CLEARDB™

CLEARDB GDPR DATA PROCESSING AGREEMENT

This Data Processing Agreement ("DPA") is an agreement between ClearDB Inc. ("**ClearDB**") and you or entity you represent ("**Customer**"). This DPA supplements the ClearDB Terms of Services, as updated from time to time between Customer and ClearDB when the GDPR applies to your use of the ClearDB Services to process Customer Personal Data.

The terms used in this Agreement shall have the meanings set forth below. Capitalized terms not defined herein shall have the meaning set forth in the Services Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

In consideration of the mutual obligations set out herein, the parties hereby agree that the terms and conditions set out below shall apply, with respect to the processing of Personal Data, in addition to the terms of the Services Agreement. Except where the context requires otherwise, references in this DPA to the Services Agreement as amended by, and including, this DPA. Each reference to the DPA below means this DPA including its Schedules and Appendices.

In the course of providing the Services to Customer pursuant to the Services Agreement, ClearDB may Process Personal Data on behalf of Customer and the parties agree to comply with the following provisions with respect to any Personal Data.

1. Effectiveness.

1.1 **Legal Authority**. Customer signatory represents to ClearDB that he or she has the legal authority to bind Customer and is lawfully able to enter into contracts (e.g., is not a minor).

1.2 **Termination**. This DPA will terminate upon the earliest of:

a) termination of the Agreement as permitted hereunder or by the ClearDB's Terms and Services conditions (and without prejudice to the survival of accrued rights and liabilities of the parties and any obligations of the parties which either expressly or by implication survive termination) or

b) as agreed by the parties in writing. ClearDB's obligations hereunder shall survive the termination of the Terms of Services Agreement until such time ClearDB no longer has access to, hosts or retains Personal Data.

2. Definitions.

"**Customer Personal Data**" means any Personal Data Processed by ClearDB (or a Sub-processor) on behalf of Customer pursuant to or in connection with the Agreement;

"**Data Protection Laws**" means all laws and regulations, including laws and regulations of the European Union, the European Economic Area and their member states, and the GDPR, applicable to the Processing of Customer Personal Data under the Agreement which are applicable to Customer.

"**GDPR**" means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

"**Sub-processor**" means any person (including any third party, but excluding an employee of ClearDB or any of its sub-contractors) appointed by or on behalf of Processor to Process Personal Data on behalf of Customer under the Agreement

The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**", "**Processor**", and "**Supervisory Authority**" shall have the same meaning as in the GDPR, and shall be construed accordingly.

3. Processing of Personal Data.

3.1 **Roles of the Parties**. The parties acknowledge and agree that with regard to the Processing of Personal Data, Customer is the Data Controller, ClearDB is a Data Processor and that ClearDB will engage Sub-processors pursuant to the requirements set forth in Section 5 "**Sub-processors**" below.

3.2 **Customer Authority**. Customer represents and warrants that it is and will at all relevant times remain duly and effectively authorized to give the instruction set forth in Section 3.4 below on behalf of itself.

3.3 **Customer's Processing of Personal Data**. Customer shall, in its use of the Services, Process Personal Data in accordance with the requirements of Data Protection Laws. Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws. In addition, Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

3.4 **Customer Instructions**. The parties agree that this DPA and the Agreement (including the provision of instructions via configuration tools such as the ClearDB management console and APIs made available by ClearDB for the Services) constitute Customer's documented instructions regarding ClearDB's processing of Customer Data ("Documented Instructions"). ClearDB will process Customer Data only in accordance with Documented Instructions. Additional instructions outside the scope of the Documented Instructions (if any) require prior written agreement between ClearDB and Customer, including agreement on any additional fees payable by Customer to ClearDB for carrying out such instructions. Customer is entitled to terminate this DPA and the Agreement if ClearDB declines to follow instructions requested by Customer that are outside the scope of, or changed from, those given or agreed to be given in this DPA.

3.5 **ClearDB's Processing of Personal Data**.

