voxbone

is now ⦿ bandwidth

DATA PROCESSING AGREEMENT

RECITALS

(A) This Data Processing Agreement (hereinafter "DPA") is entered into by and between Customer and Voxbone SA (the "Parties") and governs the mutual obligations with regards to the processing of Personal Data that Customer transmits to Voxbone by using the telecommunications Services in accordance with the Terms of Sale and any applicable Addendums (hereinafter commonly referred to as the ''Agreement'').

(B) Customer enters into this DPA on its own behalf and, where required by applicable Data Protection Laws, in the name and on behalf of its Affiliates. For the purposes of this DPA, the term "Customer" shall include Customer and its Affiliates.

(C) In the event of a conflict between any of the terms of the Agreement and this DPA, the provisions of the following documents (in order of precedence) shall prevail: a. the Standard Contractual Clauses (''SCC''); b.this DPA; c. the Agreement.

(D) This DPA is incorporated into and subject to the terms of the Agreement and shall be effective and remain in force for the duration of the Agreement. Unless otherwise expressly stated in this DPA, the terms of the Agreement shall remain in full force and effect.

1. Definitions

1.1. In this DPA, the following terms shall have the meanings set out below and cognate terms shall be construed accordingly. Any capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement.

"Affiliate'' means in relation to a Party, any entity or person controlled by or under common control with that Party, so long as such control exists. For the purpose of this definition "control" shall be understood as the direct ownership of more than 50% of the voting capital or similar right of ownership of an entity, or the legal power to direct or cause the direction of the general management of that entity, whether through the ownership of voting capital, by contract or otherwise.

"**Data Protection Law(s)**" means: a. European Data Protection laws, as applicable: the GDPR, the Belgian Data Protection Act and all applicable laws in the EEA and b. data protection laws or regulations other than European Data Protection laws; including, where relevant, guidance and codes of practice issued by the supervisory authorities, any legislation and/or regulation implementing or made pursuant to them, or which amends, replaces, re-enacts or consolidates any of them.

"**Effective Date**" means: a. 25.05.2018 if Customer has accepted and signed the terms of the Agreement prior to or on such date; or b. the data on which Customer accepted and agreed to the terms of the Agreement, if such date is after 25.05.2018.

"**EEA**" means European Economic Area.

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

"Liability Cap" means the maximum amount at which a Party's liability is capped under the Agreement.

"**Personal Data Breach**" means any accidental, unauthorized or unlawful destruction, loss, alteration, or disclosure of, or access to Personal Data.

"**Privacy Shield**" means the EU-US Privacy Shield Framework and the Swiss-US Privacy Shield framework as set forth by the US Department of Commerce.

"**Service**" means the telecommunications services provided by Voxbone and that Customer has subscribed to under the terms of the Agreement.

"**Standard Contractual Clauses (SCCs)**" means the clauses approved by European Commission for the transfer of Personal Data to processors established in third countries: for controllers (C(2004)5721) and for processors (C(2010)593).

"**Subscribers**" means Customer's customer (a natural or legal person) purchasing or otherwise obtaining Voxbone's Service from Customer as an End User and using it for its own purposes and not for resale. "Subscriber" does not include Customer's employees or agents.

"**Sub-processor"** means any third parties authorized by the Data Controller, Data Processor or by any other sub-processor of the Data Processor to have access and process Personal Data in order to support the provision of the Service.

"Whitelisted country" means any third country that, according to the European Commission, ensures an adequate level of protection by reason of its domestic law or of the international commitments it has entered into.

1.2. The terms "Data Subject", "Personal Data", "Processing", "Data Controller", " Data Processor", "Sensitive Data" and "Supervisory Authority" as used in this DPA have the meanings given in the GDPR irrespective of the applicable Data Protection Law.

1.3. The terms "Data Importer" and "Data Exporter" have the meanings given in the SCCs irrespective of the applicable Data Protection Law.

2.   Details of the processing activities and roles of the Parties

Each Party agrees to process Personal Data received under the Agreement only for the purposes set forth in the Agreement. For the avoidance of doubt, the categories of Personal Data processed and the categories of Data Subjects relevant to this DPA are described herein.

2.1. Categories of Personal Data

a) Parties are independent Data Controllers for processing the following categories of Personal Data:
- Customer information, where such data qualifies as Personal Data, such as: name, email address, phone number and when required by law, additional Personal Data such as: birth date, physical address, nationality, identification card of the appointed representative of Customer.
- Customer's Subscribers Personal Data for the purpose of enabling the Service. Parties acknowledge that exceptionally, some additional Customer's Subscribers Personal Data such as personal ID or passports may be required for the provision of the Service.
- Traffic data (such as calling data records)
- any other category of Personal Data that Parties may agree to collect and process as independent Data Controllers for the purpose of provisioning the Service.

b) Voxbone is acting as a Data Processor with regards to the processing of the following categories of Personal Data:
- Customer Sensitive data for specific Services that Customer may have subscribed to such as Speech Analytics, SMS and FAX Services.

