HR management and IT system administrators

3. Access control to data

Measures must be taken to prevent authorized users from accessing data beyond their authorized access rights and prevent the unauthorised input, reading, copying, removal modification or disclosure of data. These measures shall include:

- Differentiated access rights

- Access rights defined according to duties
- Automated log of user access via IT systems
- Measures to prevent the use of automated data-processing systems by unauthorised persons using data communication equipment

4. Disclosure control

Measures must be taken to prevent the unauthorized access, alteration or removal of data during transfer, and to ensure that all transfers are secure and are logged. These measures shall include:

- Compulsory use of a wholly-owned private network for all data transfers
- Encryption using a VPN for remote access, transport and communication of data.
- Prohibition of portable media
- Creating an audit trail of all data transfers

5. Input control

Measures must be put in place to ensure all data management and maintenance is logged, and an audit trail of whether data have been entered, changed or removed (deleted) and by whom must be maintained.

Measures should include:

- Logging user activities on IT systems
- Ensure that it is possible to verify and establish to which bodies personal data have been or may be transmitted or made available using data communication equipment
- Ensure that it is possible to verify and establish which personal data have been input into automated data-processing systems and when and by whom the data have been input;

6. Job control

Measures should be put in place to ensure that data is processed strictly in compliance with the data importer's instructions. These measures must include:

- Unambiguous wording of contractual instructions
- Monitoring of contract performance

7. Availability control

Measures should be put in place to ensure that data are protected against accidental destruction or loss.

These measures must include:

- Ensuring that installed systems may, in the case of interruption, be restored
- Ensure systems are functioning, and that faults are reported
- Ensure stored personal data cannot be corrupted by means of a malfunctioning of the system
- Uninterruptible power supply (UPS)
- Business Continuity procedures
- Remote storage
- Anti-virus/firewall systems

8. Segregation control

Measures should be put in place to allow data collected for different purposes to be processed separately.

These should include:

- Restriction of access to data stored for different purposes according to staff duties.
- Segregation of business IT systems
- Segregation of IT testing and production environments

9. Security measures required if the Supplier is integrating its IT system with Eurotunnel's IT system.

Annex 2

Description of the processing activities

Data Subjects

The personal data concern the following categories of data subjects:

[●] *[Example: Staff or other personnel working for the Customer (including employees and temporary or contract personnel)]*

Categories of data

The personal data transferred concern the following categories of data:

[●] *[Example: Identifying information: name (and previous names), contact details, date of birth, address history, country of residence, financial and banking details.]*

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data:

[●] *[Example: Health status relevant to administration of long term disability or other medical benefit programs, medical reports, return or work/adjustment reports and workplace injury reports]*

Processing operations

The personal data transferred will be subject to the following basic processing activities:

[●] *[Example: for the provision of [●] services by the Supplier to the Customer and other related purposes]*