General Terms and Conditions for the supply of services

Under these General Terms and Conditions, and any service order or annex, the Parties shall purchase and/or supply one or more Services from and/or to one another on a nonexclusive basis.

The General Terms and Conditions define the principles governing the rights and obligations between the Parties. The Service Reference Documents and Order Forms set out the specific terms governing the provision of the Services.

The Parties may agree on the provisioning of additional Services by signing an Order Form that will refer to Service Reference Document(s).

The Service Reference Documents and Order Forms are hereafter referred to as the "Service Annexes

In case of contradiction between these general terms and the specific terms set out in the Service Annexes, the specific terms of the Service Annexes shall prevail.

These General Terms and Conditions, the Service Annexes, Technical Specifications (if any), the Appendices listed below, constitute the entire agreement between the Parties (hereafter referred to as "the Agreement"). The Agreement shall prevail over all prior agreements, proposals, negotiations, representations or communications relating to the subject matter between the Parties.

The Parties acknowledge that they have not been induced to enter into this Agreement by any representations or promises not specifically stated

Article 1 Glossary

Agreement	These General Terms and Conditions, the Service Annexes, and the Appendices.
Affiliate	Any entity directly or indirectly controlling, controlled by, or under common control with a Party where an entity shall be treated as being controlled by another if that other entity has fifty percent (50%) or more of the votes in such entity, is able to direct its affairs and/or to control the composition of its board of directors or equivalent body.
Service	The communication service described in a Service Reference Document.
Order Form	The document by which a Service will be ordered.
Network	The transmission equipment and other resources to convey signals between points by wire, radio waves, by optical or other electromagnetic means.
Operational Date	Per Service supplied, moment as from which both Parties have completed all provisioning tests successfully and have confirmed completion of these tests in writing.
Service Annexes	As used in these General Terms and Conditions, either a Service Reference Document or Order Form.
Service Reference Document	An annex to these General Terms and Conditions describing the Service(s) offered by one Party to the other Party, as applicable.

Article 2 Scope of the Agreement

The Parties shall supply the Services to each other in accordance with the provisions of the Service Annex(es)

Article 3 Term and Termination

3.1 Term

The Agreement shall enter into force on the date of signature of the first Order Form between the Parties and shall remain valid as long as there exists a valid Order Form between the Parties. Unless otherwise stated in a Service Annex entered into for a fix term, which can be renewed, this Agreement may be terminated by a Party at any time upon giving a three (3) months prior written notice to the other.

3.2 Termination modalities

3.2.1. This Agreement or a Service Annex may be terminated by written notice with immediate effect by a Party – notwithstanding any other rights such

Party may have - upon any of the following events occurring:

a. If the other Party has failed in the performance of any material contractual obligation of this Agreement, provided that the non-defaulting Party shall not be entitled to terminate unless and until it has given written notice of the relevant breach to the breaching Party and the breaching Party shall have failed to remedy the breach within thirty (30) calendar days of receipt of such notice; or

b. If the other Party is the subject of a bankruptcy order, or is placed in an insolvency proceeding or becomes insolvent, or makes any arrangement or composition with or assignment for the benefit of its creditors, or if any of the other party's assets are the subject of any form of seizure, or goes into liquidation, either voluntary (otherwise than for reconstruction or amalgamation) or compulsory or if a receiver or administrator is appointed over its assets (or the equivalent of any such event in the jurisdiction of such other party).

3.2.2. In the event of a serious default by a Party, the other Party may terminate the Agreement or, independently of the Agreement, a Service Annex with immediate effect. The following are considered to be serious defaults (non-exhaustive list):

a. Not supplying a Service within two (2) months as from the Operational Date;

b. Non-payment of amounts due within five (5) calendar days after having been advised thereof by the creditor Party in writing;

c. Fraudulent or abusive use of the Service or absence of measures reasonably required to prevent such use;

d. Refusal to subscribe to or to modify the bank guarantee as provided in Article 5;

e. Call upon bank guarantee when the conditions for such call are not fulfilled.

3.2.3. In case of termination of this Agreement by one of the Parties during the Initial Term of a Service Annex, this Party will be requested to pay the recurring charges due for the remaining period, together with all costs made by the other Party in order to implement the Service.

3.2.4. The termination of the Agreement pursuant to article 3.2.1 will automatically result in the termination of all Service Annexes according to their respective termination notices.

3.2.5. The termination of a Service Annex does not affect the validity of the rest of the Agreement.

3.2.5. The termination of the present Agreement shall not prejudice or affect a right of action or remedy which shall have accrued or shall accrue subsequently under this Agreement to either Party.

3.2.6. After the termination of the Agreement or of a Service Annex for whatsoever reason, the confidentiality provisions of Article 9 remain in full force and effect during three (3) years as from such termination.

Article 4 Financial Terms

4.1 Prices

4.1.1 Prices shall be expressed in the currency mentioned in the Order Form

4.1.2 The prices for the Services are mentioned in the Service Annexes.

4.1.3 A Party may alter the price for the Service it supplies on a monthly basis unless specified otherwise in the respective Service Annex. The new price supersedes the previous price. Pricelists have to be exclusively sent to the e-mail address mentioned in Appendix 1 or otherwise communicated by a Party to the other.