(a) ClearDB shall only Process Customer Personal Data for the purpose of the provision of the Services under the Agreement and in accordance with Customer's Documented Instructions, which are consistent with the terms of the Services Agreement, unless Processing is required by Data Protection Laws to which ClearDB (or the applicable sub-processor) is subject, in which case ClearDB shall to the extent permitted by the Data Protection Laws inform Customer of that legal requirement before the relevant Processing of that Customer Personal Data.

(b) The Services Agreement and any Order Forms thereunder, or other duly Documented Instructions are Customer's complete and final instructions to ClearDB for the Processing of Customer Personal Data. Any additional or alternate instructions must be agreed upon separately. Such instructions constitute: The processing of Customer Personal Data (i) in accordance with the Services Agreement, and any Order Forms under the Services Agreement, including without limitation with the transfer of Customer Personal Data to any country or territory; and (ii) to comply with other documented instructions provided by Customer where such instructions are consistent with the terms of the Services Agreement.

(c) Where ClearDB considers that an instruction infringes GDPR or of any other legal provision of the Union or of Member States bearing on data protection, it shall immediately inform Customer of this. Where ClearDB is obliged to transfer Personal Data to a third country or an international organization, under Union law or Member State law to which ClearDB is subject, ClearDB shall inform Customer of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

3.6 **Details of the Processing**. The subject-matter of Processing of Customer Personal Data by ClearDB is the performance of the Services pursuant to the Services Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Customer Personal Data and categories of Data Subjects Processed under this Agreement, as required by article 28(3) of the GDPR are further specified in Appendix 1 to this Agreement, as may be amended by the parties from time to time.

4. ClearDB Personnel.

4.1 **Contractual Obligations**. ClearDB shall ensure that the persons authorized to process Personal Data hereunder: (i) are bound by appropriate contractual obligations of confidentiality, data protection and data security; and (ii) process Personal Data only on instructions from Customer, unless required to do so by Union, Member State, or other applicable law. ClearDB shall ensure that such confidentiality obligations set forth in clause (i) above survive the termination of the personnel engagement.

4.2 **Confidentiality of Customer Data**. ClearDB will not access or use, or disclose to any third party, any Customer Data, except, in each case, as necessary to maintain or provide the Services, or as necessary to comply with the law or a valid and binding order of a governmental body (such as a subpoena or court order). If a governmental body sends ClearDB a demand for Customer Data, ClearDB will attempt to redirect the governmental body to request that data directly from Customer. As part of this effort, ClearDB may provide Customer's basic contact information to the government body. If compelled to disclose Customer Data to a government body, then ClearDB will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless ClearDB is legally prohibited from doing so. If the Standard Contractual Clauses apply, nothing in this Section 4 varies or modifies the Standard Contractual Clauses.

4.3 **Access**. ClearDB shall restrict its personnel from Processing Customer Personal Data without authorization by ClearDB and shall limit the Processing to that which is needed for the specific individual's job duties in connection with ClearDB's provision of the Services under the Services Agreement.

5. Sub-processors.

5.1 **Appointment of Sub-processors**. For the purpose of the appointment of Sub-processors, Customer acknowledges and agrees that ClearDB may engage third-party Sub-processors in connection with the provision of the Services, including without limitation the Processing of Customer Personal Data.

5.2 **Sub-processors**. Customer agrees that ClearDB may use sub-processors to fulfill its contractual obligations under this DPA or to provide certain services on its behalf, such as providing support services. The ClearDB website (currently posted at http://w2.cleardb.net/sub-processors) lists sub-processors that are currently engaged by ClearDB to carry out processing activities on Customer Data on behalf of Customer. At least 30 days before ClearDB engages any new sub-processor to carry out processing activities on Customer Data on behalf of Customer, ClearDB will update the applicable website and provide Customer with a mechanism to obtain notice of that update. If Customer objects to a new sub-processor, then without prejudice to any termination rights Customer has under the Agreement and subject to the applicable terms and conditions, Customer may request in writing that ClearDB move the relevant Customer Data to another ClearDB sub-processor to whom Customer objects, is not engaged by ClearDB as a sub-processor for Customer Data. Customer consents to ClearDB's use of sub-processors as described in this Section. Except as set forth in this Section, or as Customer may otherwise authorise, ClearDB will not permit any sub-processor to carry out processing activities on Customer Data on behalf of Customer.