2.2. Parties have identified the categories of Data Subjects in the SCCs. Categories of Data Subjects whose Personal or Sensitive Data may be processed in order to perform the Services may include, among others, Customer representatives, employees, consultants and Subscribers.

2.3. Scope of Processing

By entering into this DPA, Customer instructs Voxbone to process Customer Personal Data and Sensitive Data in accordance with the applicable Data Protection Law in order to : a. provide the Service purchased by Customer; b.as specified further to Customer in the context of usage of the Service (including in the Customer webportal account, Voxbone website and description of the specific Service subscribed to by Customer); c. as described in the Agreement, including this DPA; d. comply with other applicable laws and regulations related to the nature of the Service, such as but not limited to telecommunications laws, national security provisions, lawful interception requirements and e. as further documented in any other written instructions given by Customer and agreed by Voxbone as instructions for the purpose of the DPA.

Voxbone will follow the above instructions, including with regards to Personal Data transfers, unless otherwise provided in the applicable Data Protection Law, in which case Voxbone will inform Customer (unless that law prevents Voxbone to do so due to public or security interests).

Customer acknowledges and agrees that Voxbone is not responsible for performing any legal research with regards to instructions received and shall have no liability in case Customer instruction infringes the applicable Data Protection Law.

In case further instructions are given by Customer as Data Controller to Voxbone as Data Processor, Parties agree to negotiate in good faith any charges or fees that may be incurred by Voxbone to comply with such instructions regarding the Processing of Personal Data which would require different or additional resources than those established for the provision of the Service.

3.   Obligations of the Parties

3.1. Obligations of Voxbone as a Data Processor

3.1.1. Voxbone shall comply with the following obligations:

a) Voxbone will process Personal Data on behalf of Customer and in accordance with its documented instructions unless otherwise required by EU or European Member State law to which Voxbone is subject.

b) Voxbone will process Personal Data for the purpose of providing and maintaining the Services or as otherwise instructed by Customer, in accordance with this DPA.

c) Any Personal Data that is no longer required for the purposes for which it was gathered will be deleted or returned to Customer –upon Customer's reasonable request- unless otherwise required by applicable law. In such case, Voxbone agrees to preserve the confidentiality of the Customer Personal Data retained by it and that it will only process such Customer Personal Data after such date in order to comply with applicable laws.

d) Voxbone shall cause any Sub-processors to return all the Customer Personal Data and copies of such data to Customer or

securely destroy them, unless applicable laws prevent Voxbone from returning or destroying all or part of the Customer Personal Data disclosed.

e) Voxbone shall inform Customer immediately if it becomes aware (i) that its employees, Sub-processors and/or any third party engaged in the processing fail to comply with any requirements regarding the protection of Personal Data or any provisions of this DPA; and/or (ii) of any other irregularity in the processing of Customer's Personal Data.

f) If Customer is required under applicable Data Protection Laws to issue information to any Supervisory Authority regarding the processing of Personal Data, Voxbone shall use reasonable endeavours to support Customer in its efforts to provide such information.

g) Voxbone will inform Customer promptly if, in Voxbone's opinion, an instruction from Customer violates applicable Data Protection Laws.

3.1.2. Sub-processors
a) Customer specifically acknowledges and authorizes Voxbone to engage with third-party Sub-processors for the performance of the Agreement. Any such Sub-processor will process Personal Data with the purpose of delivering the Services or in response to authorized law enforcement or any other public authorities requests.

b) Voxbone will use reasonable endeavours to ensure the reliability and competence of its Sub-processors and shall agree with them to protect and process the Personal Data under terms and conditions that comply, as a minimum, with GDPR requirements.

3.2. Obligations of the Parties as Data Controllers

3.2.1. The Parties shall comply with the following obligations:

a) They will treat all Personal Data as confidential information and not disclose such Personal Data except (i) to personnel and third Parties who need to process Personal Data in relation to the provision of the Services; and (ii) where it is required by a court to disclose Personal Data, or where there is a statutory or legal obligation to do so, but only to the minimum extent necessary to comply with such court order, statutory obligation or law enforcement authorities' request.

b) They will take reasonable steps to ensure that their personnel who have access to the Personal Data (i) are adequately informed with regards to handling Personal Data; (ii) are obliged to keep Personal Data confidential; and (iii) comply with their duties and obligations in accordance with this DPA.

c) If any of the Parties is required by any relevant authority to process any Customer Personal Data for a reason other than providing the Services described in the Agreement, the affected party will inform the other of this requirement in advance of any processing, unless the affected party is prohibited by law or a relevant authority from informing the other party of such processing.