4.1.4 The prices for the Services exclude VAT or any other applicable tax. The paying Party bear any taxes levied in its own country of residence and possible gross-up fee, if any, to be paid to the provider of Services, to guarantee the net payment of the price agreed upon. In the event that payment of any amount of the prices becomes subject to withholding tax, levy or similar payment obligation on sums due to the provider of Services under this Agreement, such withholding tax amounts shall be borne and paid for by the paying Party in addition to the sums due to the provider of Services and the paying Party shall ensure that the other Party actually receives and is entitled to retain, free and clear of any such deduction or withholding, the full amount which it would have received if no such deduction or withholding had been required. Should the paying Party withhold any amounts and request that the provider of Services grosses up its prices to reflect such withholding, or otherwise makes references to such amounts in its monthly accounts, the paying Party will provide the provider of Services free of charge with the appropriate certificate(s) from the relevant authorities confirming the amount of the withholding taxes, levies or similar payments borne and paid for by the paying Party.

4.2 Invoices and payments terms

4.2.1. Any invoice exchanged between the Parties must refer to Services supplied during one calendar month and has to be communicated to the other Party within the month following the month to which it refers.

If a Party is unable to send its invoice within the month following the month to which it refers, it must notify the other Party in writing before the end of this period, and such invoice has to be communicated to the other Party no later than six (6) months after the end of the month to which the invoice refers. After this six (6) month period, the Party agrees to irrevocably waive its rights to claim the payment of such invoice.

Any corrective invoice in relation to an invoice communicated in due time has to be communicated to the other Party no later than six (6) months after the end of the month to which the invoice communicated in due time refers. After this six (6) month period, the Parties agree to irrevocably waive its rights to claim the payment of such invoice.

Parties will provide electronic invoices signed with a digital certificate. These electronic invoices will be considered as valid documents. Soft copies of invoices addressed to BICS have to be sent to the e-mail address mentioned in Appendix 1 at the latest one (1) calendar day after the invoice date. All invoices which are not addressed to the correct entity will be refused and will not be paid on due date. The invoices are due and payable within thirty (30) calendar days as from the date of receipt of the invoice. Payment will be made by wire transfer, payment costs are borne by the debtor Party. If payment of undisputed amounts is not received within due date, the invoicing Party is entitled to one and a half (1,5) percent per month on the unpaid balance for late payment interests, administrative and recovery costs. Any invoice addressed to BICS has to indicate the VAT number BE 0866.977.981 of BICS such as the references to the application for VAT purposes, of the art. 21 par 2 of the Belgian VAT Code in view to apply the reverse charge mechanism for VAT. In addition, any invoice addressed to BICS has to indicate the invoice currency and the payment currency. The applicable time zone shall be for Voice Central European Time (CET): Standard Time UTC+1, Daylight Savings Time UTC+2 and for Messaging and Signalling: GMT

4.2.2. If both Parties supply Services to the other, the Parties agree to compensate the payments of due and undisputed amounts relating to the Services supplied. The debtor Party will thus pay to the creditor Party the difference between the invoices. The compensation proposal will be sent by one of the Parties.

4.2.3. This compensation principle does not release any Party to pay within thirty (30) calendar days following the date of receipt of the invoice. If a Party fails to send its invoice within the term as described in article 4.2.1, such Party will pay the entire invoice sent by the other Party before the due date of that invoice.

4.2.4. Parties hereby moreover agree to the principle of netting all undisputed overdue invoices issued under this Agreement with all undisputed overdue invoices issued under any other services agreement executed between the Parties.

4.2.5. If payment is not received by the invoicing Party within ten (10) days of the due date, the invoicing Party may temporarily suspend the Service(s) to the defaulting Party until such time as payment is received in full. Prior to suspension of the Service the invoicing Party will provide written notice to the defaulting Party at the email address mentioned in the Appendix 1 or otherwise communicated by a Party to the other.

4.2.6. Each Party shall be exclusively responsible for and pay all expenses associated with all billing, collection, and provision of customer service activities in connection with calls originated by its customers. No payments due hereunder are contingent on payment due to either Party from its own customers. Neither Party shall be obliged to establish a credit note for the supply of a Service for which the other Party could not collect the corresponding amount with its end user (e.g. in the event of insolvency or fraud), regardless of whether or not the fraudulent usage or unauthorized calling was reported by a Party to the other Party.

4.2.7. The Parties agree that the invoices will be exchanged only between the Parties having signed this Agreement, unless agreed otherwise in writing between the Parties.

4.2.8. Neither Party will accept collection of amounts by a third party in name of the other Party, unless agreed otherwise in writing between the Parties.

4.2.9. Currency

Tariff, invoice and payment currency shall be in the currency as defined in paragraph 4.1.1.

In case there are multiple currencies in the tariff agreements and the compensation principle is agreed, a compensation proposal per currency needs to be created. As a consequence, the net amounts per currency need to be paid in the

respective currencies. No conversion of net amounts is accepted for payment purposes.

4.3 Billing disputes

4.3.1 If any Party disagrees with an invoice received from the other Party, it must notify in writing the other Party thereof before the due date of such invoice. As from the due date, the invoiced Party agrees to irrevocably waive its right to dispute the invoice. All invoices and protests must at least explicitly mention the following dispute details: the invoice number, the invoice date, the invoice period, the concerned disputed amount, the period, the Service supplied, the destinations, the telecommunications route (if applicable), the object and arguments of dispute. All disputes must be sent to the email address mentioned in Appendix 1 or otherwise communicated by a Party to the other.