5.3 **Sub-processor Obligations**. Where ClearDB authorises any sub-processor as described in Section 5.2: (i) ClearDB will restrict the sub-processor's access to Customer Data only to what is necessary to maintain the Services or to provide the Services to Customer and any End Users in accordance with the Documentation Instructions and ClearDB will prohibit the sub-processor from accessing Customer Data for any other purpose; (ii) ClearDB may enter into a written agreement with the sub-processor and, to the extent that the sub-processor is performing the same data processing services that are being provided by ClearDB under this DPA, ClearDB will, to the extent reasonably possible, impose on the sub-processor the same contractual obligations that ClearDB has under this DPA; and (iii) ClearDB will remain responsible for its compliance with the obligations of this DPA and for any acts or omissions of the sub-processors that cause ClearDB to breach any of ClearDB's obligations under this DPA.

6. Security.

6.1 **Adequate Measures**. 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 and freedoms of natural persons, ClearDB shall in relation to the Customer Personal Data implement and maintain throughout the term of this Agreement, the technical and organizational measures set forth in Exhibit A (the "**Security Measures**"). Customer acknowledges and agrees that it has reviewed and assessed the Security Measures and deems them appropriate for the protection of Customer Personal Data.

6.2 **Personal Data Breach Risk**. In assessing the appropriate level of security, ClearDB shall take account of the risks that are presented by Processing, in particular from a Customer Personal Data Breach.

7. Data Subject Rights.

7.1 **Correction, Restriction and Deletion**. ClearDB shall comply with any commercially reasonable request by Customer to correct, amend, restrict processing, or delete Customer Personal Data, as required by Data Protection Laws, to the extent ClearDB is legally permitted to do so.

7.2 **Measures to assist with Data Subject Rights**. Taking into account the nature of the Processing, ClearDB shall assist Customer by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfillment of the Customer's obligations, as reasonably understood by Customer, to respond to requests to exercise Data Subject rights under the Data Protection Laws. To the extent legally permitted, Customer shall be responsible for any costs arising from ClearDB's provision of such assistance.

7.3 **Response to Requests**: ClearDB:

(a) shall promptly notify Customer if it or any Sub-processor receives a request from a Data Subject under any Data Protection Laws in respect of Customer Personal Data; and

(b) shall not and shall ensure to the extent reasonably possible that no Sub-processor responds to that request except on the documented instructions of Customer or as required by Data Protection Laws to which ClearDB or Sub-processor is subject, in which case ClearDB shall, to the extent permitted by such Data Protection Laws inform Customer of that legal requirement before it or the applicable Sub-processor responds to the request.

8. Optional Security Features.

ClearDB makes available a number of security features and functionalities that Customer may elect to use. Customer is responsible for (i) implementing the measures described in Section 6.1, as appropriate, (ii) properly configuring the Services, (iii) using the controls available in connection with the Services (including the security controls) to allow Customer to restore the availability and access to Customer Data in a timely manner in the event of a physical or technical incident (e.g. backups and routine archiving of Customer Data), and (iv) taking such steps as Customer considers adequate to maintain appropriate security, protection, and deletion of Customer Data, which includes use of encryption technology to protect Customer Data from unauthorised access and measures to control access rights to Customer Data.

9. Personal Data Breach.

9.1 Notification of Data Breach. ClearDB shall, to the extent permitted by law, notify Customer without undue delay after becoming aware of a Personal Data Breach affecting Customer Personal Data, providing Customer with sufficient information and documentation to allow Customer to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

9.2 Assistance to Customer. ClearDB shall assist Customer in relation to any personal data breach notifications Customer is required to make under the GDPR, ClearDB will include in the notification under section 9.1 such information about the Security Incident as ClearDB is reasonably able to disclose to Customer, taking into account the nature of the Services, the information available to ClearDB, and any restrictions on disclosing the information, such as confidentiality.