3.2.2. Customer shall comply with the following obligations:

a) Customer remains responsible for guaranteeing the rights of the concerned data subjects.

b) Customer shall support Voxbone in responding in a reasonable time to enquiries from any Supervisory Authority regarding the processing of relevant Personal Data.

c) Customer shall collect Subscribers Personal Data that may be transmitted by Customer to Voxbone,in order to ensure the provision of the Service under the Agreement. Customer, in its capacity of Data Controller, shall ensure that the processing of the Subscriber Personal Data complies with the applicable Data Protection Laws and that prior information has been provided to the Subscriber with respect to the purpose of the data processing. Where required, based on the type of Subscriber Personal Data and the purpose of the processing, Customer shall ensure that the Subscriber has given his or her consent unambiguously for the processing of such data.

d) Customer shall maintain the Subscriber Personal Data up to date at all times during the provision of the Service and shall always ensure that the Subscriber Personal Data provided to Voxbone corresponds at all times with the information of the effective Subscriber of a specific number.

3.2.3. Storage and erasure of data

a) The Parties shall store the Personal Data as long as it is needed for the provision of the Services and/or for compliance with authorities' requests, in accordance with Data Protection Laws and any other applicable national laws.

b) The Parties must store the Personal Data with reasonable care, together with any copies made of such Personal Data securely so that it is not accessible to third parties or non-authorized personnel.

3.2.4. Data access and modification

a) The Parties shall permit Data Subjects access to their respective Personal Data. In particular, Data Subjects shall be permitted to correct, amend or delete inaccurate Personal Data at no additional cost.

b) Both Parties agree that, in the event of receiving a Data Subject complaint or access request that may involve the other Party, they will notify the other party without delay and will provide such cooperation and assistance as may be reasonably required to enable that Party to deal with any Data Subject complaint or access request in accordance with the provisions of the applicable Data Protection Law.

4.   International data transfers

4.1. Customer acknowledges that, for the purposes described in clause 2, Customer's Personal Data may be transferred outside the EEA in the following cases:

a) Some of Voxbone's personnel outside the EEA may have access to Customer's Personal Data. However, all members of personnel, regardless of their location, will comply with the same internal policies and security measures, in accordance with the GDPR.

b) Voxbone may work with third party providers located outside the EEA. In this case, the third party provider shall ensure compliance as Data Importer, as set out in the EU Commission's "Controller-to-Processor Standard Contractual Clauses " for the transfer of Personal Data to processors established in third countries, or in case of transfers to the United States, ensure adherence to the U.S.-EU Privacy Shield. To the extent the EU-US Privacy Shield is invalidated, the third party provider shall ensure compliance as Data Importer, as set out in the EU Commission's "Controller-to-Processor Standard Contractual Clauses ".

4.2. Parties agree to comply with the obligations set out in the EU Commission's Controller-to-Controller Standard Contractual Clauses – Set II 2004 for the transfer of Personal Data to third countries and the "Controller-to-Processor Standard Contractual Clauses ", whereby Customer will be regarded as the Data Exporter and Voxbone will be regarded as the Data Importer. These clauses are part of Annex 2.

4.3. Voxbone agrees that it will provide additional information to Customer about the transfer and will cooperate, without delay, where this is required by a Supervisory Authority in the EEA. In the event that the European Commission revokes or adapts the decision that it made approving the Standard Contractual Clauses, the Privacy Shield frameworks or the list of Whitelisted Countries , the Parties will negotiate in good faith a solution to allow transfer of Personal Data to be carried out in compliance with the GDPR and applicable Data Protection Law.

5.   Security measures

5.1. In order to comply with article 32 of the GDPR and taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights of Data Subjects, the Parties shall maintain appropriate organizational and technical security measures to protect Personal Data against unauthorized or accidental access, loss, alteration, damage, theft, disclosure or destruction of Customer's Personal Data. These measures shall be appropriate to the harm which might result from any unauthorized or unlawful processing, accidental loss, destruction, damage or theft of the Personal Data and having regard to the nature of the Personal Data which is to be protected.

5.2. The Parties shall ensure that Personal Data cannot be read, copied, modified or removed without authorization during electronic transmission, transport or storage and that it is possible to examine, control and establish to which Parties the transfer of Personal Data is envisaged.