4.3.2 In the event of an invoice dispute which cannot be settled amicably before that invoice's due date, the debtor Party must in any event settle before the due date all amounts which are not in dispute.

The Parties shall resolve any dispute within 14 calendar weeks (unless extended by mutual agreement) from the date of the dispute notification by complying with the following timeframe:

The disputing Party shall have 4 calendar weeks from the date of the dispute notification to provide CDR and/or other dispute's supporting evidence to the invoicing Party. If the disputing Party fails to provide the dispute's supporting evidence(s) within the time frame set out herein, the dispute will be deemed closed in favour of the invoicing Party and the disputed amount will have to be paid to the invoicing Party.

The invoicing Party shall have 8 calendar weeks from the date of receipt of the elements from the disputing Party to provide this latter with a feedback and supporting evidence of the correctness of the invoice. If the invoicing Party fails to provide the supporting evidence of the correctness of the invoice within the time frame stated above, the dispute will be deemed closed in favour of the disputing Party and the disputed amount will have to be credited to the disputing Party.

The Parties shall have 2 calendar weeks from the receipt of these elements by the disputing Party to resolve the dispute.

Absent any resolution of the invoice dispute within the above-mentioned timeframe, the dispute shall be escalated to high management level notwithstanding the possibility for a Party to start legal proceedings in accordance with article 17 of these General Terms and Conditions.

4.3.3 The Parties agree that no dispute shall be raised if the amount in dispute is less than one percent (1%) of the corresponding invoice's total amount and less than a thousand euros (1000€) (both thresholds should apply).

4.3.4 When a dispute is settled, a credit note has to be provided within thirty (30) calendar days. If the credit note is not received within this timeframe, late payment interests will be charged on the disputed amount.

Article 5 Payment Securities

5.1 Payment securities requested by a Party or granted by a Party shall be as set out in an annex to these General Terms and Conditions.

Article 6 Representations and warranty

6.1 Each Party represents that it is qualified and able to perform, technically, organisationally, legally and financially, the obligations it assumes under this Agreement.

6.2 The Services are to be provided to the best ability of the supplying Party and in accordance with "state of the art" techniques, without warranties as to the intended result to be achieved, unless the Parties agree otherwise in a service level agreement.

6.3 The warranty is excluded for defects or service interruptions of the Services if a Party does not follow the other Party's instructions.

Article 7 Liability

7.1 Except as otherwise further limited herein, each Party's liability under this Agreement shall be limited to compensation of actual, direct, personal, and foreseeable damage or loss suffered by the other Party (including damage or loss caused by the employee(s) and/or the contractor(s)), and shall not include indirect, consequential, special or punitive damages including but not limited to loss of profits or income, additional expenses loss of customers, loss of or damage to data or loss of contracts, loss of time or loss of business.

7.2 BICS shall not be held liable for the content of information that is transferred or stored by the other Party or any third party using the BICS' Network, Systems and/or Services.

BICS shall not be liable for the content of calls or messages. BICS is likewise not liable for services

provided by third parties and accessible via either Party's network or for bills issued for such services.

7.3 Each Party's liability shall be limited to five hundred thousand euro (€500.000) for the total amount of damages occurring in the course of a single year.

7.4 Nothing in this Agreement shall operate to limit or exclude either Party's liability for damages arising from its own fraudulent or grossly negligent acts or omissions, for bodily injury it causes to the other Party's representatives or for any other liability that cannot be excluded or limited by law.

Article 8 Force majeure

8.1 Neither of the Parties shall be liable for any delay or deficiency in the performance of its obligations if this delay is due to a force majeure event. Following events are considered to be force majeure (not exhaustive list): act of God, flood, earthquake, storm, thunderstorm, frost, explosion, lighting, fire, epidemic, war, outbreak of hostilities (whether or not war is declared), riot, strikes or other labour unrest, civil or military disturbance, embargo, social conflicts, sabotage, fibre or cable cut, expropriation by governmental authorities, interruptions by regulatory or judicial authorities, interruption or break-down of electricity supply, acts or orders of government, statutory or public agencies or other acts of events that are outside the reasonable control of the concerned party.

Article 9 Confidentiality

9.1 This Agreement and any information provided by either Party under this Agreement (including but not limited to personal data, business information, product information, financial information, know-how, or any information that should reasonably be considered confidential) (the "Confidential Information") is made in strict confidence between the Parties. Neither Party will disclose whole/or a part of this Agreement or any Confidential Information of the other Party to a third party without the prior written consent of the other Party, unless this third party is either a wholly owned subsidiary or affiliate to the receiving Party, or a parent entity wholly owning the receiving Party.

9.2 The confidentiality obligation shall not apply to any information which:

- enters the public domain other than as a result of a breach of this article;
- is lawfully received from a third party which is under no confidentiality obligation in respect of that information;
- is independently developed by the receiving Party or one of its Affiliates without use of the disclosing Party's Confidential Information; or
- are required to be disclosed by law or by any competent regulatory or governmental authority but subject to article 9.4 below.

9.3 After termination of this Agreement for whatsoever reason, the obligations of confidentiality provided under this Agreement will remain in full force and effect during three (3) years as from such termination.

