Interoute GCloud 10 Supplier Terms and Conditions

Proposal Date: 23rd May 2018

ENGINEERED FOR
THE AMBITIOUS

interoute
interoute.com

VERSION HISTORY

Version	Date	Title	Author
V0.1	23rd May 2018	GCloud 10 – Supplier Terms and Conditions	Interoute

All quotes, offers or proposals are (i) made based on Interoute's standard terms and conditions (ii) subject to contract, survey and availability; and (iii) only valid for a period of 30 days from the date of this message.

CONFIDENTIALITY STATEMENT

Interoute is a trading name of Interoute Communications Limited, registered in England number 04472687, registered address: Interoute, 31st Floor, 25 Canada Square, Canary Wharf, London E14 5LQ.

Nothing within this document may be construed as an offer to supply goods or services except where explicitly stated. All sales are subject to contract.

Interoute and GTT

On Monday 26th February 2018, it was announced GTT had reached a definitive agreement to purchase 100% of the shares of Interoute. The acquisition is expected to close in the second half of 2018 as it is subject to customary regulatory clearances.

GTT Communications, Inc., is a publicly traded company on the New York Stock Exchange (NYSE: GTT) that provides multinational clients with connectivity to the cloud through a comprehensive suite of cloud networking services, including wide area networking, internet, optical transport, managed services and voice services.

Once the acquisition is complete the combination of Interoute and GTT will bring additional resources, deeper geographic reach and enhanced technical skills. This will enable us to provide you with products and services in more places than ever before. The combined company will bring together Interoute's depth and reach in Europe with GTT's fast-growing, global cloud networking business and dense connectivity footprint in North America.

As the transaction progresses towards completion over the coming months, Interoute will continue to run as an independent business, with no material changes. And as we enter this next stage of our development we will remain dedicated to serving you and supporting your business with the services it needs to thrive. Our business is joining with another like-minded, customer focused service provider that will enable us to extend our ability to support the best company's in the world, with advanced infrastructure and solutions, from the Ground to the Cloud.

Contents

1. Definitions

In these Supplier Terms and any Additional Terms as defined below (except where the context requires or stipulates otherwise) capitalised words and expressions shall have the meanings set out below:

"Affiliate" means in relation to a party, any person which, directly or indirectly, is controlled by that party or Controls that party or is under substantially common Control with that party;

"Additional Terms" means the terms applicable to each specific Service as set out in the relevant Schedule(s) 2 which are listed in Appendix 1 and available at www.interoute.com/legal;

"Agreement" means the Framework Agreement and/ or the relevant Call-Off Contract and/or Purchase Order, as the context requires, and any amendments or additions or replacements to any of the aforementioned, these Supplier Terms and any Additional Terms as defined below;

"AUP" or "**Acceptable Use Policy"** means Interoute's acceptable use policy which is available on the Interoute website, at www.interoute.com as amended from time to time;

"**Change"** means any proposed amendment or modification to the Agreement, other than an Order for the provision of Services to additional Sites, of new Service components, or for an upgrade to a higher grade Service in accordance, but including any Standard Change or other proposed amendment, addition, subtraction or modification to the scope or details of the Services;

"Charges" means the amounts payable for the Services, as set out in the relevant Order and/or any other amounts as may be payable by the Customer under the terms of the Agreement;

"Confidential Information" means the terms of the Agreement and all information whether in written or any other form which has been or may be disclosed in the course of the discussions leading up to the entering into or performance of the Agreement which may include but is not limited to information relating to the Agreement or the Services, data used or generated in the provision of the Services, or any of Customer's products, operations, processes, plans or intentions, know-how, trade secrets, market opportunities, customers and business affairs and any other information clearly designated as being confidential or which ought reasonably to be considered to be confidential (whether or not such information is marked "confidential");

"Control" means the power of a person to secure (whether by the holding of shares, possession of voting rights or by virtue of any powers conferred by articles of association, constitution, partnership agreement or other document regulating such person) that the affairs of another are conducted in accordance with its wishes and "Controlled" shall be construed accordingly;

"Customer Committed Date" means the date assigned by Interoute for the delivery of the Service. Interoute shall communicate this date to the Customer after a Purchase Order is entered into between the Parties;

"Customer Contact Centre" or "CCC" means Interoute's incident management centre;

"Customer Equipment" means any equipment either belonging to the Customer or leased to the Customer by any third party (other than Interoute);

"Customer Premise Equipment" or **"CPE"** means any equipment that is sited on the Customer Premises that is supplied and managed by Interoute or suppliers of Interoute;

"Customer Premises" means a location owned or controlled by the Customer where equipment is sited for the purpose of delivery of the Service;

"Data Processing Agreement" means Interoute's data processing agreement which are appended as Appendix 2.

"Dispute Notice" and **"Dispute Resolution Procedure"** shall have the meanings described in Clause 23 of these Supplier Terms;

"Emergency Maintenance" means works carried out in an emergency that are necessary to restore or repair (or prevent an imminent need to restore or repair) the Interoute Network or the Service upon damage or disruption to the Interoute Network or the Service;

"Employment Liabilities" means any action, award, claim, cost (including legal costs), damage, loss, demand, expense, liability, interest, fine, penalty or proceeding;

“Equipment” means equipment (which may include CPE) owned or managed by Interoute or suppliers of Interoute, including Licensed Software which is owned by Interoute or by suppliers of Interoute;

“Fixed Rate Charge” means the recurring charges payable by the Customer for the provision of the Service(s) by Interoute, as set out in the Purchase Order;

“Incoming Service Provider” means any third party who will carry out activities for or on behalf of the Customer which previously comprised all or part of the Services;

“Initial Term” with respect to each Service means a period of time starting from the Ready for Service Date of minimum 12 months and maximum 24 months as stated on the Purchase Order;

“Interoute” means the Supplier, as defined in the Agreement;

“Installation Charge” means the non-recurring Charges stated as being Installation Charges in respect of the Service specified in the relevant Order;

“**Intellectual Property Rights**” means any patent, copyright, trademark, trade name, service mark, moral right, database right, know-how and any and all other intellectual property right whether registered or not or capable of registration and whether subsisting in the United Kingdom or any other part of the world together with any and all goodwill relating thereto;

“Interoute Demarcation Point” means the edge of the Interoute Network that signifies the physical or logical boundary between the Interoute Network and Customer Equipment. For Sites where managed CPE is provided, the physical boundary between Interoute and the Customer is the interface on the CPE. For Sites where no managed CPE is provided the Interoute Demarcation Point is the Customer port;

“Interoute Network” means the fibre optic communications network which is owned or operated by Interoute and its Associated Companies from time to time;

“Liability” shall mean liability in or for breach of contract, misrepresentation, restitution or any other cause of action whatsoever relating to or arising under or in connection with this Agreement, including without limitation liability expressly provided for under this Agreement or arising by reason of the invalidity or unenforceability of any term of this Agreement (and for the purposes of this definition, all references to "this Agreement" shall be deemed to include any collateral contract);

“**Licensed Software**” means computer software in object code format made available to the Customer by Interoute for the use of any Services;

“Main Body” means clauses 1 to 28 of these Supplier Terms.

“Monthly Review Period” means the calendar monthly periods commencing on the 1st of each month during the Term;

“My Services” means the Interoute online tool that includes the Customer account details and Service(s) portfolio;

“Planned Outage” means any routine maintenance or upgrade work which affects the availability of Service;

“**Professional Service Charges**” means the professional service charges detailed on the Purchase Order;

“Ready for Service Date” shall be the date when the Service is handed over to the Customer unless stated otherwise in the relevant Additional Terms;

"Relevant End-use" includes: military use; or, use in connection with chemical, biological or nuclear weapons or other nuclear explosive devices or the development, production, maintenance or storage of missiles capable of delivering such weapons; or, use in connection with Iran's enrichment-related, reprocessing, or heavy water-related activities;

“Renewal Term” unless otherwise stated in the Purchase Order is the twelve (12) month period commencing upon expiry of the Initial Term or any subsequent anniversary thereof;

“Restrictive Sanctions” means Restrictive Sanctions measures adopted by the United Nations or implemented by the European Union, a Member State, or the United States;

"Service Handover Document" means a document made available to the Customer by Interoute indicating that the Service is ready for use and, if applicable, for testing by the Customer;

"Services" means the services identified in the Purchase Order(s), to be provided to the Customer by Interoute under this Agreement and the applicable Additional Terms;

"Service Credit" means an amount calculated as set forth in the applicable Additional Terms credited by Interoute for the failure to achieve the relevant SLA applicable to a particular Service, where applicable, subject to the service credit provisions in these Supplier Terms;

"Service Level Agreement" or **"SLA"** means the service level agreement relating to a Service as set out in the relevant Additional Terms;

"Site" means the space occupied by Customer and/or Interoute where the Customer requires the Service or for the purposes of installing any Customer Premise Equipment required to provide the Service(s) to the Customer;

"Term" shall mean the Initial Term and the Renewal Term where applicable;

"Purchase Order" means a request for the provision of Services on an order form which as agreed by Interoute and the Customer in a Call-Off Contract;

"Outgoing Service Provider" means any third party who previously carried out activities for or on behalf of the Customer which will (in whole or in part) be comprised in the Services following the commencement of the Agreement;

"Party" means Interoute and the Customer (as the case may be) and shall include their permitted assignees and **"Parties"** shall mean both of them;

"Personal Data" shall have the meaning as defined in Section 1 of the Data Protection Act 1998;

"Schedules 2" means the service schedules enclosed hereto;

"Taxes" means any tax, duty or other charges of whatever nature (but excluding any tax, duty or other charged levied on income accruing to Interoute hereunder) imposed by any taxing or government authority including, without limitation VAT;

"Transfer Regulations" means the Transfer of Undertakings (Protection of Employment) Regulations 2006 or such other applicable legislation governing the transfer of businesses from time to time in force;

"VAT" means Value Added Tax or any other similar sales or transaction tax;

"Withholding Tax" means any amount on account of tax on sources of income which the payer is obliged to deduct from payments due to the recipient and account for to any tax authority;

"Working Day" means 9.00 am to 5.00 pm on any day from Monday to Friday (inclusive) which is not Christmas Day, Good Friday or other statutory or national holiday in the jurisdiction in which the relevant notice is to be given or where the relevant activity is to be performed.

Any other undefined capitalised terms have the meaning set out in the applicable Additional Terms.

1.1 Save as agreed otherwise, in the event of conflict between the terms and provisions of any of the documents referred to in this Clause 1.1, the following order of priority will be applicable:

1.1.1 the terms and conditions of the Purchase Order;

1.1.2 the applicable Additional Terms; and then

1.1.3 the Main Body of these Supplier Terms.

1.2 In the Agreement (except where the context otherwise requires):

1.2.1 references in the Agreement to the singular include the plural and vice-versa;

1.2.2 any reference to "persons" includes natural persons, firms, partnerships, companies, corporations, associations, organisations, governments, states, governmental or state agencies, foundations and trusts (in each case whether or not having separate legal personality and irrespective of the jurisdiction in or under the law of which it was

incorporated or exists);

1.2.3 the headings contained in the Agreement are for convenience only and shall not influence the interpretation of the Agreement;

1.2.4 any reference to time of day is to the local time in the country (or countries) in which the Service is being provided;

1.2.5 general words introduced or followed by the word "other" or "including" or "in particular" shall not be given a restrictive meaning because they are followed or preceded (as the case may be) by particular examples intended to fall within the meaning of the general words;

1.2.6 a reference to a statute or statutory provision is a reference to that statute or statutory provision and to all orders, regulations, instruments or other subordinate legislation made under the relevant statute; and

1.2.7 any reference to a statute, statutory provision, subordinate legislation, code or guideline ("legislation") is a reference to such legislation as amended and in force from time to time and to any legislation which re-enacts or consolidates (with or without modification) any such legislation.

1.3 Interoute and the Customer each represents and warrants to each other that it has the power to enter into, exercise its rights under and perform and comply with its obligations under the Agreement and all actions, conditions and things required to be taken, fulfilled and done by it to so enter into, exercise its rights under and perform and comply with its obligations under the Agreement and ensure that those obligations are valid, legally binding and enforceable have been taken, fulfilled and done.

2. Handover and acceptance of the Services

2.1 Interoute shall use reasonable endeavours to ensure the Ready for Service Date occurs on or before the Customer Committed Date. Interoute shall hand over the Service to the Customer and deliver to Customer a Service Handover Document. The Service Handover Document shall state the Ready for Service Date.