9.3 Communication. Notification(s) of Security Incidents, if any, will be delivered to one or more of Customer's administrators by any means ClearDB selects, including via email. It is Customer's sole responsibility to ensure Customer's administrators maintain accurate contact information on the ClearDB management console and secure transmission at all times.

9.4 **Unsuccessful Security Incidents.** Customer agrees that:

a) an unsuccessful Security Incident will not be subject to this Section 9. An unsuccessful Security Incident is one that results in no unauthorised access to Customer Data or to any of ClearDB's equipment or facilities storing Customer Data, and may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorised access to traffic data that does not result in access beyond headers) or similar incidents; and

b) ClearDB's obligation to report or respond to a Security Incident under this Section 9 is not and will not be construed as an acknowledgement by ClearDB of any fault or liability of ClearDB with respect to the Security Incident.

10. Data Protection Impact Assessment and Prior Consultation.

ClearDB shall provide reasonable assistance to Customer with any data protection impact assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which Customer reasonably considers to be required of it by Article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Customer Personal Data by, and taking into account the nature of the Processing and information available to, ClearDB or the Sub-processors.

11. Return or Destruction of Personal Data.

11.1 **Return or Deletion**. Subject to the provisions of Section 11.2 below, at Customer's election, made by written notice to ClearDB following thirty (30) days of the date of cessation of any Services involving the Processing of Customer Personal Data (the "**Cessation Date**"), ClearDB shall, and shall procure that all Sub-processors: (i) return a complete copy of all Customer Personal Data to Customer in such format and manner requested by Customer and reasonably acceptable to ClearDB; and (ii) delete and procure the deletion of all other copies of Customer Personal Data Processed by ClearDB or any Sub-processor. ClearDB shall comply with any such written request within thirty (30) days of the Cessation Date.

11.2 **Retention of Copies**. ClearDB and each Sub-processor may retain Customer Personal Data to the extent required by applicable European Union law or the law of an EU Member State and only to the extent and for such period as required by such laws and always provided that ClearDB shall ensure the confidentiality of all such Customer Personal Data and shall ensure that such Customer Personal Data is only Processed as necessary for the purpose(s) specified in such law requiring its storage and for no other purpose.

12. Data Protection Officer.

ClearDB shall communicate to Customer the name and contact details of its data protection officer, if it has designated one in accordance with Article 37 of the GDPR.

13. Record of Processing Activities; Documentation.

13.1 Records. ClearDB maintains, and throughout the term of this Agreement shall maintain, an electronic record of any processing activities carried out on behalf of Customer.

13.2 **Documentation**. At Customer's written request, and provided that the parties have an applicable NDA in place, and to the extent possible, ClearDB shall provide Customer with the necessary documentation so that customer can reasonably verify ClearDB's obligations under this Agreement. If ClearDB declines to provide such documentation, Customer is entitled to terminate this DPA and the Terms of Services Agreement.

14. Audit.

14.1 **Customer Audits.** Customer agrees to exercise any right it may have to conduct an audit or inspection, including under the Standard Contractual Clauses if they apply, by instructing ClearDB to carry out the audit described in Section 14. If Customer wishes to change this instruction regarding the audit, then Customer has the right to request a change to this instruction by sending ClearDB written notice as provided for in the Agreement. If ClearDB declines to follow any instruction requested by Customer regarding audits or inspections, Customer is entitled to terminate this DPA and the Terms of Services Agreement. If the Standard Contractual Clauses apply, nothing in this Section varies or modifies the Standard Contractual Clauses nor affects any supervisory authority's or data subject's rights under the Standard Contractual Clauses.

15. Transfer of Data. With respect to Customer Personal Data The provisions of this Section 15 below shall apply in lieu of Section 2(d) of the Services Agreement.