9.4 If the receiving Party is required by law or by the order of a competent jurisdiction, a public authority or a private (industry led) body appointed by government to disclose (in part or in full) any Confidential Information, that Party shall immediately notify the disclosing Party thereof in writing, unless such notification is prohibited by law, and give the latter the opportunity to seek any legal remedies to maintain the confidentiality of the Confidential Information. In any case, the receiving Party shall only disclose Confidential Information that it is legally required to disclose and shall take all possible measures to maintain the confidentiality of the Confidential Information. This notification obligation does not apply in case of a valid request from law enforcement or other authorities having competence in the field of telecommunications, data protection or end users' protection regulations.

Article 10 Transfer, Assignment and Subcontracting

10.1 Neither Party may assign or transfer all or any part of its rights, benefits or obligations under the Agreement without the prior written consent of the other Party.

10.2 The Parties can subcontract the performance of Services to third parties. However, a Party remains liable for its obligations and for the subcontracted work.

Article 11 Fraud

11.1 It is the Parties' mutual interest to prevent any kind of fraud, abuse, misuse or damage of data that involves the Parties' respective Network or Service. The Parties may therefore inform each other on the occurrence of such event in due course, exchange all necessary and relevant data, including but not limited to customer information, and, in such case, will jointly discuss and work out measures either to prevent or eliminate such fraud, abuse, misuse or damage. No Party shall transfer information to the

other Party to the extent that a Party is prohibited from doing so by laws and regulations of its own country applicable to telecommunications services and/or data privacy. Each Party will strictly comply with the laws and regulations regarding telecommunications services and data privacy applicable in its respective countries, and will inform the other Party, if and what special treatment of data generated in connection with telecommunications services delivered under this Agreement may be required under such laws and regulations by the other Party.

Article 12 Publicity

12.1 Parties may agree to collaborate to the development of a joint press release (comparable to https://www.bics.com/media-room/news) to be published within one (1) month following the signature of any Service Annex, or of any other marketing material (such as success stories) referring to the name of the other Party and the existence of a commercial relationship between the Parties.

Article 13 Intellectual Property

13.1 The Parties commit not to compromise in any manner each other's registered trademarks and/or service marks.

13.2 The respective copyright, patent and other intellectual property rights (hereinafter referred to as the "Rights") owned by either Party or developed by either Party related to the Services referred to herein shall vest in that party. Unless specifically mentioned otherwise in this article 13, no title to any Rights owned by each Party are or will be transferred to the other Party.

13.3 If so indicated in a Service Annexes, BICS grants the other Party for the full term of the Agreement a non-exclusive, non-transferable, revocable right to use the Software as described in the Service Annex. Unless otherwise indicated in the Service Annex, the license granted in this article 13.3 does not include the right to: (i) sublicense or transfer the Software to another party by means of sale, lease, loan, rent, license or otherwise; (ii) receive the source code of the Software; (iii) alter, modify or adapt the Software, including (but not limited to) translating, reverse engineering, decompiling, disassembling, creating derivative works, or taking any other steps intended to produce source code out of the Software. The other Party shall also comply with all other limitations set out in the Service Annex which may apply to the license described in this article 13.3.

Article 14 Data Protection

14.1 When processing of personal data is part of the Services, by default, each Party processes said personal data as a separate autonomous data controller and shall process such personal data in accordance with applicable data protection and telecommunications laws. In cases were one of the controllers is located outside the EEA, the Parties agree that the EU Standard Contractual Clauses (Controller to Controller), which are to be found on BICS website, are applicable.

14.2 For Services implying the processing of personal data as instructed by a Party to the other, the processing Party shall act as processor of personal data and Parties shall comply with the Data Processing Agreement included in these General Terms and Conditions as Appendix 2.

Article 15 Notices

15.1 To be valid, all notices or any other communication under the Agreement, including notices relating to change of details of the Parties (address, account number, etc.), must be given in writing and sent to the address mentioned in the Appendix 1 or otherwise communicated by a Party to the other.

15.2 Corporate References will be described in the Appendix 1 or otherwise communicated by a Party to the other.

15.3 Either Party guarantee to inform the other Party of any changes to the details mentioned in the

Appendix 1 without delay to the contact referred to in such Appendix or otherwise communicated by a Party to the other.

Article 16 General Provisions

16.1 Unless explicitly stated otherwise in the Agreement, the failure of any Party to exercise any right or remedy under the Agreement shall not constitute a waiver of such right or remedy, and the waiver of any violation or breach of the Agreement by a Party shall not constitute a waiver of any prior or subsequent violation or breach.

16.2 The Parties to the Agreement are independent contractors. Neither the performance by the Parties

of their duties and obligations under this Agreement nor anything herein shall create or imply an agency relationship between the Parties, nor shall this Agreement be deemed to constitute a joint venture or partnership between the Parties.

16.3 Notwithstanding any waiver by a Party of its right to request a bank guarantee, such Party shall have the right to request such a bank guarantee in the event of a request for consent to an assignment or transfer of the obligations or rights of the other Party pursuant to the article 10 of these General Terms and Conditions or in the event of a proposed or consummated transfer of control over the other Party.

16.4 If any provision of this Agreement is determined by a court or other competent authority to be invalid, illegal or unenforceable, such invalidity, illegality or unenforceability shall not affect the validity, legality or enforceability of any other provision of this Agreement.