2.2 Unless otherwise agreed in the a Purchase Order or the applicable Additional Terms, the Customer shall have five (5) Working Days from the date of delivery of the Service Handover Document to notify Interoute of any material non-compliance of the Service with the relevant Additional Terms by performance testing, and shall provide Interoute with the results evidencing such non-compliance, if any.

2.3 If the Customer notifies Interoute in accordance with Clause 2.2, Interoute will take such action as is reasonably necessary to provide the Service in accordance with the Additional Terms. The process in Clause 2.2 shall be repeated until the performance testing has been successfully completed.

2.4 In the event that any deviation or non-compliance with the Additional Terms is attributable to the Customer's system or network or otherwise due to the act or omission of Customer, Interoute shall be entitled to invoice the Customer for any costs reasonably incurred in investigating the matter.

2.5 Unless the Customer notifies Interoute of any non-compliance within the timescales set out in Clause 2.2, the Customer shall be deemed to have accepted the Service as of the Ready for Service Date set out in the Service Handover Document and Interoute shall commence billing. Notwithstanding anything contained herein, the Customer's use of the Service other than for testing purposes will be deemed to constitute acceptance of that Service.

2.6 If the Ready for Service Date of the Service is delayed due to an act or omission of the Customer, including but not limited to:

a) a failure to provide information reasonably requested by Interoute; or

b) the information provided by the Customer is incomplete, incorrect and/or illegible; or

c) a failure to permit access to Site, Customer Equipment or Equipment or any other reason which prevents Interoute from undertaking performance testing or installation (e.g. lack of connectivity where to be provided by Customer), then Interoute reserves the right to commence charging the Charges from the date Interoute has informed the Customer that Interoute is ready to deliver the Service(s), but is unable to do so due to an act or omission of the Customer for the reasons set out in this Clause.

2.7 The following terms apply to the Customer's use of My Services:

a) Interoute is entitled to act upon and rely on any communication (including orders) received through My Services and to treat such communications as authorised by the Customer without conducting any further verification. This Clause shall apply whether or not the information contained in the communication is, in fact, correct or the communication is authorised;

b) Customer accepts full responsibility for all My Services usernames and passwords. These usernames and passwords are to be kept confidential and only accessed or used by persons authorised by the Customer;

c) Interoute is not liable for any loss whatsoever arising from information provided by the Customer through My Services.

3. Service Level Agreement and Service Credits

3.1. Interoute shall provide the Service(s) in accordance with the Service Level Agreement set out in the Additional Terms.

3.2. The Customer's sole and exclusive remedy for a cause of action that results in a deviation from the Service Level Agreement is the Service Credits as set out in the relevant Additional Terms. The Customer agrees that the compensation provided under the Additional Terms represents a reasonable pre-estimate of all of its losses and Interoute shall have no further Liability to Customer for the failure to achieve the Service Level Agreement.

3.3. If as a result of a same occurrence more than one Service Level target is failed, the Customer shall not be able to claim for more than one failure but its right to receive Service Credits shall be restricted to the Service Level target which has the highest Service Credit available.

3.4. Claims will be paid only against validated claims, provided the Customer has paid Interoute all sums due under the Agreement, any credit balance due to the Customer will be carried forward to the next billing period.

3.5. In the event that a Service Credit is due to the Customer, Interoute will issue a credit note upon Customer's request. The Customer shall not be entitled to any Service Credits in respect of a claim unless and until Interoute has received notice of the claim in writing within twenty one (21) days of the end of the month for which a credit is requested. Customer must submit a documented claim, setting out the reason for the claim and providing such evidence as shall be reasonably necessary to support the claim. Service Credits will be calculated and credited to the Customer on a monthly basis.

3.6. For the first Monthly Review Period of a Service, the Service Levels and the Charges used to calculate the Service Credits will be prorated from the Ready for Service Date until the end of the first Monthly Review Period. If a Service is cancelled during a Monthly Review Period, no Service Credit will be payable in respect of that Service for that Monthly Review Period.

37. Service Credits will not be payable by Interoute to the Customer where the failure to meet a Service Level is caused by any of the following:

a. The fault or negligence of the Customer, its employees, agents or contractors;
b. The Customer failing to comply with the terms of the Agreement;
c. Any Event of Force Majeure;
d. A failure by the Customer to give Interoute necessary access to any Equipment or Customer Equipment and/or Site after being requested to do so by Interoute;
e. Maintenance during any Planned Outage;

f. A fault in, or any other problem associated with, equipment connected on the Customer's side of the Interoute Demarcation Point. E.g. Customer LAN;
g. Any outages or degradation to existing Service that may be the result of Customer requested Service changes or upgrades;
h. Any damage or disruption to subsea cables;
i. Failure to provide spare parts for Customer Equipment;
j. Any malfunction of Customer serviced software including a failing shutdown or boot of Customer serviced software; or
k. DNS issues outside the direct control of Interoute. For instance, in all cases in which a domain is not managed by Interoute on its own DNS servers.

4. Operation and Maintenance

4.1 Should any condition exist that may impair the integrity of the Interoute Network or otherwise damage or disrupt Interoute's Network or the Services or those of Interoute's other customers, Interoute shall initiate and co-ordinate Emergency Maintenance, which may include disconnection of all or any part of the Service. Save in case of emergency Interoute shall give the Customer advance notice of Emergency Maintenance works.

4.2 From time to time planned maintenance will be carried out which may affect the Customer's Service. Interoute shall, to the extent reasonably practicable, give the Customer ten (10) days prior notice in writing (or such shorter period as may be necessary) of the timing and scope of such planned maintenance, if it is or is likely to cause a Planned Outage.

4.3 Interoute shall use reasonable efforts to conduct any Planned Outage during the hours of 11pm and 5am Greenwich Mean Time Monday to Sunday.

4.4 Interoute's Customer Contact Centre shall endeavour to inform the Customer if the Customer's Service experiences any outage. This information will be provided twenty-four (24) hours a day, seven (7) days a week. Interoute shall endeavour to notify the Customer of any Service affecting outage within two (2) hours of Interoute's first awareness of such disruption.

5 Equipment and Access

5.1 Interoute may require to locate Equipment on the Customer's Premises to enable Interoute to provide the Services. Subject to the provisions of this Agreement, Customer hereby grants to Interoute the right to locate, install and operate such Equipment at the Customer's Premises and shall provide Interoute, its employees, representatives and authorised agents, as may be reasonably required, access to the Equipment via the Interoute Network or otherwise, 24 hours a day, 7 days a week in accordance with the access procedures agreed between the Parties.

5.2 Customer shall furnish reasonable, appropriate environmental conditions for the Equipment (including, without limitation, protection from weather, security, availability of power, including a back-up generator, ventilation, heating, and cooling). If Customer reasonably requires to temporarily disconnect the power supply to the Equipment, except in an emergency, Customer will give Interoute at least fourteen (14) written days' notice in advance of such disconnection and will use all reasonable endeavours to ensure minimum disruption. Interoute shall not be liable for disruption to Services under this Clause.

5.3 The Customer undertakes (a) not to replace Equipment located on the Customer Premises, (b) not to make any modification, alteration or connection to the same other than by prior agreement in writing with Interoute nor (c) make any disconnection therefrom otherwise than in accordance with the terms and conditions of this Agreement.

5.4 Save where title passes to Customer as set out in the Purchase Order, ownership and title in Equipment provided by Interoute under this Agreement shall at all times remain with Interoute or the Interoute

supplier (if the Equipment was supplied by an Interoute supplier), and the Customer shall exercise commercially reasonable efforts to prevent third parties from asserting any rights in relation to such Equipment.

6. Charges and Payment

6.1 Unless stated otherwise in the Purchase Order and/or the relevant Additional Terms:

a. Interoute will invoice Installation Charges, charges for the sale of equipment and any other non-recurring initial Charges, upon the coming into force of a Purchase Order;
b. Interoute will invoice all recurring Charges as of the Ready for Service Date and monthly in advance thereafter;
c. Interoute shall invoice any other Charges not covered by (a) and (b) above as and when incurred; and
d. The Customer shall pay all Charges, within thirty (30) days of the date of the relevant invoice.

6.3 All amounts in respect of Charges shall be paid as specified on the Purchase Order and shall be paid free of currency exchange costs, bank charges, withholding or deductions. To the extent that any deduction or withholding is required by applicable law, Customer shall increase the amount of such payment to ensure that Interoute receives the amount it would have received had no deduction or withholding been required.

6.4 In the event that Customer in good faith disputes any portion of the Charges contained in an invoice, Customer will pay the undisputed portion of the invoice on the due date in full and submit a documented claim for the disputed amount. As a minimum such documented claim shall set out the amount in dispute, the reason for such dispute and provide such evidence as shall be reasonably necessary to support the dispute. The Parties shall negotiate in good faith in an attempt to resolve the dispute, provided that if the dispute cannot be resolved within thirty (30) days of the date of the invoice, either Party may institute legal proceedings. If Customer does not submit a documented claim prior to the due date for payment of the invoice, Customer waives all rights to dispute the invoice.

6.5 In the event of any failure by the Customer to make full payment to Interoute of any and all amounts due to Interoute pursuant to the Agreement, the Customer shall be responsible for all costs and expenses (including legal fees) incurred by Interoute, its Affiliates or its agents in collecting such amounts.

7. Taxes

7.1 All Charges and any other fees under this Agreement are exclusive of Value Added Tax (VAT) or any similar indirect or sales taxes that may be applicable. If any VAT or similar sales tax is chargeable by Interoute, this will be added to the agreed price (by way of separate invoice, if those Charges have already been invoiced) and shall be paid in addition by the Customer.

7.2 If Withholding Tax applies to any payments for supplies made under this Agreement, the Customer may withhold that element that is required under the applicable legislation but must pay an additional amount in accordance with Clause 7.3 and must notify Interoute prior to payment that Withholding Tax is required to be paid. The Parties undertake to co-operate, where possible, to minimise the amount of Withholding Tax due by making advance clearance applications under the relevant double taxation treaties (where applicable) to the relevant tax authority to reduce the rate of Withholding Tax or exempt entirely this amount if applicable. In any event, the Customer undertakes to account for any tax withheld to the tax authorities on a timely basis.

7.3 Neither Party shall be liable for the other Party's Taxes based on income (including gains from the disposal of capital).

7.4 Any other Taxes or levies arising from the use of the Services (including local profits taxes) (if any) shall be the Liability of the Customer and Interoute reserves the right to recharge these to the Customer.

7.5 Any stamp duties or registration taxes or other Taxes relating to documentation of the individual transactions entered into under this contract shall be borne by the Customer.

8. Term, Suspension and Termination

8.1 A Purchase Order shall be valid from when the Customer acknowledges the receipt of the signed copy of the signed order form by Interoute as per clause 1 (Formation of the contract) of Part A of the Call-Off Contract (Order Form), until the expiry of the Initial Term or any applicable Renewal Term thereafter (unless terminated earlier in accordance with the terms of this Agreement).

8.2 The Purchase Order shall expire and may be renewed in accordance with clause 1 of Part B of the Call-Off Contract.

8.3 Either Party may terminate this Agreement with immediate effect by written notice to the other Party on or any time after the occurrence of any of the following events:

a. The other Party ceases to trade (either in whole, or as to any part involved in the performance of this Agreement), or becomes insolvent, has a receiver, administrative receiver, administrator or manager appointed of the whole or any part of its assets or business, makes any composition or arrangement with its creditors, takes or suffers any similar action in consequence of debt, is unable to pay its debts when due, or any order or resolution is made for its dissolution or liquidation (other than for the purpose of solvent amalgamation or reconstruction) under the laws applicable to that Party; or
b. The other Party commits a material breach of this Agreement which is not capable of remedy and, if capable of remedy, the breach is not remedied within 15 Working Days following a written notice by the non-breaching Party to the other Party.

8.4 Interoute may suspend all or any Service under any Purchase Order(s) and/or the Agreement and/or any other agreement between the Customer and Interoute with immediate effect by written notice to the Customer with no Liability or penalty where the Customer:

a. provides materially incorrect, false, illegible or incomplete information to Interoute and Customer failed to remedy within five (5) Working Days from receipt of written notice by Interoute;
b. is likely to defraud Interoute, interfere with Interoute's services or create harm to the Interoute Network, Equipment or any third party's property and/or services;
c. fails to make any payment due under any Purchase Order in accordance with the terms and conditions set out in this Agreement and fails to do so within 72 hours following written notice by Interoute;
d. fails to use, or ensure the use of, any of the Services in accordance with the Acceptable Use Policy;
e. is in breach of the terms of any licence for Licenced Software; or
f. is using or allowing (or in the reasonable opinion of Interoute is likely to be using or allowing) any of the Services to be used for fraud, misconduct or any other illegal purpose,

8.5 Any exercise of such right of suspension shall not prejudice Interoute's right to payment hereunder.

8.6 If Interoute suspends any Service in accordance with Clause 8.4 above, Interoute may claim and Customer shall pay upon demand, a reasonable Charge for re-commencing the provision of the Services if applicable.