5.3. As a minimum, the measures to be adopted by the Parties are specified in Annex 1.

6. Data Breaches

6.1. Voxbone shall notify Customer promptly and in writing if it becomes aware of any Personal Data Breach and promptly take reasonable steps to minimize harm and secure Customer Personal Data. Voxbone notification of the Personal Data Breach will not be construed as an acknowledgement by Voxbone of any fault or liability with regards to the Personal Data Breach.

6.2. Voxbone will investigate the Personal Data Breach and provide the Customer, to the extent possible, with a detailed description, the type of data and other Personal Data that was the subject to the breach including the reasonable steps taken to mitigate the potential risks and steps that Voxbone may recommend Customer to take to address and minimize the Personal Data Breach. Voxbone will send the description of the data breach to the contact person identified in the Customer account. Therefore, Customer shall be responsible for ensuring that such contact details remain valid.

6.3. Customer shall not release or publish any filing, communication, notice, press release, or report concerning the Data Breach without Voxbone prior written approval (except where it is required to do so by law).

6.4. For the categories of Personal Data where Customer acts as Data Controller, Customer acknowledges and agrees that it will remain responsible for informing the affected Data Subjects of the Personal Data Breach and shall be solely responsible to provide third party notifications in accordance with the applicable Data Protection Laws regarding breach notifications.

7. Liability

7.1. Parties agree that the liability provisions set out in the Agreement and the respective Liability Cap shall apply to this DPA, including the SCCs. Notwithstanding anything to the contrary, Voxbone shall not be liable for any damages arising from Voxbone's compliance with Customer's instructions or specifications.

7.2. The Parties shall be liable for the acts and omissions of its Sub-processors to the same extent that the relevant party would be liable if performing the Services of each Sub-processor directly under the terms of this DPA.

8. Term

8.1. The term of this DPA shall be coextensive with the term of the Agreement. All Parties' obligations under this DPA shall terminate upon expiration or termination of the Agreement, unless otherwise mandated under the applicable Data Protection Law.

9. Miscellaneous

9.1 This DPA is intended to ensure an adequate level of protection of Personal Data processed by Parties in the context of the Service and does not otherwise affect the rights and obligations under any other agreements between the Parties.

9.2. Should any provision of this DPA be held invalid or unenforceable, then the remainder of this DPA shall remain valid and in force. The invalid or unenforceable provision shall be either (i) amended as necessary to ensure its validity and enforceability, while preserving the Parties' intentions as closely as possible or, if this is not possible, (ii) construed in a manner as if the invalid or unenforceable part had never been contained therein.

9.3. Voxbone may propose any other variations to this DPA which reasonably considers to be necessary to address the requirements of Data Protection Laws.

10. Applicable Law

This DPA and any contractual obligations arising out of or in relation to it shall be governed by Belgian law. Any dispute between the Parties arising out of or relating to this DPA shall be exclusively submitted to the French speaking courts of Brussels.

This DPA is made in two originals, each Party acknowledging having received one.

For Voxbone: DocuSigned by:

Stef Konings
6222F17E4AB24ED...

Name: Stef Konings

Title: CFO

For Customer:

Name:

Title:

Date:

ANNEX 1: Technical Security Measures

1. Data Centers

All data centers should provide the full range of hosting facility features such as fully redundant power as well as the highest levels of security.

Datacenter access is logged and monitored. 24x7 onsite staff provides additional protection against unauthorized entry.

Multiple levels of power redundancy, heating, ventilation and air conditioning (HVAC) should be provided at the highest level of availability.

Parties should replicate and backup data over multiple systems to help to protect against accidental destruction or loss.

Parties have designed and regularly plans and tests its business continuity planning/disaster recovery programs.

2. Network and transmission

The data centers should be connected via high-speed private links to provide secure and fast data transfer. This is designed to prevent data from being read, copied, altered or removed without authorization during electronic transfer or transport or while being recorded onto data storage media.

The datacenters should contain redundant network connectivity with multiple Internet Service Providers, and should employ robust routing to allow network traffic to take the best path.

Parties should provide encryption when communicating with the application so that no data is transferred in clear text. Also referred to as TLS connection, minimum protocol has to be TLS 1.1.

Logical access to the datacenters is restricted and protected by firewalls and network isolation.

3. Data storage

For data protection, Parties should use effective and efficient storage-based technologies that enable daily "snapshot" backups. These can be used within a datacenter for quick data recovery. For offsite backups, Parties should mirror all production data to a different datacenter at least once every 24 hours or less.

4. Service continuity

Parties load-balance at every tier in the infrastructure, from the network to the database servers. Application server clusters are enabled to ensure that servers can fail without interrupting the user experience. Database servers are clustered for failover.