16.5 The signing persons are duly authorised by legal and corporate rules to represent and engage their respective Party and declare to act within the authority delegated to them. Any Party to the Agreement may require proof of the powers delegated to the person representing and engaging the other Party.

16.6 Notwithstanding the right of a Party to modify unilaterally prices under this Agreement as provided in the relevant Service Annex, any modification to this Agreement must be mutually agreed upon in writing.

16.7 Each Party hereby undertakes that, at the date of the entering into force of this Agreement there are no regulatory constraints to contract the Services, nor any embargo's adverse to contracting the Services with the other Party. Each Party further agrees that it will inform the other Party in the event a regulatory or legal constraint would raise.

Article 17 Disputes

The Agreement and the relationship of the Parties in connection with the subject matter of the Agreement shall be governed by and determined in conformity with Belgian law. Any dispute shall be brought before Brussels courts.

Article 18 Anti-Corruption

18.1. Each Party hereby undertakes that, at the date of the entering into force of this Agreement, itself, its directors, officers or employees have not offered, promised, given, authorized, solicited or accepted any undue pecuniary or other advantage of any kind (or implied that they will or might do any such thing at any time in the future) in any way connected with the Agreement and that it has taken reasonable measures to prevent subcontractors, agents or any other third parties, subject to its control or determining influence, from doing so.

18.2. The Parties agree that, at all times in connection with and throughout the course of the Agreement and thereafter, they will comply with and that they will take reasonable measures to ensure that their subcontractors, agents or other third parties, subject to their control or determining influence, will comply with the following provisions:

18.2.1. Parties will prohibit the following practices at all times and in any form, in relation with a public official at the international, national or local level, a political party, party official or candidate to political office, and a director, officer or employee of a Party, whether these practices are engaged in directly or indirectly, including through third parties:

a) Bribery is the offering, promising, giving, authorizing or accepting of any undue pecuniary or other advantage to, by or for any of the persons listed above or for anyone else in order to obtain or retain a business or other improper advantage, e.g. in connection with public or private procurement contract awards, regulatory permits, taxation, customs, judicial and legislative proceedings.

Bribery often includes:

(i) kicking back a portion of a contract payment to government or party officials or to employees of the other contracting Party, their close relatives, friends or business partners or

(ii) using intermediaries such as agents, subcontractors, consultants or other third parties, to channel payments to government or party officials, or to employees of the other contracting Party, their relatives, friends or business partners.

b) Extortion or Solicitation is the demanding of a bribe, whether or not coupled with a threat if the demand is refused. Each Party will oppose any attempt of Extortion or Solicitation and is encouraged to report such attempts through available formal or informal reporting mechanisms, unless such reporting is deemed to be counter-productive under the circumstances.

c) Trading in Influence is the offering or Solicitation of an undue advantage in order to exert an improper, real, or supposed influence with a view of obtaining from a public official an undue advantage for the original instigator of the act or for any other person.

d) Laundering the proceeds of the Corrupt Practices mentioned above is the concealing or disguising the illicit origin, source, location, disposition, movement or ownership of property, knowing that such property is the proceeds of crime.

"Corruption" or "Corrupt Practice(s)", as used in this ICC Anti-corruption Clause, shall include Bribery, Extortion or Solicitation, Trading in Influence and Laundering the proceeds of these practices.

18.2.2. With respect to third parties, subject to the control or determining influence of a Party, including but not limited to agents, business development consultants, sales representatives, customs agents, general consultants, resellers, subcontractors, franchisees, lawyers, accountants or similar intermediaries, acting on the Party's behalf in connection with marketing or sales, the negotiation of contracts, the obtaining of licenses, permits or other authorizations, or any actions that benefit the Party or as subcontractors in the supply chain, Parties should instruct them neither to engage nor to tolerate that they engage in any act of corruption; not use them as a conduit for any corrupt practice; hire them only to the extent appropriate for the regular conduct of the Party's business; and not pay them more than an appropriate remuneration for their legitimate services.

18.3. If a Party, as a result of the exercise of a contractually-provided audit right, if any, of the other Party's accounting books and financial records, or otherwise, brings evidence that the latter Party has been engaging in material or several repeated breaches of Paragraphs 18.1 and 18.2 above, it will notify the latter Party accordingly and require such Party to take the necessary remedial action in a reasonable time and to inform it about such action. If the latter Party fails to take the necessary remedial action or if such remedial action is not possible, it may invoke a defence by proving that by the time the evidence of breach(es) had arisen, it had put into place adequate anti-corruption preventive measures, as described in Article 10 of the ICC Rules on Combating Corruption 2011, adapted to its particular circumstances and capable of detecting corruption and of promoting a culture of integrity in its organization. If no remedial action is taken or, as the case may be, the defence is not effectively invoked, the first Party may, at its discretion, either suspend or terminate the Agreement, it being understood that all amounts contractually due at the time of suspension or termination of the Agreement will remain payable, as far as permitted by applicable law.

18.4. Any entity, whether an arbitral tribunal or other dispute resolution body, rendering a decision in accordance with the dispute resolution provisions of the Agreement, shall have the authority to determine the contractual consequences of any alleged non-compliance with this ICC Anti-corruption Clause.