8.7 Interoute may terminate all or any Service under any Purchase Order(s) and/or this Agreement and/or any other agreement between the Customer and Interoute with immediate effect by written notice to the Customer with no Liability or penalty where Interoute has exercised its suspension right under Clause 8.4 and the Customer has not remedied the underlying cause of suspension within ten (10) Working Days of the date of the notice of suspension.

8.8 Where Interoute suspends Service(s) in accordance with the provisions of Clause 8.4 of these Supplier Terms save where Interoute is entitled to and subsequently elects to terminate the Agreement in respect of such Service(s) in accordance with the terms of the Agreement, Interoute shall use its reasonable endeavours to reinstate the Service as soon as is reasonably practical in the circumstances upon Interoute

becoming satisfied (acting reasonably) that the grounds for suspension as aforesaid are no longer applicable and subject to the Customer having paid to Interoute the reinstatement fee as per clause 8.6.

8.9 If Interoute exercises its right of suspension under these Supplier Terms this will not exclude its right to terminate the Agreement later in respect of that or any other event, nor will it prevent Interoute claiming damages from the Customer in respect of any breach.

8.11 Interoute reserves the right to terminate the Agreement with immediate effect by written notice and without further obligation or liability to the Customer as required by any law enforcement or other government or regulatory organisation or authority or by the courts.

9. Consequences of Termination

9.1 On expiry or termination of the Agreement or a Purchase Order:

a. all sums due to Interoute up to the date of termination shall become immediately due and payable to Interoute;
b. the Customer must immediately return to Interoute in good condition all Equipment which Interoute has leased or loaned to the Customer and which is under Customer's possession or control. In the event that the Customer fails to return all Equipment, then the Customer shall allow Interoute or Interoute's supplier reasonable access, without charge, to its premises to recover the Equipment Interoute may charge the Customer for all costs incurred in repossessing or acquiring replacement Equipment which the Customer has failed to return to Interoute or which is returned to Interoute in a damaged or defective condition; and
c. Interoute will have the right to retain any Customer Equipment which is used in respect of the Service and which is on premises made available by Interoute, until receipt of all sums due or and payable to Interoute. If Interoute has not received such sums due and/or payable within a reasonable time frame to be determined by Interoute, Interoute reserve the right to sell any Customer Equipment necessary, at such price as it is able to obtain in the open market, to recoup all sums due and payable to it.

9.2 Unless otherwise agreed in a Purchase Order, where the Customer terminates all or part of the Call-Off Contract without cause and the termination takes effect before expiry of the Initial Term or any applicable Renewal Term the Customer will be liable to pay the following early termination costs which will be reasonable, proven and itemised to the Customer in accordance with Clause 18.3 of the Part B of the Call-Off Contract (Terms and Conditions):

9.2.1 costs of administering the termination including without limitation the destruction or return (or 'off-loading') of data where requested by the Customer,

9.2.2 costs of any reasonable migration assistance requested by the Customer;

9.2.3 costs of storing or removing Equipment which the Customer has not collected or failed to return to Interoute or which is returned to Interoute in a damaged or defective condition,

9.2.4 costs of any unused licenses, amortised equipment or other third party costs relating o the unexpired remainder of the Initial Term or any applicable Renewal Term;

9.2.5 Unexpired equipment lease commitments or unamortised equipment costs still outstanding at the termination date;

9.2.6 costs of accounting to the Customer in relation to the above termination costs as; and

9.2.7 any other costs reasonably incurred by Interoute as a consequence of the termination namely any third party cancellation/termination charges associated with the Service/s so terminated or the equivalent of seventy five percent (75%) of the Fixed Rate Charges, actual or projected, for each month remaining in the Initial Term or the relevant Renewal Term, whichever is greater.

9.3 The Customer agrees that the termination charges in Clause 11.2.7 are a genuine pre-estimate of loss and are not a penalty.

9.4 The Customer acknowledges that Interoute does not hold insurance in relation to the costs arising as a result of any termination by Customer under Clause 18.3 of the Part B of the Call-Off Contract (Terms and Conditions) and as such will be unable to reduce its unavailable costs arising from such a termination by claiming on insurance.

9.5 All rights and obligations or Liabilities of the parties shall cease to have effect immediately upon termination of this Agreement except that termination shall not affect:

a) accrued rights and obligations or Liabilities of the parties at the date of termination; and
b) the continued survival and validity of the rights and obligations of the parties under any provisions of the Agreement or these Supplier Terms that are necessary for the interpretation or enforcement of the Agreement including these Supplier Terms.

9.6 For the avoidance of doubt, save where otherwise agreed in writing between the parties, termination of any Site or Service component does not constitute termination of the Call-Off Agreement, and, where the Call-Off Contract has been terminated in accordance with its terms, all Service components will automatically terminate upon such termination.

9.7 The following Clauses shall survive the termination or expiration of this Agreement in addition to those whose provisions by their content or nature will so survive: Equipment and Access, Liability and Indemnity, Intellectual Property Indemnity, Severability, Waiver, Notices, Confidentiality, Press Announcements, Associated Company Orders and Rights of Third Parties and Governing Law and Jurisdiction.

10. Exit Plan

10.1 Upon expiry or termination of the Services, in order to start implementation of the exit strategy plan, the Customer shall request in writing to Interoute the date on which the Customer wishes such transition to start and, to this end, the date from when Interoute requires the transition assistance of an Interoute Project Manager and/or Technical Manager.

10.2 Interoute shall provide the Customer with a Project Manager and/or a Technical Manager as requested by the Customer at a rate agreed between the parties.

10.3 An exit strategy plan shall be jointly drafted by the Customer and Interoute.

10.4 During the exit transition up to the end date of the Services Interoute shall:

10.4.1 continue to provide the Services to the Customer subject to payment by the Customer of the relevant Charges.

10.4.2 provide the Customer with access to such records and documentation as reasonably required to ensure continuity of the Services to the Customer and for the purpose of the transfer of the Services relating to the Services to the new supplier (to the extent permitted by applicable law).

10.4.3 facilitate the transfer of any knowledge of the Customer that is reasonably required to ensure continuity of the Services, to the extent permitted by applicable law.

10.4.4 answer all reasonable questions related to the Customer's Services, posed by the Customer reasonably required to ensure continuity of the Services;

10.4.5 withhold no data related to the Services from the Customer that is reasonably required to ensure continuity of the Services.

11. Force Majeure

11.1 Under no circumstances shall the Customer be entitled to rely upon Force Majeure in relation to any obligation to pay Charges in accordance with the Agreement.

11.2 A Party shall not be deemed in default of any of its obligations under this Agreement if, and to the extent that, performance of such obligation is prevented or delayed by acts of God or public enemy, civil war, insurrection or riot, fire, flood, explosion, earthquake, labour dispute causing cessation slowdown or interruption of work, national emergency, act or omission of any governing authority or agency thereof, inability after reasonable endeavours to procure equipment, data or materials from suppliers, damage or disruption to subsea cables, or any other circumstances beyond its reasonable control ("Event of Force Majeure"), provided that such Event of Force Majeure is not caused by the negligence of that Party, and that Party has notified the other in writing of the Event of Force Majeure.

11.3 If either of the parties becomes aware of an Event of Force Majeure which gives rise to or which is likely to prevent the performance of any obligations on its part it shall as soon as reasonably possible serve notice in writing on the other party specifying the nature and extent of the circumstances giving rise to Force Majeure.

11.4 Upon the occurrence of an Event of Force Majeure, the time for performance shall be extended for the period of delay or inability to perform due to such occurrence, but if an Event of Force Majeure continues for a continuous period of more than fifteen (15) consecutive calendar days the other Party shall be entitled to terminate this Agreement.

12. Disaster Recovery Plan

12.1 For the purposes of compliance with clause 6 of Part B of the Call-Off Contract any disaster recovery and/or business continuity plan needs to be agreed between the Parties.

13. Intellectual Property Rights

13.1 Each Party will defend and hold the other Party harmless against any claim, suit or proceeding brought against that Party so far as it is based on any actual or threatened infringement of any Intellectual Property Rights by it, provided that it is given prompt notice in writing of any such claim and is given full authority and such information and assistance as is reasonably necessary for the defence of such claim.

13.2 The Customer has no right to an indemnity under the Call-Off Contract to the extent that the negligence of the Customer, its Affiliates or customers or their respective officers, employees or agents has contributed to the loss, demand, claim, damage, cost, expense or liability for which the Customer is claiming an indemnity.

13.3 Interoute shall have no Liability in respect of any alleged infringement which is based on the sale or use of any Service in combination with any other products not supplied by Interoute (unless expressly agreed by Interoute).

13.4 Interoute shall have no Liability in respect of any unauthorised modifications, changes or alterations by the Customer or its agents of the Services supplied by Interoute, other than in respect of modifications, changes or alterations carried out by Interoute.

14. Software

14.1 If and to the extent that the Customer requires the use of Licensed Software in order to use the Services, the Customer will be provided with a non-exclusive non-transferable licence for the Term to use such Licensed Software solely for its internal purposes and solely to the extent required to use the Services. To the extent such Licensed Software is sourced from a third party provider, such licence shall be subject to the terms of the applicable software licence embedded in the relevant software.

14.2 Customer will not, and shall use all its reasonable endeavours to ensure that others do not:

a. obtain or claim any ownership in any Licensed Software (or in any derivation thereto or improvement thereof);

b. copy the Licensed Software except as agreed in writing by Interoute and in accordance with the terms of the applicable software licence;
c. save as permitted by law, reverse engineer, decompile or disassemble Licensed Software;
d. sell, lease, licence or sublicence the Licensed Software;
e. create, write or develop any derivative software or any other software based on the Licensed Software; or
f. take any action prohibited by the applicable software license.

15. Staff

15.1 The parties consider that the Transfer Regulations will not apply on the commencement or cessation (in whole or in part) of the provision of the Services by Interoute under the Agreement.

15.2 The Customer shall indemnify Interoute and keep Interoute indemnified (or procure that any Outgoing Service Provider or Incoming Service Provider (as applicable) shall indemnify Interoute and keep Interoute indemnified) from and against all Employment Liabilities arising out of or in connection with any claim or allegation made by any person (or representative(s) of such person) that they have rights against Interoute or any supplier of Interoute by virtue of the application of the Transfer Regulations (including any claim in respect of the termination of such person's employment or any alleged failure by the Customer, the Outgoing Service Provider, the Incoming Service Provider, Interoute or its supplier to comply with any information and consultation obligations).

16. Liability

In addition to the provisions of Clause 24 of Part B of the Call-Off Contract (Liability):

16.1 Except as otherwise set forth in this Agreement, Interoute shall have no Liability (a) for any transaction, which the Customer may enter into with a third party using the Services; (b) for the contents of any communications transmitted via Services or for any information or content on the Internet.

16.2 Interoute gives no warranties, nor makes any representations or other agreements, express or implied with respect to the Services in particular Interoute does not warrant that any Service shall be uninterrupted or fault free or that such Service will interoperate effectively with Customer Equipment, or Customer’s network or services.

16.3 These terms are in lieu of all other conditions, warranties or other terms concerning the supply or purported supply of, failure to supply or delay in supplying the Services which might but for this Clause 16 have effect between Interoute and the Customer or would otherwise be implied into or incorporated into this Agreement or any collateral contract, whether by statute, common law or otherwise, all of which are hereby excluded (including, without limitation, the implied conditions, warranties or other terms as to satisfactory quality, fitness for purpose or as to the use of reasonable skill and care).

16.4 Subject to Clause 16.5, neither Party shall have any Liability for (a) loss of revenue; (b) loss of actual or anticipated profits; (c) downtime costs (d) loss of contracts; (e) loss of the use of money; (f) loss of anticipated savings; (g) loss of business; (h) loss of opportunity; (i) loss of goodwill; (j) loss of reputation; (k) loss of, damage to or corruption of data; or (l) any indirect or consequential loss and such Liability is excluded whether it is foreseeable, known, foreseen or otherwise. For the avoidance of doubt, 16.4 (a) – 16.4 (l) apply whether such losses are direct, indirect, consequential or otherwise.

16.5 Nothing in this Clause 16 shall exclude or limit the Liability of the Customer to:

a. Pay the Charges and/or
b. Repair (or if repair is not practicable, replace) any tangible physical property intentionally or negligently damaged by the Customer or its employees or agents.

