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: .....

Tel.: ..... ; fax: ..... ; e-mail: .....

Other information needed to identify the organisation:

.....
(the data **exporter**)

And

Name of the data importing organisation: Blue Jeans Network, Inc.

Address: 3098 Olsen Drive, 2nd Floor, San Jose, CA 95128

Tel.: 408-550-2828; fax: .....; e-mail:.....

Other information needed to identify the organisation:

.....
(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;

(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;

(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

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.

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. 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.

Clause 13

Further Obligations

The data importer agrees:

1. it will ensure that where it receives a legally binding request from a law enforcement agency or state security body for disclosure of data exporter personal information transferred outside Europe, it will, unless prohibited from doing so by the requesting authority:
   - put the request on hold; and
   - promptly notify the data exporter and the supervisory authority competent for each of the
     data exporter and the processor.
2. if it outside Europe receives a legally binding request for disclosure of information transferred outside Europe and is prohibited by a law enforcement authority from
   putting the request on hold and/or from notifying the competent supervisory authorities, it will:
   - use its best efforts to obtain a waiver of this prohibition in order to communicate as much
     information as it can and as soon as possible to the competent supervisory authorities; and
   - demonstrate to the competent supervisory authorities the steps it followed to deal with the
     request in accordance with these provisions.

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……..

(stamp of organisation)

On behalf of the data importer:

Name (written out in full): David Squellati

Position: General Counsel

Address:3098 Olsen Drive, 2nd Floor, San Jose, CA 95128

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

Signature……..

(stamp of organisation)

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

Data Exporter:

The Data Exporter is:

The Customer of Blue Jeans Network, Inc. that has purchased and/or subscribed to certain BlueJeans Services ("Data Exporter"), specifically:

Name of the data exporting organisation: .....

Data Importer:

The Data Importer is:

Blue Jeans Network, Inc. (including subsidiaries) ("BlueJeans" or "Data Importer") and its Subprocessors provide certain cloud services that include the hosting of its video conferencing and collaboration services and the provision of related support ("BlueJeans Services") to Customer and its authorized users as contemplated the agreement between the Data Exporter and Blue Jeans Network, Inc. ("Agreement").

Data Subjects:

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

Unless otherwise provided by the Data Exporter, the Data Subjects may include the Data Exporter's employees, contractors, agents or other individuals that Data Exporter designates as a host user (with a unique username and password) of the BlueJeans Services that Data Exporter has purchased from BlueJeans pursuant to the Agreement.

Categories of Data:

The personal data transferred concern the following categories of data:

The Data Exporter determines the data transferred pursuant to the BlueJeans Services. This information may include:

- Data used for users to sign on (which may include single sign on user token information, first and/or last name, email address, authorization data, account information, pass codes, conference codes).
- Job title, employer name.
- Connection data.
- As requested by Data Exporter, conference recordings.
- Information provided for monitoring, training and quality purposes.

Special Categories of Data

BlueJeans' services are designated for general business use and not for processing of sensitive personal information. Any processing of special categories of data would be incidental.

Purpose of the Processing:

The processing is made for the following purposes to the extent that it is required for the delivery or support of BlueJeans Services:

- Account set up and account management for users.
- Support, maintenance and resolution of user inquiries.
- Invoicing and collection purposes.
- As specifically requested by Data Exporter, recording and storage of video files, allowing Data Exporter to download and share such files.

- Complying with legal obligations.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses.

Description of the technical and organizational measures implemented by the Data Importer in accordance with Clauses 4(d) and 5(c):

Technical and Organizational Measures

The following sections define the current security measures established by BlueJeans. These measures are subject to technical progress and development. Therefore, BlueJeans may change these measures at any time without notice ***provided*** that such changes result in a comparable or better level of security. In no event will changes to these measures diminish the security level. In addition, BlueJeans is entitled to terminate this agreement to the extent BlueJeans applies an alternative means to protect the information of the Data Subjects recognized by the US government and the European Commission

1. Physical Access Control:

Unauthorized persons shall be prevented from gaining physical access to premises, buildings or rooms where data processing systems that process and/or use personal data are located.

Measures:

All premises, buildings or rooms where data processing systems that process personal data are located adhere to physical security measures that may include:

- Restriction of access rights to the minimum necessary.
- Effective control of access rights through an adequate locking system (*e.g.*, security key with documented key management, and/or electronic locking systems with documented management of authorization).
- Documented processes for approval, changes and withdrawal of access authorization.
- Regular documented review of access authorizations granted.
- Reasonable measures for the prevention and detection of unauthorized access and access attempts (*e.g.*, which may include regular review of protection of the doors, gates and windows, burglar alarm system, video surveillance, security guards, and/or security patrol).
- Written regulations for employees and visitors dealing with technical access security measures.
- Restricting physical access to the servers by using electronically-locked doors, separate cages and/or locked racks within co-location facilities.

2. System Access Control:

Use of data processing systems by unauthorized persons must be prevented.