5. Decommissioning

Certain disks containing data may experience performance issues, errors or hardware failure that lead them to be decommissioned ("Decommissioned Disk"). Every Decommissioned Disk has to be subject to a series of data destruction processes before leaving Parties' premises either for reuse or destruction.

For Voxbone:

DocuSigned by:

Stef Konings

6222F17E4AB24ED...

Stef Konings

Name:

Title: CFO

For Customer:

Name:

Title:

Date:

ANNEX 2: Model Clauses

Commission Decision C(2010)593

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation:

Address:

Other information needed to identify the organisation:

…………………………………………………………

(the data **exporter**)

And

Name of the data importing organisation: VOXBONE SA

Address: Avenue Louise 489, 1050 Brussels (Belgium)

Tel.: 02 808 00 00; e-mail: legal.intl@bandwidth.com

……………………………………………………………

(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a)   *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];

(b)   '*the data exporter'* means the controller who transfers the personal data;

(c)   *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d)   *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

---

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

(e) '*the applicable data protection law*' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures 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;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g)   to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h)   to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i)   that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j)   that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[2]

The data importer agrees and warrants:

(a)   to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b)   that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c)   that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d)   that it will promptly notify the data exporter about:

(i)   any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii)   any accidental or unauthorised access, and

(iii)   any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e)   to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f)   at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g)   to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h)   that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i)   that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j)   to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

---

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

Clause 6

Liability

1.   The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2.   If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3.   If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1.   The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

(a)   to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b)   to refer the dispute to the courts in the Member State in which the data exporter is established.

2.   The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1.   The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2.   The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3.   The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1.   The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[3]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2.   The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3.   The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.

4.   The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1.   The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2.   The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

On behalf of the data exporter:

Name (written out in full):

Position:

Address:

Other information necessary in order for the contract to be binding (if any):

Signature………………………………………..

On behalf of the data importer:

Name (written out in full): Stef Konings

Position: CFO

Address: Avenue Louise 489, 1050 Brussels, Belgium

Other information necessary in order for the contract to be binding (if any):

Signature………………………………………..

[3] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

Appendix 1 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter
The data exporter is (please specify briefly your activities relevant to the transfer):

Data importer
The data importer is (please specify briefly activities relevant to the transfer):
Telecommunications service provider.

Data subjects
The personal data transferred concern the following categories of data subjects (please specify):

- Calling and called parties (traffic data).
- Customer's Subscribers

Categories of data
The personal data transferred concern the following categories of data (please specify):
- any other category of Personal Data that Parties may agree to collect and process as independent Data Controllers for the purpose of provisioning the Service.

Special categories of data (if appropriate)
The personal data transferred concern the following special categories of data (please specify):

- Customer Sensitive data for specific Services that Customer may have subscribed to such as Speech Analytics, SMS and FAX Services

Processing operations
The personal data transferred will be subject to the following basic processing activities (please specify):

- Performance of the telecommunications Services contract, which include, but is not limited to: generation and storage of calling data records, the exchange of commercial communications between Voxbone and Customer, billing purposes, Customer administration, provisioning,verification of Customer identity and solvency, maintenance, support, fraud detection and prevention or sales purposes.
- Compliance with applicable national laws (including but not limited to Data Protection Laws, telecommunications laws).
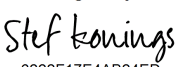- Response to information requests from relevant authorities.

DATA EXPORTER

Name:

Authorised Signature …………………….

DATA IMPORTER

Name: Stef Konings

Authorised Signature …………………….

DocuSigned by:

Stef konings

6222F17E4AB24ED…

is now ⓦ bandwidth

Appendix 2 to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

As described in Annex 1 of the DPA.

DATA EXPORTER

Name:

Authorised Signature ……………………

DATA IMPORTER

Name: Stef Konings

Authorised Signature ……………………

DocuSigned by:

Stef Konings

6222F17E4AB24ED…

Commission Decision C(2004)5721

SET II

Standard contractual clauses for the transfer of personal data from the Community to third countries (controller to controller transfers)

Data transfer agreement

between

.... (name)

.... (address and country of establishment)

hereinafter "data exporter"

and

Voxbone SA, with registered office at avenue Louise, 489, 1050 Brussels (Belgium)

hereinafter "data importer"

each a "party"; together "the parties".