16.6 Except where explicitly stated otherwise in the Call-Off Contract or in the applicable Additional Terms, and subject to Clauses 16.5, 16.7, 16.8 and 16.9, the Liability of each Party for any claim, loss, expense, or

damage under this Agreement shall be limited to the equivalent of the total amount of Charges owed by Customer to Interoute in the twelve months immediately preceding the cause of action. If the Service(s) have been in service for less than twelve (12) months, then Liability shall be limited to the estimated Charges for twelve (12) months of service. The Liability set out in this Clause 16.6 is subject to a maximum of Euro 250,000 for any one incident or a series of related incidents and to Euro 500,000 for all incidents in any period of twelve (12) months.

16.7 The limitation of Liability under Clause 16.6 above has effect in relation both to any Liability expressly provided for under this Agreement and to any Liability arising by reason of the invalidity or unenforceability of any term of this Agreement.

16.8 Nothing in this Agreement shall exclude or limit either Party's Liability:

a. for fraud or fraudulent misstatement;
b. for death or personal injury;
c. in relation to the intellectual property indemnity set out in Clause 13; or
d. for breach of confidentiality;
e. for any other Liability which cannot be excluded or limited by applicable law.

16.9 The Customer shall indemnify and hold harmless Interoute against all actions, losses, costs, damages, awards, expenses, fees (including legal fees incurred and/or awarded against Interoute) proceedings, claims or demands in any way connected with this Agreement, including claims, brought or threatened against Interoute by a third party related to content or arising out of the use by Customer of the Services, or any wilful or negligent act or omission of the Customer or Customer's customer(s) and /or agents. The Customer shall also provide, at the Customer's sole expense, Interoute with full authority, information and assistance as is reasonably necessary for the defence, compromise or settlement of such claim.

16.10 Customer hereby agrees that it shall use its best endeavours to mitigate any losses that may arise from this Agreement.

16.11 The Parties agree that Clause 16 represents a fair and equitable position.

16.12 The Customer acknowledges that Interoute would not enter into the Agreement at the prices herein without the foregoing limitations of liability. Each Party acknowledges that the allocation of risk in the Agreement (including the exclusions and limitations set out in these Supplier Terms) has been freely negotiated at arm's length and is regarded by it as reasonable.

17. DATA PROTECTION

17.1 The customer acknowledges and agrees that Interoute may, in the course of performing its obligations under this agreement, process personal data on behalf of the Customer. Interoute undertakes to the Customer that it shall process the customer personal data only in accordance with Interoute's Data Processing Agreement which sets out the data protection provisions that apply so as to meet the requirements of Applicable Law (as defined in the Data Processing Agreement) in relation to the protection of personal data. The Parties shall comply with the terms of the Data Processing Agreement.

17.2 In respect of services which involve processing of personal data the parties will enter a Data Processing Agreement ("**DPA**") as per the template under Appendix 2. As regards the Cloud Connect and Internet Access services, Interoute acts as a telecoms service provider for all data transmitted and processes this data for the sole purpose of transmitting these communications. Interoute has no access to user level data and carries out no data processing activities on this data.

17.3 In addition to any other responsibilities and obligations set out in the Additional Terms for Virtual Data Centre Service contained in Schedule 2N, where Customer is provided VDC Self Care the Customer shall be responsible for the following:

17.3.1 Design and implement a secure, fault resilient, solution in line with the Customer's business requirements. This includes location of data, encryption of data, access to data, firewall rules, network access and server topology.

17.3.2 Design and implement a data backup, retention and restore policy in line with the Customer's business requirements. Type of (e.g. Block level or application aware backups), frequency and location of backups and procedures to restore.

17.3.3 Design and implement a patch and anti-virus policy in line with the Customer's business requirements

17.3.4 Design and implement a suitable administrator management access policy for administrators.

17.4 In addition to any other responsibilities and obligations set out in clause the Additional Terms for Hosted Skype for Business contained in Schedule 2U, where Customer is provided Hosted Skype for Business the Customer shall be responsible for the following:

17.4.1 Managing the Service in line with the associated technical description or Statement of Work .

17.4.2 Design, implement and manage the Customer's active directory to support the Hosted Skype for Business Service in line with the Customer's business requirements in a secure, and fault resilient manner.

17.4.3 Provide where required for direct active directory integration named active directory accounts for Interoute's support engineers.

17.4.4 Any customer performed adds, changes and deletions of user accounts.

17.5 Notwithstanding anything to the contrary foreseen in section k) of clause 16.4 of these Supplier Terms, where Interoute provides Virtual Data Centre Service and Hosted Skype for Business:

17.5.1 Interoute's liability for loss of or corruption of or damage to data shall be limited to the loss or corruption of or damage to Customer data arising as a result of a wilful act or gross negligence on the part of Interoute subject to limits of liability set forth in the Call-Off Contract and these Supplier Terms and subject to the Customer's obligation to mitigate the consequences of such a loss through the maintenance of appropriate security, protection and backup of such data.

17.5.2 Where Interoute provides Managed VDC Services and in respect of any other loss or corruption of or damage to data attributable to an act or omission of Interoute, which does not cause a breach under the Data Processing Agreement between the parties, Interoute's liability is limited as follows:

17.5.2.1 To restore the data (at its own cost), subject to the Recovery Time Objective and the Recovery Point Objective from the last successfully carried out backup.

17.5.2.2 If the last successfully carried out backup is not the last scheduled backup, in the event of a loss of data that is caused by or attributable to an act or omission of Interoute, then Interoute shall also be liable for the Customer's costs in recovering data up to the last scheduled backup.

18. Compliance with Laws

18.1 Customer shall use the Services in accordance with and subject to all provisions of applicable law and any order or determination of any competent authority.

18.2 Customer shall obtain all necessary licences, approvals, permits and consents including building permits and landlords' consent required by any applicable governmental or regulatory authority or body necessary for Customer to use the Services.

18.3 Customer shall at all times use the Services in accordance with Interoute's Acceptable Use Policy.

18.4 In addition to the above the following shall apply to address export control/sanctions issues:

a. **Termination if contract affected by sanctions**
Interoute shall be entitled to terminate this Agreement with immediate effect by giving notice in writing to Customer in the event of any of the following: if Restrictive Sanctions measures adopted by the United Nations or implemented by the European Union, a European Union Member State ("Member State"), or the United States, directly or indirectly, affects the ability of the Parties to perform their duties;

b. **Warranty for economic sanctions and for end-use controls**
The Customer warrants and represents to Interoute that (i) the performance of their duties will not result in any funds, economic resources, or wider benefits being made available, directly or indirectly, to any individual, entity, or body designated under Restrictive Sanctions measures adopted by the United Nations or implemented by the European Union, a Member State, or the United States, or any party acting on behalf or at the direction of such an individual, entity, or body and (ii) it will not sell, export, transfer, re-export, or re-transfer of any goods, works, or services provided by Interoute which may be intended for a "Relevant End-use" unless prior authorisation by a competent authority has been granted. A "Relevant End-use" includes: military use; or, use in connection with chemical, biological or nuclear weapons or other nuclear explosive devices or the development, production, maintenance or storage of missiles capable of delivering such weapons; or, use in connection with Iran's enrichment-related, reprocessing, or heavy water-related activities;

c. **Cooperation with compliance**
Where Interoute is required by a competent authority to provide records and/or information, Customer upon request by Interoute, shall promptly provide Interoute with all information, pertaining to the particular end customers, the particular destinations and the particular end use of the goods, works and services provided by Interoute;

d. **Indemnity for actions by counter-party**
Customer shall indemnify and hold harmless Interoute from and against any claim, proceeding, action, fine, loss, cost and damages arising out of or relating to any non-compliance of Customer with (i) Clause 11.4 lit. b above or (ii) with international sanctions measures adopted by the United Nations or implemented by the European Union, a Member State, or the United States and shall compensate Interoute for all losses and expenses resulting thereof.

19. Anti-Bribery and Corruption

19.1 In addition to the provisions of Clause 8.13 - 8.17 of the Framework Agreement:

19.2 The Customer warrants and represents that it has not and will not carry out any Prohibited Act as defined in the the Call-Off Contract Contract.

19.3 The Customer undertakes to advise the General Group Counsel of Interoute immediately if it suspects that any director, employee, agent or associates of the Customer requesting or soliciting any bribe or otherwise conducting themselves in a manner that could a Prohibited Act as defined in the Call-Off Contract.

19.4 The Customer represents and warrants that it has adequate procedures in its business to prevent bribery occurring.

19.5 Interoute may, at any time and from time to time audit the Customer's procedures to ensure that it is satisfied that such procedures are adequate. If the procedures are found to be materially inadequate, the Customer undertakes to improve its procedures and in such event the costs of such audit and improvement in its procedures shall be to the sole account of the Customer.

20. Confidentiality

20.1 Without prejudice to any other rights and remedies that the disclosing party may have, the receiving party agrees that if Confidential Information is used or disclosed or threatened to be used or disclosed other than in accordance with the terms of the Agreement, the disclosing party shall, without proof of special

damage, be entitled to seek an injunction, specific performance or other equitable relief for any actual or threatened breach of the confidentiality provisions of the Agreement.

21. Audit

21.1 The nature and scope of any audit or inspection conducted pursuant to the Agreement shall be reasonable, proportionate and agreed in advance by both Parties.

21.2 Interoute will authorise Customer and any Customer authorised auditors or advisors to perform audits solely related to the Services provided by Interoute to Customer under this Agreement (excluding access to any documentation, configuration facilities or other information of Interoute not directly associated with the Services).

- The Customer shall provide at least 10 Working Days' notice of its intention to conduct an audit.
- The number of audits shall be limited to one (1) per year.
- The Customer shall comply with the defined operational procedures for access to Interoute facilities.

21.3 Subject to the Customer's obligations of confidentiality, Interoute shall provide the Customer (and its auditors and other advisers) with all reasonable co-operation, access and assistance in relation to each audit.

22. Assignment

22.1 The Service is provided for the Customer's use and the use of its Affiliates, employees, sub- contractors, agents and customers only (subject always to such use being in accordance with the terms of the Agreement) and the Customer undertakes not to otherwise resell, hire or lease the Service to any third party without the prior written consent of Interoute. The Customer is and shall remain liable to Interoute for any act or omission of any of its Affiliates, employees, sub-contractors, agents, and/or customers.

22.2 Save as provided in Clause 8.35 of the Framework Agreement, the Customer may not assign or delegate its rights or obligations under the Call-Off Agreement without the prior written consent of Interoute. Any such permitted assignment by the Customer shall be in writing on terms agreed by Interoute to any of its Affiliates provided that the financial standing of such Affiliate is equal to or of higher financial standing to the Customer and provided that the Customer shall procure that such assignee shall assign those rights to another Affiliate of the Customer on the assignee ceasing to be an Affiliate of the Customer. The cost of any assignment shall be for the account of the Customer.

23. Dispute Resolution

23.1 Subject to either party's rights and remedies under and in accordance with the Agreement, prior to initiating any proceedings in the English courts, the parties agree to follow the procedure set out in the Framework Agreement. Either party may trigger the application of the Dispute Resolution Procedure by serving notice in writing of any such Dispute (setting out in reasonable detail the nature of the Dispute) ("**Dispute Notice**"). In the case of Dispute Notices to be sent to Interoute, all such Dispute Notices shall be marked for the attention of the Interoute Account Manager.

23.5 All rights of the parties in respect of the Dispute during the dispute resolution procedure shall be and remain fully reserved, and the entire procedure involving authorised representatives of the parties shall be strictly confidential and shall be conducted "without prejudice" to any subsequent proceedings.

23.6 If a Dispute is resolved pursuant to the dispute resolution procedure, the Customer and Interoute shall create a written memorandum of their agreement in relation to the Dispute which shall be signed by both the Customer and Interoute and following which the parties shall, as soon as reasonably practicable, execute such documents and do such things as may be necessary to give effect to such agreement.

23.7 The dispute resolution procedure will not prevent either party from:

- Seeking injunctive relief in the case of any breach or threatened breach by the other of any obligation of confidentiality or any infringement by the other of the first- named party's Intellectual Property rights; or
- Commencing any proceedings where this is reasonably necessary to avoid any loss of a claim due to the rules on limitation of actions.

24. Insurance

In addition to clause 9 of Part B of the Call-Off Contract:

24.1 Each Party will maintain in effect at all times during the performance of this Agreement such insurance policies with a reputable insurance company as it is required to hold under applicable law and such other policies as a prudent business conducting similar operations in the region would maintain. Coverage limits will be sufficient to cover the Party's Liabilities under this Agreement.