Article 19 Security requirements

19.1. The Parties shall ensure that the Services will comply with the security requirements as defined in this article and in the Annexes, if applicable, and with the provisions of their respective applicable laws and regulations.

19.2. Each Party shall ensure that the information disclosed under this Agreement will be treated by its staff, contractors and third parties acting on its behalf in accordance with the provisions of the article 9 of this Agreement.

19.3. Each Party will use all reasonable efforts to identify vulnerabilities, threats or risks linked to the Services at any time during the term of this Agreement. Each Party shall advise the other Party in case of security related flaws.

19.4. The Parties shall advise each other immediately on becoming aware of any security breach, potential security breach or any suspected misuse that may affect the Services.

Parties shall collaborate in order to eliminate any kind of security incident.

19.5. Each Party shall implement the necessary business continuity measures and, if required, the recovery and testing plans associated to the Services.

APPENDIX 1 – CORPORATE REFERENCES AND CONTACT, FINANCE AND BANKING DETAILS

Corporate information	
	BICS
Full name of the company	Belgacom International Carrier Services
Legal form	Société Anonyme (S.A.)
Date of incorporation	August 27, 2004
Registered office	Boulevard Roi Albert II 27, 1030 Brussels, BELGIUM
Number VAT registration	BE 0866.977.981

General Contact details	
Prices lists	carrier.pricelist@bics.com
e-invoices	bics.billing@bics.com
Disputes	disputes@bics.com
Suspension notices related to 4.2.5	settlements@bics.com
Notices related to security payment	credit.risk.mgt@bics.com
Formal legal notices	Legal@bics.com
Numbering plan	plan.numbering@bics.com
Customer Care	customer.care@bics.com

Any changes to the data included in this Appendix must be sent without delay to the following addresses:
For BICS: refdata@bics.com

APPENDIX 2 - DATA PROCESSING AGREEMENT ("DPA")

IN CONSIDERATION OF THE FOLLOWING:

A. The Parties are entering into the Agreement for the provision of Services by a Party to the other as described in the Agreement (here below he "**Services**").
B. Under a Service Annex, a Party may process certain personal data on behalf of the other Party or of the other Party's own customers, such data being made available by that other Party directly or indirectly under the Agreement or any related document.

PARTIES AGREE AS FOLLOWS:

1. Definitions

For the purpose of this DPA, the following definitions shall apply:

- "**Affiliates**" means any legal entity, existing, to be acquired or to be created, that directly or indirectly (i) is Controlled by, (ii) Controls, or (iii) is under common Control with the Customer, whereby the term "**Control**" and its derivatives as used herein shall refer to the possession of the power to direct or cause the direction of the management and the policies of an entity, whether through the ownership of a majority of the outstanding voting rights or by contract or otherwise;
- "**Applicable Data Protection Law**" shall mean Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, "GDPR")), together with any replacement legislation or any equivalent legislation of any other applicable jurisdiction and all other applicable laws and regulations in any relevant jurisdiction relating to the processing of personal data and privacy (such as, without limitation, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector as may be amended from time to time);
- "**Schedule**" shall mean a schedule to this Appendix 2, which shall form an integral part of this DPA; and
- The terms used in this DPA shall have their meanings given in the Applicable Data Protection Law.

2. Processing of personal data

2.1 The provisions of this DPA shall apply to the extent a Party would process, on behalf of the other, any personal data provided by that other Party or its Affiliates, directly or indirectly, in connection with the Agreement as described in the Data Processing Schedule attached to this DPA (the "**Data**"). With regard to the processing of such Data, the Party processing the Data on behalf of the other will act as processor (the "**Processor**") and the Party on which behalf the Data is processed will act as controller (the "**Controller**"). Data may include personal data relating to (a) end-users of a Party's or its Affiliates' customers and/or (b) individuals who are employed by or have a working relationship with a Party or its Affiliate. Processing may include processing by a Party or any of its Affiliates.
2.2 Each Party shall fully comply with the obligations that apply to it under the Applicable Data Protection Law. It is expressly agreed upon between the Parties that the Data shall remain at all times the Controller's property.

2.3 In its capacity as Processor, a Party shall:
(a) Treat the Data as Confidential Information and process the Data solely and exclusively for the purpose of providing Services to the Controller and on Controller's behalf. The processing by the Processor shall consist of all permitted processing operations as stipulated in the Data Processing Schedule or in the Agreement. The categories of personal data to be processed by the Processor will be limited to the Data that are necessary to deliver the Services to the Controller. The duration of the processing by the Processor is limited to the duration described in the Agreement or the Data Processing Schedule.
(b) The Processor shall provide at all times durink,kg the performance of this DPA sufficient guarantees for its compliance with the requirements of the Applicable Data Protection Law. The Processor shall not process any Data for purposes other than that which is strictly necessary for the performance of its obligations under the Agreement and shall only process the Data strictly in accordance with the Controller's documented instructions (the "**Permitted Purpose**") given in this DPA, the Agreement or by any other means during the performance of this DPA. If the Processor would be required by any applicable legislation to process any Data otherwise than as permitted herein, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. The Processor shall immediately inform the Controller if, in its opinion, an instruction infringes the Applicable Data Protection Law and shall provide details of the breach or potential breach.
(c) Implement appropriate and sufficient, technical and organisational security measures prior to and during processing of any Data to protect the security, confidentiality and integrity of the Data and to protect the Data against any form of accidental, unlawful or unauthorized processing. In particular, without limitation, the Processor shall protect the Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, use or access to Data transmitted, stored or otherwise processed and against any form of unlawful processing. The Processor shall ensure a level of security appropriate to the risks presented by the processing of Data and the nature of such Data. Such measures shall include, as appropriate:

- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

- The ability to restore the availability and access to the Data in timely manner in the event of a physical or technical incident;
- A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- At a minimum, such measures shall include the organizational and technical measures, which meet or exceed relevant industry practice. These measures shall remain in place throughout the duration that Processor provides Services to the Controller or until Processor ceases to process Data (whichever is later);

(d) Treat Data with strict confidence and take all appropriate steps to ensure that disclosure of or access to Data is restricted to its employees, consultants or agents that strictly require such Data to perform the tasks allotted to them by the Processor in the performance of the Processor's obligations under the Agreement (the "**Authorized Persons**") and excluding all access to Data which are not strictly necessary for the Authorized Persons to perform its part of the Services. The Processor shall ensure that the Authorized Persons who will process Data:

- Are aware of and shall comply with the provisions of this DPA;
- Are under a duty of confidentiality with respect to the Data no less restrictive than the duties set forth herein prior to any access to the Data. Processor shall ensure that such confidentiality obligations survive the termination of the employment or contracting agreement;
- Have received appropriate training in relation to the Applicable Data Protection Law;
- Are subject to user authentication and log-on processes when accessing the Data; and
- Shall only process the Data as necessary for the Permitted Purpose and in accordance with the Controller's instructions.

(e) Not engage any subcontractor for the processing of Data without the Controller's prior written specific or general written authorisation approval (the "**Approved Sub-processor**"), to be provided in Controller's sole discretion but not to be unreasonably withheld. In the frame of the Parties' relationship as of the date of this Agreement, each Party allows the other to be assisted by subcontractors strictly with a view to deliver and improve the agreed Services, provided said Party has contracted with said subcontractors with terms substantially similar to the ones included herein. When the use of subcontractors does not fall within the scope of the present general authorization, the Processor shall inform the Controller at least one month in advance and by means of a written communication about its intention to engage a subcontractor, including details on the identity of the subcontractor, the location where the Data will be processed by such subcontractor and the concerned data processing activities. The Processor will enter into written contracts with such Approved Sub-processor guaranteeing at least a level of data protection and information security as provided for herein and in any event Processor will remain fully liable to the Controller for any breach of the Approved Sub-processor that is caused by an act, error or omission of the Approved Sub-processor. The Processor shall maintain and provide upon reasonable request a copy of the list of concerned subcontractors. If the Controller would refuse to consent to the appointment of a subcontractor on grounds relating to the protection of the Data, then the Processor will not appoint such subcontractor.

3. International transfers of personal data

The Processor or any Approved Sub-processor shall not process or transfer any Data (nor permit the Data to be transferred) outside of the European Economic Area unless an adequate level of protection in accordance with the Applicable Data Protection Law is ensured (the "Safeguards"). Such Safeguards may include without limitation: (1) a transfer is to countries which do ensure an adequate level of data protection according to an adequacy decision of the European Commission, or (2) such transfer is needed for the performance of the Agreement, or (3) it is governed by the latest version of the EU Standard Contractual Clauses (Controller to Controller module), which are to be found on BICS website.

4. Duty to Notify and Cooperate

Processor shall promptly give written notice to and/or shall fully cooperate with the Controller:

(a) if for any reason (i) Processor cannot comply, or has not complied, with any portion of this DPA, (ii) it would be in breach of or has breached any Applicable Data Protection Law governing its processing of Data, or (iii) Applicable Data Protection Law no longer allows the lawful transfer of Data from the Controller to Processor. In such cases, Processor shall take all reasonable, necessary and appropriate steps to remedy any non-compliance, or cease further processing of Data, and the Controller may immediately terminate the Agreement and this DPA or access to Data, or take any other necessary action, as determined in its sole discretion;

(b) to enable the Controller to comply with its obligations with regard to the security of the processing of Data, taking into account the nature of the processing and the information available to the Processor;

(c) upon becoming aware of any Data breach or suspected Data breach. In such case, the Processor shall promptly inform the Controller of the (suspected) Data breach without undue delay and shall provide all such timely information and cooperation as the Controller may reasonably require including in order for the Controller to fulfil its data breach reporting obligations under (and in accordance with the timescales required by) Applicable Data Protection Law. Processor shall further take all such measures and actions as are necessary to remedy or mitigate the effects of the (suspected) Data breach and shall keep the Controller up-to-date about all developments in connection with the (suspected) Data breach;

(d) in the preparation of any data protection impact assessments performed by the Controller, whether on a mandatory or voluntary basis. The Processor shall provide the Controller with all such reasonable and timely assistance as the Controller may require in order to conduct a data

protection impact assessment in relation to the Data and, if necessary, to consult with its relevant data protection authority. Processor agrees and acknowledges that if the Controller receives a request from a data protection authority, the Controller may share the terms of this DPA, the Agreement and any other information Processor provides to demonstrate compliance with this DPA or Applicable Data Protection Law.

In addition to the foregoing, if the Processor believes or becomes aware that its processing of the Data is likely to result in a high risk (as defined in the Applicable Data Protection Law, relevant regulatory guidance and case law) with regard to the data protection rights and freedoms of data subjects, it shall promptly inform the Controller.