Measures:

- Restriction of authorization rights to IT systems and non-public networks to the minimum necessary.
- Effective control of authorization through personalized and unique user identifications and secure authentication process.
- Technical methods ensure password quality – number of characters, degrees of complexity, etc. Passwords must be changed every 180 days.
- Authentication via asymmetric key methods (*e.g.*, certificates, private-public-key-methods) requires that secret (private) keys are always protected with a password (passphrase) with the same password requirements noted above.
- Documented processes for approval, changes and withdrawal of access authorization.
- Regular documented review of access authorizations granted.
- Appropriate measures to secure the network infrastructure (*e.g.*, firewall, router and VPN-based access controls, network port security IEEE 802.1X, separation of networks, and/or encrypted network protocols).
- Written policies for employees regarding security measures and safe use of passwords.

- Automatically securing workstations controlled by BlueJeans with password-protected screensavers after a short timeout period.
- Timely implementation of critical/important security updates or patches.

3. Data Access Control:

Persons authorized to use data processing systems shall gain access only to the personal data that they have a right to access, and personal data must not be read, copied, modified or removed without authorization.

Measures:

- Access to personal, confidential or sensitive information is granted on a minimal basis to provide and support the BlueJeans Services.
- Authorization for access is controlled through unique login credentials and role-based access control.
- Regular documented review of access authorizations granted.
- Reasonable measures for the protection of servers and other infrastructure elements against unauthorized access (*e.g.*, application firewall, desktop firewalls, system hardening, content encryption).
- Media encryption with algorithms classified as safe for protection of mobile devices (laptops, tablet PCs).
- Access by BlueJeans personnel is logged, including access by administrators.
- Documented processes for approval, changes and withdrawal of access authorization.

4. Data Transmission Control:

Personal data must not be read, copied, changed or removed without authorization during electronic transfer or during transportation or storage on data carriers.

Measures:

- Appropriate measures implemented to secure the network infrastructure (*e.g.*, firewall, router and VPN-based access controls network port security IEEE 802.1X, separation of networks, and/or encrypted network protocols) to help protect data in transit on networks controlled by BlueJeans.
- Media encryption with algorithms classified as safe for protection of mobile devices (laptops, tablet PCs, etc.).
- Use of encrypted communication protocols (such as TLS-based protocols) for web-based access to data by BlueJeans personnel with a need-to-know and by end users.
- Customer data at rest on databases controlled by BlueJeans is stored in an encrypted manner.
- Customer data transmitted by BlueJeans is protected in transit using, as applicable, transport layer protocols and encrypted electronic communications.
- Testing mechanisms to identify remote terminals during transmissions.
- Written policies for employees regarding the handling and security of mobile devices and data carriers.
- Users are responsible for ensuring the use of equipment and/or systems that support the encryption used by BlueJeans.

5. Data Input Control:

It shall be possible to review and verify whether and by whom personal data can be entered into, modified in, or removed from data processing systems.

Measures:

- Appropriate authentication and authorization policies for entering, reading, modifying and deletion of personal data.
- Use of unique identification credentials for users accessing personal data.
- Separation of production and test data and protection using logical access controls and/or encryption.
- Secure storage for logging of the creation and revision of data entry.
- Backup log files that are secured from tampering.
- Logging and analysis of failed access attempts.

6. Job Control:

Personal data shall be processed in accordance with the applicable agreement and related lawful end user instructions.

Measures:

- Controls and processes to ensure compliance with contracts between BlueJeans and its customers, sub-processors, or other service providers, taking data protection laws and technical considerations into account.
- Timely review and implementation upon introduction of new procedures or changes to existing procedures for processing personal data.
- Regular verification of the correct application of data processing programs used to process personal data.
- Communicating the purpose of processing in the BlueJeans Privacy Policy.
- Facilitating the exercise of data subjects' rights.
- Notification in the event of unlawful acquisition of personal data.
- Correction or deletion (including by de-identifying or pseudonymization) of personal data upon reasonable request.

7. Availability Control:

Personal data shall be protected against accidental or unauthorized destruction or loss.

Measures:

- Utilizing data centers in secure co-location facilities with redundant infrastructure that supports business continuity and disaster recovery.
- Carefully selecting data center locations and Internet Service Providers and connecting users to the closest data center for optimal performance.
- Creation of daily backups stored in a separate storage environment designed for rapid recovery and reliable availability.
- Regular integrity review of backups.
- Maintaining a disaster recovery (DR) site and periodically testing DR procedures.
- Redundant systems and failover equipment have been installed to aid in the possible recovery of and access to personal data.
- Processes and documentation for the recovery of systems and data.

8. Data Separation Control

Personal data collected for different purposes can be processed separately.

Measures:

- Logical and/or physical separation of test, development and production systems.
- Separation of duties within the processing systems and at interfaces.
- Suitable measures to ensure that personal data collected for different purposes and different customers can be processed separately.

9. Data Integrity Control

Ensures that personal data will remain intact, complete and current during processing activities:

Measures:

- Physical and logical access to data based on business-need-to-know and principle of least privilege.
- Segregation of duties.
- Auditability of changes to data.
- Security monitoring.
- Antivirus software.
- Backup and recovery.
- External and internal penetration testing.
- Pseudonymizing personal data where applicable.

10. Deletion of Data

Personal data collected is deleted or pseudonymized when it is no longer required, service data is deleted a reasonable period after the termination of Services, and processes are in place to respond to data subject requests.

Measures:

- Deletion or pseudonymization of personal data upon reasonable request.
- Processes, tools and documentation for secure deletion so that recovery is not possible using current standard technology (*e.g.* by overwriting).
- Guidelines for employees on responding to data subject requests and methods of how and when personal data should be deleted.