24.2 With specific regard to Equipment, during the continuance of this Agreement, it shall be the Customer's responsibility to insure at its own expense, and keep insured (i) Equipment which is on Customer Premises and (ii) Customer Equipment on Interoute premises, in each case with a reputable insurer against loss, theft, damage or destruction howsoever arising (unless such damage or destruction is caused by Interoute or its agents) at an amount not less than the full replacement value of the Equipment. Such Equipment and Customer Equipment shall at all times be at the Customer's risk.

24.3 Each Party will, at the request of the other Party, provide copies of such documentation as the requesting Party reasonably requires in evidence of the other Party's compliance with this Agreement.

25. Press and public announcements

25.1 No press or public announcements, circulars or communications relating to this Agreement or the subject matter of it shall be made or sent by either of the Parties without the prior written approval of the other Party such approval not to be unreasonably withheld or delayed.

26. Miscellaneous

26.1 No Failure or delay of either party in exercising its rights hereunder (including the right to require performance of any provision of the Agreement) shall be deemed to be a waiver or release of such rights. Any waiver or release must be specifically granted in writing signed by the party waiving its rights and shall:

26.1.1 be confined to the specific circumstances in which it is given;

26.1.2 not affect any other enforcement of the same or any other right; and

26.1.3 (unless it is expressed to be irrevocable) be revocable at any time in writing.

Any single or partial exercise of any right, power or remedy provided by law or under the Agreement shall not preclude any other or further exercise of it or the exercise of any other right, power or remedy.

26.2 If at any time any provision of the Agreement is or becomes illegal, invalid or unenforceable in any respect under the law of any jurisdiction that shall not affect or impair:

26.3 the legality, validity, or enforceability in that jurisdiction of any other provision of the Agreement; or

26.3.1 the legality, validity, or enforceability under the law of any other jurisdiction of that or any other provision of the Agreement.

26.4 All work performed by Interoute under the Agreement shall be performed as an independent contractor and not as an agent of the Customer and neither party shall be, nor represent itself to be, the employee, agent, representative, partner or joint venture of the other. Neither party shall have the right or authority to assume or create an obligation on behalf of or in the name of the other or to otherwise act on behalf of the other. The performing party shall be responsible for its employees' compliance with all applicable laws, rules, and regulations while performing work under the Agreement.

26.5 No modification, amendment or other Change may be made to these Supplier Terms or to Agreement or any part thereof unless reduced to writing and executed by authorised representatives of Interoute and the Customer. Unless expressly so agreed, no modification or variation of the Agreement shall constitute or be construed as a general waiver of any provisions of the Agreement, nor shall it affect any rights, obligations or liabilities under the Agreement which have already accrued up to the date of such modification or waiver, and the rights and obligations of the parties under the Agreement shall remain in full force and effect, except and only to the extent that they are so modified or varied.

26.6 Save to the extent expressly set out in this Agreement, nothing in this Agreement shall vest in or confer on the Customer:

a. any patent or any other right or licence in the Intellectual Property Rights arising from or relating to any apparatus, system or method used by Interoute or by the Customer in connection with the use of the Services; or
b. any ownership or property rights or liens of any nature in or over Equipment or property, including the Interoute Network.

All rights granted hereby and obligations entered into under this Agreement are purely contractual. Nothing in this Agreement shall grant to the Customer any ownership, proprietary or possessory rights in any of the subject-matter of the Agreement.

27. Entire Agreement

27.1 With effect from the date of the Call-Off Agreement all Services shall be provided solely in accordance with the terms of the Agreement and all prior agreements and understandings between the parties in relation to the same shall be deemed terminated from the date thereof. Save in respect of rights and liabilities arising prior to such date, all such prior agreements and understandings shall cease to be of effect from the date of signature of the Agreement. In no event shall the pre-printed terms and conditions found on any Customer purchase order, acknowledgement, or other form be considered an amendment or modification of the Agreement, even if such documents are signed by representatives of both parties; such pre-printed terms and conditions shall be null and void and of no force and effect.

27.2 Neither party shall have any liability or remedy in tort (including negligence) in respect of any representation, warranty or other statement (including any contained in the Agreement) being false, inaccurate or incomplete unless it was made fraudulently.

27.3 Each party acknowledges and agrees that in entering into the Agreement or in amending any part of the Agreement, it has not relied on any statement, representation, warranty, understanding, undertaking, promise or assurance (whether negligently or innocently made) of any person (whether party to the Agreement or not) other than as expressly set out in the Agreement. Each party irrevocably and unconditionally waives all claims, rights and remedies which but for this clause it might otherwise have had in relation to any of the foregoing.

28. Notices

28.1 Any notice given or made under the Agreement or required by law or regulation shall be in writing and in English and signed by or on behalf of the party giving it and shall be served by sending an email in accordance with clause 8.63 of the Framework Agreement, hand delivering it or sending it by prepaid first class recorded delivery (including special delivery) or first class recorded post or, in the case of an address for service outside the United Kingdom, by prepaid international recorded airmail, to the registered office address of the relevant party and marked for the attention of the Company Secretary (or as otherwise notified by that party under this clause). Any notice shall be deemed to have been received at the time of delivery.

28.3 Either party may at any time notify the other of a change of address or person for the purposes of the serving of notices.

Appendix 1

List of Additional Terms applicable to the Services

The text of the following Additional Terms are available at www.interoute.com/legal.

Service	Applicable Additional Terms
Interoute One Bridge	Schedule 2B
Interoute One	Schedule 2K
Hosted Skype for Business	Schedule 2U(c)
Virtual Data Centre (VDC)	Schedule 2N VDC Definitions Annex VDC Managed Operations Annex VDC Self-Care Operations Annex VDC SLA Annex VDC Dedicated Equipment Annex Security Annex – PCI DSS Compliance Commitments
Enterprise Edge	Schedule 2EDGE
Cloud Connect	Schedule 2V
Object Storage	Schedule 2Q
Two Factor Authentication	Security Annex – Two Factor Authentication Service
Next Generation Firewalls	Security Annex – Firewall Service
Content Filtering	Security Annex – Content Filtering Service
DDoS Protection	Security Annex – DDoS Protection
Intrusion Prevention	Security Annex – IPS Service
Internet Access	Schedule 2F

Appendix 2

Data Processing Agreement ("DPA")

This Data Processing Agreement (the "Agreement") is made between:

(1) **[Full name of legal entity]**, a company incorporated under the laws of [•] (registered number: [•]) with its registered office at [•] (the "**Customer**"); and

(2) [**Name of Interoute entity**] a company incorporated under the laws of [•] (registered number: [•]) with its registered office at [•] and which has signed a master services agreement with the Customer (the "**Interoute**")

Each a "**party**" and together the "**parties**"

RECITALS:

a. The Customer and Interoute have entered into a master services agreement dated [ ] or Customer accepted Interoute's webterms ("**the MSA"**) for the provision of one or more communications services (each a "**Service**", together **the** "**Services**").

b. When supplying the Services Interoute will process customer personal data on the Customer's behalf.

c. The parties have agreed to enter into this Agreement in order to confirm the data protection provisions relating to their relationship and so as to meet the requirements of applicable law in relation to the protection of personal data.

1. INTERPRETATION

1.1 For the purposes of this Agreement:

1.1.1 "**Applicable Law"** means any law or regulation relating to privacy and data protection which applies to a party to this Agreement (including the General Data Protection Regulation (EU) 2016/679);

1.1.2 **"Customer Personal Data"** means personal data processed on behalf of the Customer for the purpose of providing the Services;

1.1.3 **"Data Controller"** means the entity which alone or jointly with others determines the purposes and means of the processing of personal data;

1.1.4 **"Data Processor"** means the entity which processes personal data on behalf of the data controller;

1.1.5 **"EEA"** means the European Economic Area (as defined by the agreement on the European Economic Area of 2 May 1992 as amended and supplemented by relevant instruments from time to time);

1.1.6 **"GDPR"** means the General Data Protection Regulation (EU) 2016/679;

1.1.7 **"Personal Data"** shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable 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; and

1.1.8 "**Processing of personal data"** (**"Processing"**) means any operation or set of operations which is performed upon personal data or on sets of personal data, whether or not by automatic means, such as collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

1.2 With respect to the parties' rights and obligations under this Agreement, the parties agree that the Customer is the data controller and Interoute is the data processor in relation to the Customer Personal Data.

1.3 The subject matter of the data processing under this Agreement is the performance of the Services and the Processing will be carried out for the duration of the MSA. Annex 1 sets out the nature and purposes of the Processing by Interoute under this Agreement, the types of Personal Data Processed by Interoute under this Agreement and the categories of data subjects to which such Personal Data relates.

1.4 References to the singular shall include the plural and vice versa.

1.5 Capitalised terms not defined herein shall have the meaning ascribed to them in the MSA.

In consideration of their mutual promises, it is agreed between the parties as follows:

2. INTEROUTE OBLIGATIONS

2.1 Interoute undertakes to the Customer that it shall:

2.1.1 Process the Customer Personal Data only in accordance with the Customer's written instructions from time to time, including as set out in Annex 1 of this Agreement, unless required to do otherwise by law, in which case, to the extent permitted by law, Interoute shall inform the Customer of this legal requirement prior to carrying out the processing;

2.1.2 implement appropriate technical and organisational measures, as set out in Annex 2 of this Agreement(which Interoute may update from time to time), to protect the Customer Personal Data against unauthorised or unlawful processing and accidental destruction or loss;

2.1.3 ensure that any of its personnel required to process the Customer Personal Data are informed of the confidential nature of such data and require such personnel to comply with confidentiality obligations in respect of such Customer Personal Data;

2.1.4 at the Customer's cost and expense, and taking into account the nature of the Processing and the information available to Interoute, provide such information and such assistance as the Customer may reasonably require and within timescales reasonably specified by the Customer to assist the Customer to comply with its obligations under Applicable Law, such asassisting the Customer to:

2.1.4.1 comply with its security obligations;

2.1.4.2 subject to clause 2.1.5 below, discharge its obligations to respond to requests relating to the exercise of data suject rights;

2.1.4.3 comply with its obligations to inform data subjects about serious personal data breaches;

2.1.4.4 carry out a data privacy impact assessment. Such assistance will be provided in accordance with the audit terms specified in the MSA;

2.1.4.5 consult with the supervisory authority following privacy impact assessment;

2.1.4.6 make the Customer Personal Data available to the Customer if and to the extent such Customer Personal Data is not accessible to the Customer through the Services.

2.1.5 to the extent lawfully able to do so, notify the Customer without undue delay if it receives from any data subject whose Personal Data forms part of the Customer Personal Data:

2.1.5.1 any communication seeking to exercise rights conferred on the data subject by the Applicable Law. The Customer is responsible for responding to requests relating to the exercise of data subjects rights under the Applicable Law. If Interoute receives a data

subject request (DSAR) it shall promptly redirect the data subject to the Customer and inform the Customer of this without undue delay;

2.1.5.2 any complaint or any claim for compensation arising from or relating to the processing of the Customer Personal Data.

2.1.6 notify the Customer without undue delay after becoming aware of any breach of security that results in the accidental, unauthorised or unlawful destruction, loss, alteration or unauthorised disclosure of, or access to Customer Personal Data;

2.1.7 make available to the Customer all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR by way of the use of external auditors to verify the adequacy of its security measures. This audit: (a) will be performed at least annually; (b) will be performed according to ISO 27001 standards or such other alternative standards that are substantially equivalent to ISO 27001; (c) will be performed by independent third party security professionals at Interoute's selection and expense; and (d) will result in the generation of an audit report ("Report"), which will be Interoute's confidential information. At the Customer's written request, Interoute will provide the Customer with the related certificate and a description of the scope so that the Customer can reasonably verify Interoute's compliance with this clause 2.1.7;

2.1.8 on expiry or termination of this Agreement, upon receipt of a written request of the Customer to be delivered at least fourteen (14) days prior to such expiry or termination of this Agreement, at the choice of the Customer, either promptly and securely return the Customer Personal Data to the Customer or (unless its continued storage by Interoute is required by law) promptly and securely delete the Customer Personal Data;

2.1.9 not transfer any of the Customer Personal Data to a country outside the EEA without the prior written consent of the Customer and in accordance with its documented instructions;

2.1.10 not disclose Customer Personal Data to any third party save as permitted by this Agreement or as subsequently directed by the Customer. This clause shall not prevent Interoute from disclosing Customer Personal Data if required to do so for any of the reasons under clause 25.3 of the MSA.

3. CUSTOMER OBLIGATIONS

3.1 The Customer shall comply at all times with Applicable Law in relation to the processing of Customer Personal Data in connection with this Agreement and the Services.