(e) cooperate, at its own expense, as requested by the Controller to enable it to respond and comply with (i) the exercise of rights of data subjects pursuant to Applicable Data Protection Law (such as their right of access, right to rectification, right to object to the processing of their personal data, right to erasure, right to restriction of processing of their personal data and their right to data portability) and (ii) any other correspondence, enquiry or complaint received from a data subject, regulatory authority or any other third party in respect of Data processed by the Processor under this DPA.

The Processor shall promptly inform the Controller of any requests relating to the exercise of such rights or complaints, enquiry or correspondence if they are received directly by Processor and shall provide all details thereof. Furthermore, Processor shall provide all Data requested by the Controller, within a reasonable timescale specified by the Controller and shall provide such assistance to the Controller to comply with the relevant request within the applicable timeframes. Processor understands that any response to such direct requests requires prior written authorization from the Controller. If necessary, the Processor shall co-operate with the competent supervisory authority;

(f) upon the Controller's request, to make all such records, appropriate personnel, data processing facilities and any relevant materials available relating to the processing of the Data available to the Controller in order to allow the Controller to demonstrate compliance with its obligations laid down in the Applicable Data Protection Law. In particular, the Controller or a third party appointed by the Controller (the "**Auditor**") may enter the Processor's premises and more specifically the rooms or locations where the Data is processed by the Processor to verify Processor's compliance hereunder, provided that such inspection shall be carried out with reasonable notice (except where such notice would defeat the purpose of the Audit) during regular business hours and under a duty of confidentiality. The Controller or the Auditor may inspect, audit and copy any relevant records, processes and systems to verify compliance with the Applicable Data Protection Law and this DPA. The Controller shall take all reasonable measures to prevent unnecessary disruption to the Processor's operations. The Controller will not exercise its inspection rights as set forth in this clause more than once in any twelve (12) calendar month period, except (i) if and when required by instruction of a competent data protection authority or (ii) the Controller believes a further audit is necessary due to a Data breach suffered by the Processor.

5. Effect of Termination

As soon as it is no longer required for the performance of the Services and at the latest upon the expiration or termination of the Agreement, Processor shall promptly notify the Controller of all Data in its possession and promptly return or delete all such Data (at the Controller's sole election) and any existing copies thereof, at Processor's sole expense, unless any applicable law requires the further storage of the Data. The Processor shall certify to the Controller that all Data has been returned or destroyed in accordance with the foregoing and Controller's instructions. If the Processor cannot destroy or delete the Data due to technical reasons, the Processor will immediately inform the Controller and will take all appropriate steps to:

- Come to the closest possible to a complete and permanent deletion of the Data and to fully and effectively anonymize the remaining Data; and
- Make the remaining Data which is not deleted or effectively anonymized unavailable for any further processing except to the extent required by any applicable law.

6. Indemnification

The Processor acknowledges that the obligations set forth in this DPA are essential and that any violation thereof may seriously harm the Controller. The Processor shall have full and sole liability for all damages resulting from a failure on its part to comply with the provisions of this DPA. Should any data subject to whom the Data relates, a data protection authority or any other regulatory body lodge a claim for compensation against the Controller that results from the Processor's breach of its obligations under the Applicable Data Protection Law (a "**Claim**"), the Processor shall assist and intervene in the Controller's defence against such Claim upon the Controller's request and shall indemnify and hold harmless the Controller against all costs and damages resulting from such Claim. The Controller shall give the Processor prompt written notice of any such Claim and shall provide all reasonable cooperation in the defence and settlement of such Claim, at the Processor's expense. The Controller shall not make any admission as to the Processor's liability in respect of such a Claim and shall not agree to any settlement in respect of such a Claim without the Processor's written consent.

7. Order of Precedence

In the event of a conflict between the provisions of this DPA and those of the Agreement in respect of the processing and protection of Data, the provisions of this DPA will prevail. Except as expressly modified herein, all terms and conditions of the Agreement shall remain in full force and effect.

Schedule 1 to Appendix 2 : Data Processing Schedule

1. Categories of Data

The Data processed are the personal data provided by the Controller to the Processor in connection with the services provided by the Processor, which may include first name, last name, address, e-mail address, telephone number, location data, contact information, log-in information.

2. Categories of data subjects

Data subjects are the persons whose Data are processed by the Data Processor may include end users or employees and members of the staff of the Controller

3. Permitted processing operations for the Processor

The processing consists of all data processing activities that are performed following the instructions of the Controller and that are necessary to deliver the Services to the Controller and for the Permitted Purposes, or as otherwise required by law.

4. Permitted Purposes

The Processor may process Data in accordance with the purposes set out in the Agreement and, generally, to provide its Services to the Controller; for fraud detection, prevention and mitigation purposes; for maintaining and enhancing the Services it or its Affiliates offer, as well as to enhance or further develop its services' offer or the one of its Affiliates as contracted by other customers, as the case may be by processing Data in aggregated form only; as required and permitted by law.

5. Duration

The duration of the processing is limited to the duration needed to perform its obligations under the Agreement, unless a legal obligation applies. The obligations of the Processor with regard to the Data processing shall in any case continue until the Data have been properly deleted or have been returned at the request of the Controller