15.1 **Standard Contractual Clauses**. Subject to the provisions of Section 15.2 below, to the extent Customer Personal Data is transferred under this Agreement from the European Economic Area and/or its Member States to countries which do not ensure an adequate level of data protection within the meaning of Data Protection Laws and Regulations, to the extent such transfers are subject to such Data Protection Laws and Regulations, the Customer (as "data exporter") and ClearDB (as "data importer") hereby enter into the contractual clauses set out in Exhibit B (the "**Standard Contractual Clauses**"), amended as indicated (in square brackets and italics) in such Exhibit and under Section 15.2 below in respect of the transfers.

15.2 **Applicability**. Section 15.1 shall not apply to a cross border transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant cross border to take place without breach of applicable Data Protection

Law and Regulation. The Standard Contractual Clauses apply to (i) the legal entity that has executed the Standard Contractual Clauses as a Data Exporter and, (ii) all affiliates of Customer, if any, established within the European Economic Area (EEA) and Switzerland that have purchased Services on the basis of an Order Form. For the purpose of the Standard Contractual Clauses and this Section 15, the Customer and its affiliates shall be deemed to be “Data Exporters”.

15.3 **Precedence**. In the event of any conflict or inconsistency between this Agreement and the Standard Contractual Clauses in Exhibit B hereof, the Standard Contractual Clauses shall prevail.

16. Indemnification; Limitation of Liability.

If ClearDB is held liable for a violation of this Agreement and/or the Standard Contractual Clauses committed by Customer, the latter will, to the extent to which it is liable, indemnify ClearDB for any cost, charge, damages, expenses or loss it has incurred in accordance with the provisions of the "Indemnification" Section of the Services Agreement. Each party’s liability, taken together in the aggregate, arising out of or related to this Agreement and/or the Standard Contractual Clauses, whether in contract, tort or under any other theory of liability, is subject to the ‘Limitation of Liability’ section of the Services Agreement. For the avoidance of doubt, ClearDB’s total liability for all claims from the Customer or any third party arising out of or related to the Services Agreement and this Agreement shall apply in the aggregate for all claims under both the Services Agreement and this Agreement.

EXHIBIT A

TO DATA PROCESSING AGREEMENT: SECURITY CONTROLS

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.

Data Center & Network Security.

(a) Data Centers.

Server Operating Systems. The Data Importer servers use a Linux based implementation customized for the application environment. Data is stored using proprietary algorithms to augment data security and redundancy. The Data Importer employs a code review process to increase the security of the code used to provide the Services and enhance the security products in production environments.

Businesses Continuity. The Data Importer replicates data over multiple systems to help to protect against accidental destruction or loss. The Data Importer has designed and regularly plans and tests its business continuity planning/disaster recovery programs.

(b) Networks and Transmission.

Data Transmission. Services are typically connected via high-speed private links to provide secure and fast data transfer between data centers. 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 Data Importer transfers data via Internet standard protocols.

Intrusion Detection. Intrusion detection is intended to provide insight into ongoing attack activities and provide adequate information to respond to incidents. The Data Importer intrusion detection involves:

1. tightly controlling the size and make-up of the Data Importer's attack surface through preventative measures;
2. employing intelligent detection controls at data entry points; and
3. employing technologies that automatically remedy certain dangerous situations.

Incident Response. The Data Importer monitors a variety of communication channels for security incidents, and The Data Importer's security personnel will react promptly to known incidents.

Encryption Technologies. The Data Importer makes HTTPS encryption (also referred to as SSL or TLS connection) available. ClearDB servers support ephemeral elliptic curve

Diffie-Hellman cryptographic key exchange signed with RSA and ECDSA. These perfect forward secrecy (PFS) methods help protect traffic and minimize the impact of a compromised key, or a cryptographic breakthrough.