4. SUB PROCESSING

4.1 The Customer specifically consents to Interoute engaging Associated Companies within the EEA, from time to time as sub-contractors to process the Customer Personal Data in order to assist Interoute to carry out its processing activites (**"Associated Company Sub-processors"**).

4.2 The Customer agrees that Interoute may engage third parties that are not Associated Company Sub-processors as sub-contractors to process the Customer Personal Data in order to assist Interoute to deliver the Services (**"Third Party Sub-processors**") provided that:

4.2.1 Interoute shall provide the Customer with details of any Third Party Sub-Processors engaged by Interoute for the provision of the processing activities;

4.2.2 Interoute shall give the Customer thirty (30) days' notice in writing of any intended changes concerning the addition or replacement of any Third Party Sub-Processor during which period the Customer may raise objections to the Third Party Sub-Processor's appointment; and

4.2.3 Interoute shall use reasonbale endeavours to impose obligations in relation to the Processing of the Customer Personal Data that are equivalent to those imposed on Interoute under this Agreement on any sub-processor;

and, for the avoidance of doubt, where any sub-processor fails to fulfil its obligations under any sub-processing agreement or under Applicable Law Interoute will remain fully liable to the Customer for the fulfilment of its obligations under this Agreement.

4.3 Where the Customer elects to use a virtual data centre which is not located in the EEA or a country in respect of which an adequacy finding is in place under Article 45 GDPR, the Customer shall enter into Standard Contractual Clauses (in the form adopted by decision 2010/87/EU of 5 February 2010) with the Associated Company of Interoute which provides that virtual data centre. Such election shall be deemed consent under clause 2.1.9.

5. WARRANTIES AND INDEMNITY

5.1 The Customer represents and warrants that the security measures set out in Annex 2 ensure a level of security appropriate to the risks presented by the Processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation.

5.2 The Customer will indemnify Interoute against all actions, losses, costs, damages, awards, expenses, fines, fees proceedings, claims or demands in any way connected with this Agreement brought against Interoute by a data subject or any other third parties arising out of or in connection with the Customer's breach of its representation and warranty contained in clause 5.1 of this Agreement.

6. INSTRUCTIONS

6.1 Interoute shall comply with all Applicable Laws in its role as a Data Processor including in respect of security requirements. Interoute is not responsible for complying with laws applicable to the Customer as the Data Contoller. The Customer shall comply with the Applicable Laws that apply to the Customer as a Data Controller.

6.2 Where the Customer is itself acting as Data Processor for a Customer Associated Company, the Customer represents and warrants that it is authorised by the Data Controller to instruct Interoute to process the Customer Personal Data as set out herein.

6.3 The Customer shall indemnify Interoute against all actions losses, costs, damages, awards, expenses, fines, fees, proceedings, claims, or demands in any way connected with this Agreement brought against Interoute by a data subject or any third party arising out of or in connection with Customer's breach of the representation and warranty given in clause 6.2 directly above.

6.4 The Parties agree that whenever in this Agreement the Data Controller is not the Customer but another Associated Company of the Customer:

a. any information, instruction, consent, permission or other authorisation that is required to be given by the Data Controller; or

b. any information or notification that is required to be given by Interoute to the Data Controller

shall be given by or provided to, as the case may be, the Customer on behalf of such Data Controller or Interoute. The Customer warrants that: (a) the Customer has the required written authorisation from the Data Controller to give any such information, instruction, consent, permission or other authorisation on behalf of such Data Controller and or to receive any information or notification on behalf of such Data Controller from Interoute; (b) this Agreement complies with any law applicable to the relevant Customer's Associated Company and that all data protection requirements arising from such applicable law are being effectively satisfied hereunder; (c) the Customer's Associated Company has appointed the Customer as their agent for the purpose of any liability and/or responsibility that may arise out of or in connection with this Agreement; and (d) this Agreement fulfils the requirements of Article 28.4 of the GDPR.

6.5 The Customer is responsible for notifying Interoute of any rule, law or regulation relating to data Processing that is specific to the requirements of their industry and/or if there is a change in the type of Personal Data, set out in Annex 1, to be Processed by Interoute under this Agreement. If such change requires an amendment to the technical and organisational measures captured in Annex 2, the Parties agree that Interoute may in order to comply with its obligations under the GDPR as a Data Processor update Annex 2 as required . If so required, the Parties shall meet and apply good faith efforts to agree on any amendments to Annex 2 in writing. The Customer acknowledges and agrees that changes to Annex 2 may attract additional Charges.

6.6 If a supervisory authority imposes fines, penalties, sanctions, liabilities or other remedies (a "Regulatory Sanction") upon the Customer as a result of a breach by Interoute of its obligations under this Agreement, Interoute shall not be liable for any element of or an aggravation or increase to the Regulatory Sanction which arises directly or indirectly as a result of the Customer's acts or omissions.

6.7 If a supervisory authority imposes a Regulatory Sanction upon Interoute as a result of a breach by the Customer of its obligations under this Agreement, the Customer shall not be liable for any element of or an aggravation or increase to the Regulatory Sanction which arises directly or indirectly as a result of Interoute's acts or omissions.

6.8 The Customer acknowledges that Interoute is reliant on the Customer for direction as to the extent to which Interoute is entitled to use and process the Customer Personal Data. Consequently, Interoute will not be liable for any claim brought by a data subject arising from any action or omission by Interoute, to the extent that such action or omission resulted directly from the Customer's instructions.

7. MISCELLANEOUS

7.1 In the event of any conflict or inconsistency between this Agreement and the Master Services Agreement or the terms and conditions of any Purchase Order, this Agreement shall prevail, but only to the extent of such conflict or inconsistency.

IN WITNESS WHEREOF, the parties' authorised signatories have duly executed this Agreement, including its appendices

FOR THE CUSTOMER

_____ _____

Name of signatory **Date**

_____

Position

_____

Company

FOR INTEROUTE

_____ _____

Name of signatory **Date**

_____

Position

_____

Company

Annex 1

Data Processing Instructions for each applicable service

1. Interoute One Bridge

Interoute One Video Connect and Video Trunk

Interoute One Video Connect provides customers the ability to register their video endpoints to the Interoute One Bridge conferencing service. Interoute One Video Trunk provides customers with a SIP trunk into the Interoute One Bridge conferencing service. Both services are to provide voice and video communication services.

Purpose of the data processing

Purpose of customer data processing
The Video Connect and Video Trunk services store IP addresses of customer video endpoints or gateway equipment to enable them to register the endpoints and equipment so that video calls can be made into the Interoute video platform. When calls are made, the system records logs and call detail records which may contain the name of the calling and called video endpoints.

Purposes of data processing for delivery of the service
For troubleshooting purposes, the records identified above can be inspected by Interoute engineers and system supplier engineers. This is only done on a case by case basis with the agreement of the customer and files are transferred to 3rd parties only if necessary and only via encrypted methods.

There are certain specific data types which are identified below which are processed by the service. The purpose of this processing is for the successful provision and management of the service itself.

Categories of data processed

Customer Content Data
Any type of type of data including any personal data in electronic form could be stored (and therefore processed) as this is a feature of the service. Individuals will often use the service to share content generated by themselves or others. This and the service is able to store voice and video calls.

Data Processed Automatically to Deliver the Service
To deliver the service Interoute also needs to process certain types of data which may be personal. This will include communication addresses and computer device identifiers such as:

SIP Address
Which can be an IP address, E.164 number, or registered name
IP addresses
Such data will also be logged by the system as will certain operating system events.

Video Connect and Trunk services will process the above data to control access to the service at our Session Border Controllers. Interoute stores and processes this as authenticating information to protect service security. To administer the service Interoute engineers are also able to inspect recorded information for trouble-shooting purposes.

Storage and Transmission
Customer endpoint data will normally be processed and stored in the Interoute Telepresence Management Suite and the Session Border Controllers which are in the Interoute Video POP locations in EU, US, HK. Customer traffic entering the video core network must always traverse an edge server or a session border controller (for SIP or H.323 sessions) before being routed onwards to its destination.

For troubleshooting and reporting purposes data may be moved from the Video POP locations and processed and stored elsewhere within the EU, US, HK. This is only processed with the consent of the customer who remains the Controller as they select the Video POP which each endpoint will use.

Calls made using the video service are encrypted by default (covering the signalling for the call, the video and audio and presentation content); meaning that calls are more secure.

2. Interoute One Termination Service (SIP Trunks)

Interoute One Termination Services (SIP) provides customers the ability to call the PSTN or other Interoute customers.

Purpose of the data processing

Purpose of customer data processing
The SIP services store IP addresses of customer endpoints or gateway equipment to enable calls to be made into the Interoute voice platform. When calls are made, the system records logs and call detail records which may contain the name of the calling and called endpoints.

Purposes of data processing for delivery of the service
For troubleshooting purposes, the records identified above can be inspected by Interoute engineers and system supplier engineers. This is only done on a case by case basis with the agreement of the customer and files are transferred to 3rd parties only if necessary and only via encrypted methods.

There are certain specific data types which are identified below which are processed by the service. The purpose of this processing is for the successful provision and management of the service itself.

Categories of data processed

Customer Content Data
No customer content data is processed using typical features of this service and Interoute do not store or process the content of customer calls except for troubleshooting purposes as described above.

Data Processed Automatically to Deliver the Service
To deliver the service Interoute also needs to process certain types of data which may be personal. This will include communication addresses and computer device identifiers such as:

SIP Address
Which can be an IP address, E.164 number, or registered name
IP addresses
Telephone number
Such data will also be logged by the system as will certain operating system events.

SIP services will process the above data to control access to the service at our Session Border Controllers. Interoute stores and processes this as authenticating information to protect service security. To administer the service Interoute engineers are also able to inspect recorded information for trouble-shooting purposes.

Storage and Transmission
Customer endpoint data will normally be processed and stored in the Session Border Controllers which are in the Interoute POP locations in EU, US, HK and SG. Customer traffic entering the voice network must always traverse a session border controller (for SIP or H.323 sessions) before being routed onwards to its destination.

For troubleshooting and reporting purposes data may be moved from the POP locations and processed and stored elsewhere with the consent of the customer. This activity is only undertaken with the consent of the customer.

3. Hosted Skype for Business

Purpose of the data processing for Interoute Skype for Business

Purpose of customer data processing

Skype for business is able to record all electronic communications, as configured by or for the customer. Processing of personal data includes, for the purposes of the GDPR, storage of data.

Purposes of data processing for delivery of the service

For troubleshooting purposes the records identified above can be inspected by Interoute engineers and system supplier engineers. This is only done on a case by case basis with the agreement of the customer and files are transferred to 3rd parties only if necessary and only via encrypted methods.

There are certain specific data types which are identified below which are processed by the service. The purpose of this processing is for the successful provision and management of the service itself.

Categories of data processed

Customer Content Data

Any type of type of data including any personal data in electronic form could be stored (and therefore processed) as this is a feature of the service. Individuals will often use the service to share content generated by themselves or others and the service is able to store voice and video calls.

Data Processed Automatically to Deliver the Service

To deliver the service Interoute also needs to process certain types of data which may be personal. This will include communication addresses and computer device identifiers such as:
Email addresses

Telephone numbers

IP addresses

MAC addresses

Such data will also be logged by the system as will certain operating system events.
Skype for Business will also process authentication data to control access to the service. Interoute stores and processes authenticating Information such as passwords, used to protect service security and protect access to any sensitive information stored in logs. Such information will also include end user data: including data relating to end users created, collected processed or when accessed by Interoute in order to provide our services.
To administer the service Interoute engineers are also able to inspect recorded information for trouble-shooting purposes

Storage and Transmission

Data will normally be processed and stored in the customer's chosen Interoute Virtual Data Centre location(s) (VDC) as specified on the customer's order.
Where the customer order does not specify the required VDC locations then Interoute may at its discretion pick one or more VDC locations and confirm with the customer that this is acceptable before proceeding with the installation of the service.
For troubleshooting and reporting purposes data may be moved from the VDC locations and processed and stored elsewhere within the EU, US, SG, HK. This is only processed with the consent of the customer.
Calls between Microsoft Skype for Business client users are encrypted by default, unlike many other telephony solutions, meaning that calls are more secure.

4. Virtual Data Centre (VDC)

Purpose of the data processing for VDC

Purpose of customer data processing
The VDC platform is a virtual data centre and as a cloud based operating system can support the processing of all forms of personal data for any purpose at the discretion of the customer.

Purposes of data processing for delivery of the service
In order to allow communication with the VDC certain address and authentication data must be processed. There are certain specific data types, identified below which are processed by the service. The purpose of this processing is for the successful provision and management of the service itself.