Definitions

For the purposes of the clauses:

a)   "personal data", "special categories of data/sensitive data", "process/processing", "controller", "processor", "data subject" and "supervisory authority/authority" shall have the same meaning as in Directive 95/46/EC of 24 October 1995 (whereby "the authority" shall mean the competent data protection authority in the territory in which the data exporter is established);

b)   "the data exporter" shall mean the controller who transfers the personal data;

c)   "the data importer" shall mean the controller who agrees to receive from the data exporter personal data for further processing in accordance with the terms of these clauses and who is not subject to a third country's system ensuring adequate protection;

d)   "clauses" shall mean these contractual clauses, which are a free-standing document that does not incorporate commercial business terms established by the parties under separate commercial arrangements.

The details of the transfer (as well as the personal data covered) are specified in Annex B, which forms an integral part of the clauses.

I.   Obligations of the data exporter

The data exporter warrants and undertakes that:

a)   The personal data have been collected, processed and transferred in accordance with the laws applicable to the data exporter.

b)   It has used reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses.

c)   It will provide the data importer, when so requested, with copies of relevant data protection laws or references to them (where relevant, and not including legal advice) of the country in which the data exporter is established.

d)   It will respond to enquiries from data subjects and the authority concerning processing of the personal data by the data importer, unless the parties have agreed that the data importer will so respond, in which case the data exporter will still respond to the extent reasonably possible and with the information reasonably available to it if the data importer is unwilling or unable to respond. Responses will be made within a reasonable time.

e)   It will make available, upon request, a copy of the clauses to data subjects who are third party beneficiaries under clause III, unless the clauses contain confidential information, in which case it may remove such information. Where information is removed, the data exporter shall inform data subjects in writing of the reason for removal and of their right to draw the removal to the attention of the authority. However, the data exporter shall abide by a decision of the authority regarding access to the full text

of the clauses by data subjects, as long as data subjects have agreed to respect the confidentiality of the confidential information removed. The data exporter shall also provide a copy of the clauses to the authority where required.

II.   Obligations of the data importer

The data importer warrants and undertakes that:

a)   It will have in place appropriate technical and organisational measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, and which provide a level of security appropriate to the risk represented by the processing and the nature of the data to be protected.

b)   It will have in place procedures so that any third party it authorises to have access to the personal data, including processors, will respect and maintain the confidentiality and security of the personal data. Any person acting under the authority of the data importer, including a data processor, shall be obligated to process the personal data only on instructions from the data importer. This provision does not apply to persons authorised or required by law or regulation to have access to the personal data.

c)   It has no reason to believe, at the time of entering into these clauses, in the existence of any local laws that would have a substantial adverse effect on the guarantees provided for under these clauses, and it will inform the data exporter (which will pass such notification on to the authority where required) if it becomes aware of any such laws.

d)   It will process the personal data for purposes described in Annex B, and has the legal authority to give the warranties and fulfil the undertakings set out in these clauses.

e)   It will identify to the data exporter a contact point within its organisation authorised to respond to enquiries concerning processing of the personal data, and will cooperate in good faith with the data exporter, the data subject and the authority concerning all such enquiries within a reasonable time. In case of legal dissolution of the data exporter, or if the parties have so agreed, the data importer will assume responsibility for compliance with the provisions of clause I(e).

f)   At the request of the data exporter, it will provide the data exporter with evidence of financial resources sufficient to fulfil its responsibilities under clause III (which may include insurance coverage).

g)   Upon reasonable request of the data exporter, it will submit its data processing facilities, data files and documentation needed for processing to reviewing, auditing and/or certifying by the data exporter (or any independent or impartial inspection agents or auditors, selected by the data exporter and not reasonably objected to by the data importer) to ascertain compliance with the warranties and undertakings in these clauses, with reasonable notice and during regular business hours. The request will be subject to any necessary consent or approval from a regulatory or supervisory authority within the country of the data importer, which consent or approval the data importer will attempt to obtain in a timely fashion.

h)   It will process the personal data, at its option, in accordance with:

    i.   the data protection laws of the country in which the data exporter is established, or

    ii.   the relevant provisions[4] of any Commission decision pursuant to Article 25(6) of Directive 95/46/EC, where the data importer complies with the relevant provisions of such an authorisation or decision and is based in a country to which such an authorisation or decision pertains, but is not covered by such authorisation or decision for the purposes of the transfer(s) of the personal data[5], or

    iii.   the data processing principles set forth in Annex A.

Data importer to indicate which option it selects: iii

Initials of data importer:VB ;

i)   It will not disclose or transfer the personal data to a third party data controller located outside the European Economic Area (EEA) unless it notifies the data exporter about the transfer and

    i.   the third party data controller processes the personal data in accordance with a Commission decision finding that a third country provides adequate protection, or

---

[4] "Relevant provisions" means those provisions of any authorisation or decision except for the enforcement provisions of any authorisation or decision (which shall be governed by these clauses).