2. Access Controls.

Infrastructure Security Personnel. The Data Importer has, and maintains, a security policy for its personnel, and requires security training as part of the training package for its personnel. The Data Importer's infrastructure security personnel are responsible for the ongoing monitoring of the Data Importer's security infrastructure, the review of the Services, and responding to security incidents.

Access Control and Privilege Management. The Data Exporter's administrators must authenticate themselves via a central authentication system or via a single sign on system in order to administer the Services.

Internal Data Access Processes and Policies – Access Policy. The Data Importer's internal data handling processes and policies are designed to prevent unauthorized persons and/or systems from gaining access to systems used to process personal data. The Data Importer designs its systems to: (i) only allow authorized persons to access data they are authorized to access; and (ii) ensure that personal data cannot be read, copied, altered or removed without authorization during processing, use and after recording. The systems are designed to detect any inappropriate access. The Data Importer employs a centralized access management system to control personnel access to production servers, and only provides access to a limited number of authorized personnel. LDAP, Kerberos and a proprietary system utilizing SSH certificates are designed to provide the Data Importer with secure and flexible access mechanisms. These mechanisms are designed to grant only approved access rights to site hosts, logs, data and configuration information. The Data Importer requires the use of unique user IDs, strong passwords, two factor authentication and carefully monitored access lists to minimize the potential for unauthorized account use. The granting or modification of access rights is based on: the authorized personnel's job responsibilities; job duty requirements necessary to perform authorized tasks; and a need to know basis. The granting or modification of access rights must also be in accordance with The Data Importer's internal data access policies and training. Approvals are managed by workflow tools that maintain audit records of all changes. Access to systems is logged to create an audit trail for accountability. Where passwords are employed for authentication (e.g., login to workstations), password policies that follow at least industry standard practices are implemented. These standards include restrictions on password reuse and sufficient password strength.

3. Data.

(a) Data Storage, Isolation and Logging.

The Data Importer stores data in a Geo distributed environment on the Data Importer-owned servers. The data and file system architecture are replicated between multiple geographically dispersed data centers. The Data Importer also logically isolates the Data

Exporter's data, and the Data Exporter will be given control over specific data sharing policies. Those policies, in accordance with the functionality of the Services, will enable the Data Exporter to determine the product sharing settings applicable to end users for specific purposes. The Data Exporter may choose to make use of certain logging capability that the Data Importer may make available via the Services.

(b) Decommissioned Data and Data Erase Policy.

Data containing data may experience performance issues, errors or hardware failure that lead them to be decommissioned ("Decommissioned Data"). Every Decommissioned Data is subject to a series of data destruction processes (the "Data Erase Policy") before leaving the Data Importer's premises either for reuse or destruction. Decommissioned Data are erased in a multi-step process and verified complete by at least two independent validators.

4. Personnel Security.

The Data Importer personnel are required to conduct themselves in a manner consistent with the company's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. The Data Importer conducts reasonably appropriate backgrounds checks to the extent legally permissible and in accordance with applicable local labor law and statutory regulations.

Personnel are required to execute a confidentiality agreement and must acknowledge receipt of, and compliance with, the Data Importer's confidentiality and privacy policies. Personnel are provided with security training. Personnel handling Customer data are required to complete additional requirements appropriate to their role (eg., certifications). The Data Importer's personnel will not process Customer data without authorization.

Exhibit B – Model Contractual 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

The entity identified as "Customer" in the DPA (the "data exporter") and ClearDB (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;

(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.

[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.

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

[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.

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, namely…………………………………………………………………………….

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, namely …………………………………… ……………………………………………………………………………… ………………………………………………………………………………

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

[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.

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.

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 the entity identified as “Customer” in the DPA

Data importer

The data importer is ClearDB Inc., a ClearDB of managed database services.

Data subjects

Data subjects are defined in Section 3.5 of the DPA.

Categories of data

The personal data are defined in Section 3.5 of the DPA.

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify): The processing operations are defined in Section 3.5 of the DPA

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed 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):

The technical and organisational security measures implemented by the data importer are as described in the DPA.