Categories of data processed

Data Processed Automatically to Deliver the Service
To deliver the service Interoute also needs to process certain types of data which may be personal. This will include communication addresses and computer device identifiers such as:

Email addresses
Telephone numbers
IP addresses
MAC addresses
Such data will also be logged by the system as will certain operating system events.

VDC will also process authentication data to control access to the service. Interoute stores and processes authenticating Information such as user names and passwords, used to protect service security and protect access to any sensitive information stored in logs. Such information will also include end user data: including data relating to end users created, collected processed or when accessed by Interoute in order to provide our services.

To administer the service Interoute engineers are also able to inspect operating system information for trouble-shooting purposes

Storage and Transmission
Data will normally be processed and stored in the customer's chosen Interoute Virtual Data Centre location(s) (VDC) as specified on the customer's order.

Where the customer order does not specify the required VDC locations then Interoute may at its discretion pick one or more VDC locations and confirm with the customer that this is acceptable before proceeding with the installation of the service.

For troubleshooting and reporting purposes data may be moved from the VDC locations and processed and stored elsewhere within the EU, US, SG, HK. This is only processed with the consent of the customer.

Additional data you may choose to process

Customer Content Data
Any type of type of data including any personal data in electronic form could be processed as VDC is a general purpose compute service. If you choose to process personal data on VDC you should consider whether a Data Protection Impact Assessment is required in line with Article 35 of the GDPR and / or by local laws and regulations.

The nature of the VDC product allows customers to store and process any kind of personal information. Under the GDPR personal data has a very wide meaning, as a data controller (or potentially a processor processing on behalf of a data controller) the customer is responsible for assessing the privacy risks of processing such data. A range of security features are built into the VDC solution and the related operational activities. However, Interoute is not in a position to understand the risks to individuals that may arise should their data be compromised, the VDC user must make this judgement.

Some Categories of data to consider whether they are being processed, this list is provided simply as an example and to give an idea of the breadth of data to be considered under the GDPR:

Identification data, e.g. names, electronic IDs	Psychological data, e.g. personality or character.	Consumer habits, e.g. consumed or provided	Behavioural Data	Data on sexual behavior
Financial data	Household composition	Characteristics of the home	Computer Devices	Political opinions
Personal characteristics, e.g. age, sex,	Interests and leisure interests	Health data	Authenticating data	Trade union membership
Physical description data, e.g. height	Affiliations, e.g. clubs	Studies and training	Demographic	Philosophical or religious convictions
Lifestyle habits, e.g. smoker	Judicial data, e.g. arrests, convictions,	Occupation and employment	Life History	Image recordings
Social Network	Ownership	National Registry Number / NINo.	Racial or ethnic data	Sound recordings
Tracking Data	Location Data			

5. Enterprise Edge

Purpose of the data processing for Interoute Edge
The purpose of processing the data categories outlined below is for the successful provision and management of Interoute Edge connectivity services.

Categories of data processed
Interoute processes communication logs or "metadata" in real time as part of the service. This allows Edge to make dynamic, automated decisions based on the quality of communications. The service adapts to provide improved performance and reliability of connections when compared to basic networks. These logs are also stored to facilitate IT service management functions.

Authorised customer users and Interoute authorised engineers can inspect logs of this traffic metadata. This metadata includes source and destination IP addresses, ports, protocols, applications, locations. This data could be related to directly to an individual user/subscriber. However, this requires a database to be held on users and IP addresses. Interoute does not hold such a database, but our customers could (an area outside our control).

The actual content of customer data is neither logged or stored. The exception to this is where an optional WAN optimisation service is purchased, where some data is temporarily stored as an AES-128 encrypted cache. This cache is constantly changing. It cannot be decrypted or viewed by customers or Interoute staff and is only understandable to the system itself. No other data is stored in relation to users of the network.

Interoute stores and processes authenticating Information such as passwords, used to protect service security and protect access to any sensitive information stored in logs. Such information will also include end user data: including data relating to end users created, collected processed or when accessed by Interoute in order to provide our services.

Additional data you may choose to process

The nature of the Edge product allows customers to also store and process the information below. Interoute advises (as a precaution) that customers of Interoute consider whether and how they may use these data categories but does not require their use in order to successfully supply the customer with the Edge product.

Identifying

Information that uniquely or semi-uniquely identifies a specific individual. For your administration of Edge services you may decide to use certain identifying data. Broadly identifying data includes:

name, user-name, unique identifier, government issued identification, picture, biometric data

Behavioural

Information that describes an individual's behaviour or activity, on-line or off-line. Depending on how you choose to use Edge services certain behavioural data may be captured. Broadly, behavioural data includes such data as:

browsing behaviour, call logs, links clicked, demeanour, attitude

Computer Device

Information about a device that an individual uses for personal use. Depending on how you choose to use Edge personal device data may be captured. Broadly, Computer device data includes such data as:

IP address, Mac address, browser fingerprint.

Location

Information about an individual's location. Depending on how you choose to use Edge location data may be captured. Broadly location data includes such data as:

country, GPS coordinates, room number

Other User Generated Data

Interoute is not prescriptive about how you choose to use the Edge Product, therefore the list above is not meant to be comprehensive but is offered as a guide to considering your data protection approach.

6. Object Storage

Purpose of the data processing for Object Storage

Purpose of customer data processing

The Object Storage service is a cloud based data storage service and can support the storage of all forms of personal data for any purpose at the discretion of the customer.

Purposes of data processing for delivery of the service

In order to allow communication with the Object Storage service certain address and authentication data must be processed. There are certain specific data types, identified below which are processed by the service. The purpose of this processing is for the successful provision and management of the service itself.

Categories of data processed

Data Processed Automatically to Deliver the Service

To deliver the service Interoute also needs to process certain types of data which may be personal. This will include communication addresses and computer device identifiers such as:

Email addresses
Telephone numbers
IP addresses
MAC addresses
Such data will also be logged by the system as will certain operating system events.

Note that under the General Data Protection Regulation storage is considered to also be processing.

Object Storage will also process authentication data to control access to the service. Interoute stores and processes authenticating Information such as user names and passwords, used to protect service security and protect access to any sensitive information stored in logs. Such information will also include end user data: including data relating to end users created, collected processed or when accessed by Interoute in order to provide our services.

To administer the service Interoute engineers are also able to inspect operating system information for trouble-shooting purposes

Storage and Transmission

Data will normally be processed and stored in the customer's chosen Data Centre location(s) as specified on the customer's order.

Where the customer order does not specify the required locations then Interoute may at its discretion pick one or more locations and confirm with the customer that this is acceptable before proceeding with the installation of the service.

For troubleshooting and reporting purposes data may be moved from these locations and processed and stored elsewhere within the EU, US, SG, HK. This is only processed with the consent of the customer.

Additional Data you may choose to process

Customer Content Data

Any type of type of data including any personal data in electronic form could be stored (processed) as Object Storage is a general purpose storage service. If you choose to store personal data on Object Storage you should consider whether a Data Protection Impact Assessment is required in line with Article 35 of the GDPR and / or by local laws and regulations.

The nature of the Object Storage product allows customers to store and process any kind of personal information. Under the GDPR personal data has a very wide meaning and includes data storage, as a data controller (or potentially a processor processing on behalf of a data controller) the customer is responsible for assessing the privacy risks of processing such data. A range of security features are built into the Object Storage solution and the related operational activities. However, Interoute is not in a position to understand the risks to individuals that may arise should their data be compromised, the Object Storage user must make this judgement.

Some Categories of data to consider whether they are being processed, this list is provided simply as an example and to give an idea of the breadth of data to be considered under the GDPR:

Identification data, e.g. names, electronic IDs	Psychological data, e.g. personality or character.	Consumer habits, e.g. consumed or provided	Behavioural Data	Data on sexual behaviour
Financial data	Household composition	Characteristics of the home	Computer Devices	Political opinions
Personal characteristics, e.g. age, sex,	Interests and leisure interests	Health data	Authenticating data	Trade union membership
Physical description data, e.g. height	Affiliations, e.g. clubs	Studies and training	Demographic	Philosophical or religious convictions
Lifestyle habits, e.g. smoker	Judicial data, e.g. arrests, convictions,	Occupation and employment	Life History	Image recordings

Social Network	Ownership	National Registry Number / NINo.	Racial or ethnic data	Sound recordings
Tracking Data	Location Data			

7. Two Factor Authentication

Purpose of the data processing for Interoute Two Factor Authentication (2FA) services
The purpose of processing the data categories outlined below is for the successful provision and management of Interoute Two Factor Authentication (2FA) services.

Categories of data processed
Interoute processes authentication logs or "metadata" in real time as part of the service. These logs are stored either on the 2FA platform itself or in a centralised log collector and assist Interoute in management of the service and troubleshooting. These logs are also stored to facilitate IT service management functions.

Authorised Interoute engineers can inspect logs of this metadata. This metadata includes source and destination IP addresses, applications, locations, usernames and attempted authentication sessions (both successful and unsuccessful). This data could be related to directly to an individual user/subscriber, however as Interoute will typically only hold username data and not full user details, relating this data to a user would require a database to be held on users and IP addresses/usernames. Interoute does not hold such a database, but our customers could (an area outside our control).

Interoute does not typically store user authentication data for 2FA services beyond username as first factor authentication is against external databases, however for second factor Interoute will store usernames. For some implementations (dependent on customer requirements) Interoute may store and process additional authenticating Information such as passwords, used to protect service security and protect access to any sensitive information stored in logs. Such information will also include end user data: including data relating to end users created, collected processed or when accessed by Interoute in order to provide our services.

Additional Data you may choose to process
The nature of the Interoute 2FA service product allows customers to also store and process the information below. Interoute advises (as a precaution) that customers of Interoute consider whether and how they may use these data categories but does not require their use in order to successfully supply the customer with the 2FA product.

Identifying
Information that uniquely or semi-uniquely identifies a specific individual. For your administration of Interoute IDS services you may decide to use certain identifying data. Broadly identifying data includes:

name, user-name, unique identifier, government issued identification, picture, biometric data

Behavioural
Information that describes an individual's behaviour or activity, on-line or off-line. Depending on how you choose to use Interoute 2FA services certain behavioural data may be captured. Broadly, behavioural data includes such data as:

Authentication logs, connectivity logs

Computer Device
Information about a device that an individual uses for personal use. Depending on how you choose to use Interoute 2FA services personal device data may be captured. Broadly, Computer device data includes such data as:

IP address, Mac address

Location
Information about an individual's location. Depending on how you choose to use Interoute 2FA services location data may be captured. Broadly location data includes such data as:

country, GPS coordinates

Other User Generated Data
Interoute is not prescriptive about how you choose to use Interoute IDS services, therefore the list above is not meant to be comprehensive but is offered as a guide to considering your data protection approach.

8. Next Generation Firewalls

Purpose of the data processing for Interoute Next-Generation Firewall Services
The purpose of processing the data categories outlined below is for the successful provision and management of Interoute Next-Generation Firewall services.

Categories of data processed
Interoute processes communication logs or "metadata" in real time as part of the service. These logs are stored either on the firewall itself or in a centralised log collector and assist Interoute in making decisions on configuration changes or in troubleshooting. These logs are also stored to facilitate IT service management functions.

Authorised customer users and Interoute authorised engineers can inspect logs of this traffic metadata. This metadata includes source and destination IP addresses, ports, protocols, applications, locations. This data could be related to directly to an individual user/subscriber. However, this requires a database to be held on users and IP addresses. Interoute does not hold such a database, but our customers could (an area outside our control).

The actual content of customer data is neither logged or stored.

Interoute does not typically store authentication data as authentication is against external databases, however for some services (dependent on customer requirements) Interoute may store and process authenticating Information such as passwords, used to protect service security and protect access to any sensitive information stored in logs. Such information will also include end user data: including data relating to end users created, collected processed or when accessed by Interoute in order to provide our services.

Additional Data you may choose to process
The nature of the Interoute Next-Generation Firewall services product allows customers to also store and process the information below. Interoute advises (as a precaution) that customers of Interoute consider whether and how they may use these data categories but does not require their use in order to successfully supply the customer with the Interoute Next-Generation Firewall product.

Identifying
Information that uniquely or semi-uniquely identifies a specific individual. For your administration of Interoute Next-Generation Firewall services you may decide to use certain identifying data. Broadly identifying data includes:

name, user-name, unique identifier, government issued identification, picture, biometric data

Behavioural
Information that describes an individual's behaviour or activity, on-line or off-line. Depending on how you choose to use Interoute Next-Generation Firewall services certain behavioural data may be captured. Broadly, behavioural data includes such data as:

browsing behaviour, connectivity logs

Computer Device

Information about a device that an individual uses for personal use. Depending on how you choose to use Interoute Next-Generation Firewall services personal device data may be captured. Broadly, Computer device data includes such data as:

IP address, Mac address, browser fingerprint.