[5] However, the provisions of Annex A.5 concerning rights of access, rectification, deletion and objection must be applied when this option is chosen and take precedence over any comparable provisions of the Commission Decision selected.

ii.   the third party data controller becomes a signatory to these clauses or another data transfer agreement approved by a competent authority in the EU, or

iii.   data subjects have been given the opportunity to object, after having been informed of the purposes of the transfer, the categories of recipients and the fact that the countries to which data is exported may have different data protection standards, or

iv.   with regard to onward transfers of sensitive data, data subjects have given their unambiguous consent to the onward transfer

III.   Liability and third party rights

a)   Each party shall be liable to the other parties for damages it causes by any breach of these clauses. Liability as between the parties is limited to actual damage suffered. Punitive damages (i.e. damages intended to punish a party for its outrageous conduct) are specifically excluded. Each party shall be liable to data subjects for damages it causes by any breach of third party rights under these clauses. This does not affect the liability of the data exporter under its data protection law.

b)   The parties agree that a data subject shall have the right to enforce as a third party beneficiary this clause and clauses I(b), I(d), I(e), II(a), II(c), II(d), II(e), II(h), II(i), III(a), V, VI(d) and VII against the data importer or the data exporter, for their respective breach of their contractual obligations, with regard to his personal data, and accept jurisdiction for this purpose in the data exporter's country of establishment. In cases involving allegations of breach by the data importer, the data subject must first request the data exporter to take appropriate action to enforce his rights against the data importer; if the data exporter does not take such action within a reasonable period (which under normal circumstances would be one month), the data subject may then enforce his rights against the data importer directly. A data subject is entitled to proceed directly against a data exporter that has failed to use reasonable efforts to determine that the data importer is able to satisfy its legal obligations under these clauses (the data exporter shall have the burden to prove that it took reasonable efforts).

IV.   Law applicable to the clauses

These clauses shall be governed by the law of the country in which the data exporter is established, with the exception of the laws and regulations relating to processing of the personal data by the data importer under clause II(h), which shall apply only if so selected by the data importer under that clause.

V.   Resolution of disputes with data subjects or the authority

a)   In the event of a dispute or claim brought by a data subject or the authority concerning the processing of the personal data against either or both of the parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

b)   The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

c)   Each party shall abide by a decision of a competent court of the data exporter's country of establishment or of the authority which is final and against which no further appeal is possible.

VI.   Termination

a)   In the event that the data importer is in breach of its obligations under these clauses, then the data exporter may temporarily suspend the transfer of personal data to the data importer until the breach is repaired or the contract is terminated.

b)   In the event that:

i.   the transfer of personal data to the data importer has been temporarily suspended by the data exporter for longer than one month pursuant to paragraph (a);

ii.   compliance by the data importer with these clauses would put it in breach of its legal or regulatory obligations in the country of import;

iii.   the data importer is in substantial or persistent breach of any warranties or undertakings given by it under these clauses;

   iv. a final decision against which no further appeal is possible of a competent court of the data exporter's country of establishment or of the authority rules that there has been a breach of the clauses by the data importer or the data exporter; or

   v. a petition is presented for the administration or winding up of the data importer, whether in its personal or business capacity, which petition is not dismissed within the applicable period for such dismissal under applicable law; a winding up order is made; a receiver is appointed over any of its assets; a trustee in bankruptcy is appointed, if the data importer is an individual; a company voluntary arrangement is commenced by it; or any equivalent event in any jurisdiction occurs

then the data exporter, without prejudice to any other rights which it may have against the data importer, shall be entitled to terminate these clauses, in which case the authority shall be informed where required. In cases covered by (i), (ii), or (iv) above the data importer may also terminate these clauses.

c) Either party may terminate these clauses if (i) any Commission positive adequacy decision under Article 25(6) of Directive 95/46/EC (or any superseding text) is issued in relation to the country (or a sector thereof) to which the data is transferred and processed by the data importer, or (ii) Directive 95/46/EC (or any superseding text) becomes directly applicable in such country.

d) The parties agree that the termination of these clauses at any time, in any circumstances and for whatever reason (except for termination under clause VI(c)) does not exempt them from the obligations and/or conditions under the clauses as regards the processing of the personal data transferred.

VII. Variation of these clauses

The parties may not modify these clauses except to update any information in Annex B, in which case they will inform the authority where required. This does not preclude the parties from adding additional commercial clauses where required.

VIII. Description of the Transfer

The details of the transfer and of the personal data are specified in Annex B. The parties agree that Annex B may contain confidential business information which they will not disclose to third parties, except as required by law or in response to a competent regulatory or government agency, or as required under clause I(e). The parties may execute additional annexes to cover additional transfers, which will be submitted to the authority where required. Annex B may, in the alternative, be drafted to cover multiple transfers.

FOR DATA IMPORTER   FOR DATA EXPORTER

VOXBONE,SA

ANNEX A

DATA PROCESSING PRINCIPLES

1.   Purpose limitation: Personal data may be processed and subsequently used or further communicated only for purposes described in Annex B or subsequently authorised by the data subject.

2.   Data quality and proportionality: Personal data must be accurate and, where necessary, kept up to date. The personal data must be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further processed.

3.   Transparency: Data subjects must be provided with information necessary to ensure fair processing (such as information about the purposes of processing and about the transfer), unless such information has already been given by the data exporter.

4.   Security and confidentiality: Technical and organisational security measures must be taken by the data controller that are appropriate to the risks, such as against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, presented by the processing. Any person acting under the authority of the data controller, including a processor, must not process the data except on instructions from the data controller.

5.   Rights of access, rectification, deletion and objection: As provided in Article 12 of Directive 95/46/EC, data subjects must, whether directly or via a third party, be provided with the personal information about them that an organisation holds, except for requests which are manifestly abusive, based on unreasonable intervals or their number or repetitive or systematic nature, or for which access need not be granted under the law of the country of the data exporter. Provided that the authority has given its prior approval, access need also not be granted when doing so would be likely to seriously harm the interests of the data importer or other organisations dealing with the data importer and such interests are not overridden by the interests for fundamental rights and freedoms of the data subject. The sources of the personal data need not be identified when this is not possible by reasonable efforts, or where the rights of persons other than the individual would be violated. Data subjects must be able to have the personal information about them rectified, amended, or deleted where it is inaccurate or processed against these principles. If there are compelling grounds to doubt the legitimacy of the request, the organisation may require further justifications before proceeding to rectification, amendment or deletion. Notification of any rectification, amendment or deletion to third parties to whom the data have been disclosed need not be made when this involves a disproportionate effort. A data subject must also be able to object to the processing of the personal data relating to him if there are compelling legitimate grounds relating to his particular situation. The burden of proof for any refusal rests on the data importer, and the data subject may always challenge a refusal before the authority.

6.   Sensitive data: The data importer shall take such additional measures (e.g. relating to security) as are necessary to protect such sensitive data in accordance with its obligations under clause II.

7.   Data used for marketing purposes: Where data are processed for the purposes of direct marketing, effective procedures should exist allowing the data subject at any time to "opt-out" from having his data used for such purposes.

8.   Automated decisions: For purposes hereof "automated decision" shall mean a decision by the data exporter or the data importer which produces legal effects concerning a data subject or significantly affects a data subject and which is based solely on automated processing of personal data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc. The data importer shall not make any automated decisions concerning data subjects, except when:

a)   i.   such decisions are made by the data importer in entering into or performing a contract with the
data   subject, and

         ii.   the data subject is given an opportunity to discuss the results of a relevant automated decision
with a   representative of the parties making such decision or otherwise to make representations to that
parties.

or

b)   where otherwise provided by the law of the data exporter.

ANNEX B

DESCRIPTION OF THE TRANSFER

Data subjects

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

- Calling and called parties (traffic data).
- Customer's Subscribers
- Customer's commercial contacts and legal representatives.

Purposes of the transfer(s)

The transfer is made for the following purposes:

- Performance of the telecommunications Services contract, which include, but is not limited to: generation and storage of calling data records, the exchange of commercial communications between Voxbone and Customer, billing purposes, Customer administration, provisioning,verification of Customer identity and solvency, maintenance, support, fraud detection and prevention or sales purposes.
- Compliance with applicable national laws (including but not limited to Data Protection Laws, telecommunications laws).
- Response to information requests from relevant authorities.

Categories of data

The personal data transferred concern the following categories of data:

- Traffic data (such as calling data records)
- any other category of Personal Data that Parties may agree to collect and process as independent Data Controllers for the purpose of provisioning the Service.
- Customer information, where such data qualifies as Personal Data, such as: name, email address, phone number and when required by law, additional Personal Data such as: birth date, physical address, nationality, identification card of the appointed representative of Customer.
- Customer's Subscribers Personal Data for the purpose of enabling the Service.

Recipients

The personal data transferred may be disclosed only to the following recipients or categories of recipients:

- Employees of Voxbone outside the EEA
- Sub-processors

Sensitive data (if appropriate)

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

Data protection registration information of data exporter (where applicable)

Additional useful information (storage limits and other relevant information)

Contact points for data protection enquiries

Data importer   **Data exporter**

privacy@bandwidth.com   ……………………………………………………