Location

Information about an individual's location. Depending on how you choose to use Interoute Next-Generation Firewall services location data may be captured. Broadly location data includes such data as:

country, GPS coordinates, room number

Other User Generated Data

Interoute is not prescriptive about how you choose to use Interoute Next-Generation Firewall services, therefore the list above is not meant to be comprehensive but is offered as a guide to considering your data protection approach.

9. Content Filtering

Purpose of the data processing for Content Filtering Services

The purpose of processing the data categories outlined below is for the successful provision and management of Interoute Web and Email Security services.

Categories of data processed

Log Data is recorded and stored by the third party cloud security provider's infrastructure.
Authorised customer users and Interoute authorised engineers can inspect logs of this traffic metadata. This metadata includes source and destination IP addresses, ports, protocols, applications, locations. This data could be related to directly to an individual user/subscriber. However, this requires a database to be held on users and IP addresses. Interoute does not hold such a database, but our customers could (an area outside our control).
The actual content of customer data is neither logged nor stored, e.g. the log may record that an email server was contacted but will not contain any of the email content.
Interoute does not typically store authentication data as authentication is against external databases, however for some services (dependent on customer requirements) Interoute may store and process authenticating Information such as passwords, used to protect service security and protect access to any sensitive information stored in logs. Such information will also include end user data: including data relating to end users created, collected processed or when accessed by Interoute in order to provide our services.

Additional Data you may choose to process

The nature of the Interoute Web and Email Security Services product allows customers to also store and process the information below. Interoute advises (as a precaution) that customers of Interoute consider whether and how they may use these data categories but does not require their use in order to successfully supply the customer with the Interoute Web and Email Security Services product.

Identifying

Information that uniquely or semi-uniquely identifies a specific individual. For your administration of Interoute Web and Email Security Services you may decide to use certain identifying data. Broadly identifying data includes:
name, user-name, unique identifier, government issued identification, picture, biometric data

Behavioural

Information that describes an individual's behaviour or activity, on-line or off-line. Depending on how you choose to use Interoute Web and Email Security Services certain behavioural data may be captured. Broadly, behavioural data includes such data as:
browsing behaviour, connectivity logs

Computer Device

Information about a device that an individual uses for personal use. Depending on how you choose to use Interoute Web and Email Security Services personal device data may be captured. Broadly, Computer device data includes such data as:
IP address, Mac address, browser fingerprint.

Location

Information about an individual's location. Depending on how you choose to use Interoute Web and Email Security Services location data may be captured. Broadly location data includes such data as:
country, GPS coordinates, room number

Other User Generated Data

Interoute is not prescriptive about how you choose to use Interoute Web and Email Security Services, therefore the list above is not meant to be comprehensive but is offered as a guide to considering your data protection approach.

10. DDoS Protection

Purpose of the data processing for Interoute Distributed Denial of Service (DDoS) services
The purpose of processing the data categories outlined below is for the successful provision and management of Interoute Distributed Denial of Service (DDoS) services.

Categories of data processed

Interoute processes communication logs or "metadata" in real time as part of the service. These logs are stored either on the DDoS itself or in a centralised log collector and assist Interoute in making decisions on configuration changes or in troubleshooting. These logs are also stored to facilitate IT service management functions.

Authorised customer users and Interoute authorised engineers can inspect logs of this traffic metadata. This metadata includes source and destination IP addresses, ports, protocols, applications, locations. This data could be related to directly to an individual user/subscriber. However, this requires a database to be held on users and IP addresses. Interoute does not hold such a database, but our customers could (an area outside our control).

The actual content of customer data is neither logged or stored.

Interoute does not typically store authentication data for DDoS services as authentication is against external databases, however for some services (dependent on customer requirements) Interoute may store and process authenticating Information such as passwords, used to protect service security and protect access to any sensitive information stored in logs. Such information will also include end user data: including data relating to end users created, collected processed or when accessed by Interoute in order to provide our services.

Additional Data you may choose to process

The nature of the Interoute DDoS service product allows customers to also store and process the information below. Interoute advises (as a precaution) that customers of Interoute consider whether and how they may use these data categories but does not require their use in order to successfully supply the customer with the DDoS product.

Identifying

Information that uniquely or semi-uniquely identifies a specific individual. For your administration of Interoute DDoS services you may decide to use certain identifying data. Broadly identifying data includes:
name, user-name, unique identifier, government issued identification, picture, biometric data

Behavioural

Information that describes an individual's behaviour or activity, on-line or off-line. Depending on how you choose to use Interoute DDoS services certain behavioural data may be captured. Broadly, behavioural data includes such data as:

browsing behaviour, connectivity logs

Computer Device

Information about a device that an individual uses for personal use. Depending on how you choose to use Interoute DDoS services personal device data may be captured. Broadly, Computer device data includes such data as:
IP address, Mac address, browser fingerprint.

Location

Information about an individual's location. Depending on how you choose to use Interoute DDoS services location data may be captured. Broadly location data includes such data as:
country, GPS coordinates, room number

Other User Generated Data

Interoute is not prescriptive about how you choose to use Interoute DDoS services, therefore the list above is not meant to be comprehensive but is offered as a guide to considering your data protection approach.

11. Intrusion Prevention

Purpose of the data processing for Interoute Intrusion Prevention System services
The purpose of processing the data categories outlined below is for the successful provision and management of Interoute Intrusion Prevention System (IPS) services.

Categories of data processed

Interoute processes communication logs or "metadata" in real time as part of the service. These logs are stored either on the IPS itself or in a centralised log collector and assist Interoute in making decisions on configuration changes or in troubleshooting. These logs are also stored to facilitate IT service management functions.
Authorised customer users and Interoute authorised engineers can inspect logs of this traffic metadata. This metadata includes source and destination IP addresses, ports, protocols, applications, locations. This data could be related to directly to an individual user/subscriber. However, this requires a database to be held on users and IP addresses. Interoute does not hold such a database, but our customers could (an area outside our control).
The actual content of customer data is neither logged or stored.
Interoute does not typically store authentication data for IPS services as authentication is against external databases, however for some services (dependent on customer requirements) Interoute may store and process authenticating Information such as passwords, used to protect service security and protect access to any sensitive information stored in logs. Such information will also include end user data: including data relating to end users created, collected processed or when accessed by Interoute in order to provide our services.

Additional Data you may choose to process

The nature of the Interoute IPS service product allows customers to also store and process the information below. Interoute advises (as a precaution) that customers of Interoute consider whether and how they may use these data categories but does not require their use in order to successfully supply the customer with the IPS product.

Identifying

Information that uniquely or semi-uniquely identifies a specific individual. For your administration of Interoute IPS services you may decide to use certain identifying data. Broadly identifying data includes:
name, user-name, unique identifier, government issued identification, picture, biometric data

Behavioural

Information that describes an individual's behaviour or activity, on-line or off-line. Depending on how you choose to use Interoute IPS services certain behavioural data may be captured. Broadly, behavioural data includes such data as:
browsing behaviour, connectivity logs

Computer Device

Information about a device that an individual uses for personal use. Depending on how you choose to use Interoute IPS services personal device data may be captured. Broadly, Computer device data includes such data as:
IP address, Mac address, browser fingerprint.

Location

Information about an individual's location. Depending on how you choose to use Interoute IPS services location data may be captured. Broadly location data includes such data as:
country, GPS coordinates, room number

Other User Generated Data

Interoute is not prescriptive about how you choose to use Interoute IPS services, therefore the list above is not meant to be comprehensive but is offered as a guide to considering your data protection approach.

Annex 2 - Security Measures

Description of the technical and organisational security measures implemented by Interoute for each Service provided.

1 PHYSICAL

1.1 PHYSICAL SECURITY

Interoute shall implement:

1.1.1 a building access control system for the Site;

1.1.2 a building alarm system for the Site;

1.1.3 appropriate CCTV for the Site.

1.2 EMPLOYEE, VISITOR, AND TRUSTED AGENT ACCESS

In areas where Services are being provided, Interoute shall:

1.2.1 restrict access to authorized persons only;

1.2.2 utilize identification and authentication controls to authorize and validate the access;

1.2.3 securely maintain an audit trail of all access, including times of entry and departure;

1.2.4 securely manage visitors:

(a) grant access only for specific authorized purposes;

(b) record the date and time of entry; and

(c) ensure that all visitors are escorted and supervised at all times.

2 TECHNICAL

2.1 SYSTEM ADMINISTRATION

2.1.1 Where systems allow, all privileged account shall be uniquely identifiable and each user shall be accountable and responsible for any action taken under that user's own user ID and password.

2.1.2 Where systems allow, system accounts or built-in application accounts shall not be used to provide generic or unauthorized access.

2.1.3 All access to Information Systems shall be authenticated. This includes console access, individual accounts, administrative accounts, and any automated relationships with other systems.

2.2 PASSWORD CONTROLS

2.2.1 Passwords shall be protected at all times, including appropriate encryption.

2.2.2 All passwords shall be promptly changed if they are suspected of being compromised or known to have been disclosed to unauthorized parties; users shall be able to change their own passwords.

2.2.3 Where systems allow, passwords shall be uniquely identifiable and each user shall be accountable and responsible for any action taken under that user's own user ID and password. Users shall not share or divulge their password to anyone.

2.2.4 On rare occasions where the requirement of hardcoded usernames and passwords is necessary and where systems allow, the system will be configured with a service account with the lowest set of privileges possible.

2.2.5 Where systems allow, passwords complexity should never be less than 3 out of 4 character classes and shall have character class choices such as upper case letters, lower case letters, numeric digits, or special characters. Where possible an increased password length will be used to increase entropy probabilities.

2.3 SEGREGATION CONTROL

Where the customer solution utilises a shared environment, appropriate security controls will be deployed to ensure appropriate customer segregation.

2.4 PERIMITER DEFENCE

Firewalls and intrusion detection systems are place to monitor and resist malicious activity.

2.5 OPERATING SYSTEM SECURITY CONTROLS

2.5.1 Anti-Virus Configuration

Anti-Virus software can be supplied as a service and configured upon the Customers express consent. Where this service is provided it will be configured to run real-time and to download automatic updates no less than once per week.

2.5.2 Patch Management

Where possible patch management systems are in place to deploy critical security patches to Interoute managed devices. For customer facing services, patches will not be deployed without a customer request to do so.

2.6 SYSTEM AND DEVICE HARDENING

Where possible all operating systems and devices will be hardened to remove any weak protocols and services that are not required.

2.7 VULNERABILITY DISCOVERY

Where possible regular system vulnerability scanning will be carried out with the express permission of the customer to identify any technical issues that may need to be resolved.

3 PROCESS

3.1 SYSTEM ADMINISTRATION

3.1.1 Privileged account requests shall be subject to proper justification, provisioning and an approvals process, and assigned to named individuals

3.1.2 Interoute Service Provider personnel privileges shall be reviewed to ensure they have the appropriate privileges to undertake their duties

3.1.3 Starters and leavers process is in place to remove accounts that are no longer required.

3.2 INFORMATION SECURITY TRAINING

3.2.1 Staff information security training is available through the company Intranet and regular information security communications are provided to all staff.

3.3 ACCESS CONTROLS TO DATA

The Interoute Service Provider shall follow Customer instructions with regards to the movement of data. All requests to move customer data shall be made in writing to the Interoute Service Provider.

3.4 DESTRUCTION OF MEDIA

All hard drives shall follow Interoute's processes and procedures for their erasure or destruction prior to disposal of the system.

3.5 DISCLOSURE CONTROL

The Interoute Service Provider shall not:

3.5.1 allow copying of customer hosting environments other than for back up or forensic purposes; and

3.5.2 allow the removal Customer Personal data from the premises unless at the specific request of the customer.

4 CUSTOMER RESPONSIBILITIES IN RELATION TO DATA CONFIDENTIALITY AND ENCRYPTION

4.1 Interoute recommends that the Customer further protects the confidentiality of the Customer's data with additional cryptographic controls. Such controls would include encrypting data at rest through application and database level encryption. In addition, the application controls should ensure that all access to sensitive data is tightly controlled through strong access control mechanisms and all such access is thoroughly audited.

4.2 Cryptographic keys for the protection of data by the customer as recommended above is also the responsibility of the customer. The Customer should design their key management system taking into account the same issues about protecting data at rest.