DATA PROCESSING AGREEMENT
NEC to UNIVERGE Blue Partner

This Data Processing Agreement (the "DPA")") completes and forms part of the NEC UNIVERGE BLUE Privacy Policy and the Master Service Agreement (the Agreement) between the Company, and the Partner(s) reselling the Services.

This DPA is subject to the terms, conditions, restrictions and limitations set forth in the Agreement.

In consideration of the mutual obligations set out herein, the Parties hereby agree that the terms and conditions set out below shall be added as DPA to the Agreement. Except where the context requires otherwise, references in this DPA to the Agreement are to the Agreement as amended by, and including, this DPA.

1. Definitions

1.1 In this DPA the following terms shall have the meanings set out below and cognate terms shall be construed accordingly:

"**Applicable Laws**" means any applicable laws, rules, regulations or interpretations of relevant l Authorities or self-regulatory bodies applicable to the services thereof.

"**Company"** in the context of this DPA means NEC Nederland B.V.

"Partner (s)" in the context of this DPA means (i) Distributors acting on behalf of their Resellers and; (ii) Resellers acting on behalf of their Customers.

Company and Partner (s) are collectively referred to herein as the "Parties"

"**Customer"** means the end customer of such Partner(s) on behalf of which Personal Data is processed.

"**Data Protection Laws**" means the General Data Protection Regulation 2016/679 and the e-Privacy Directive 2002/58/EC (as amended by Directive 2009/136/EC) and applicable Member State laws implementing or supplementing the GDPR, the Swiss Federal Data Protection Act, Data Protection Acts of the EEA countries and UK Data Protection 2018 (all as amended and replaced from time to time).

"Services"means NEC UNIVERGE BLUE services and other activities to be supplied to or carried out currently or in the future pursuant to the Agreement, involving processing of Personal Data by the Company on behalf of the Partner(s) with the subject-matter and duration of the processing and the type of personal data and categories of data subjects provided in Schedule A (Processing of Personal Data) to this DPA.

1.2 The terms, "**Data Controller**", "**Data Processor",** "**Data Subject**", **"Data Transfers"** "**Member State**", "**Personal Data**", "**Personal Data Breach**", "**Processing**", **"Sub**

Processor" and "**Supervisory Authority**" shall have the same meaning as in the Data Protection Laws, and their cognate terms shall be construed accordingly.

1.3 The word "**include**" shall be construed to mean include without limitation, and cognate terms shall be construed accordingly.

2. Processing of Personal Data

Company shall only process Personal Data on behalf of the Partner in accordance with Partner's instructions and not for any other purposes than those specified in Schedule A as part of this DPA or, as otherwise approved by the Partner writing.

Company may also process Personal Data where required to do so by applicable law. In such a case, Company shall inform the Partner of that legal requirement before processing unless that law prohibits such information on important grounds of public interest.

3. Company Personnel

Company shall take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know / access the relevant Personal Data, as strictly necessary for the purposes of the Agreement, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

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 individuals, Company shall, in relation to the Personal Data necessary for the purposes of the Agreement, implement appropriate technical and organizational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred in Data Protection Laws. Measures are specified in Schedule B as part of this DPA.

5. Sub Processing

5.1 The Parties acknowledge that Data Protection Laws permit the Partner to provide the Company a written authorization to Sub Processing. Under the DPA, Partner authorises Company to appoint (and permit each Sub Processor appointed in accordance with this section 5) Sub Processors in accordance with this section and any restrictions in the Agreement.

5.2 A list of Company's current Sub-Processors is available upon demand at privacy@EMEA.NEC.COM.

5.3 Company shall provide Partner with advance notice before a new Sub Processor processes any Personal Data, including full details of the processing to be undertaken by the Sub Processor. Partner may object to the new Sub Processor within fifteen (15) days of such notice on reasonable grounds relating to the protection of Personal Data In such case, Company shall have the right to cure the objection through one of the following options: (1) Company will cancel its plans to use the Sub Processor with regards to processing of Personal Data or will offer an alternative to provide the Services without such Sub Processor; or (2) Company will take the corrective steps requested by Partner in its objection notice and proceed to use the Sub processor or (3) Company may elect to proceed with its use of the new sub-processor in which case Partner or Customer may decide (a) not to use, whether temporarily or permanently, the particular aspect or feature of the Services that would involve the use of such Sub Processor (b) in case (a) is not feasible to terminate its use of the Services.

5.4 Company shall: (a) enter into a written agreement in accordance with same requirements as set forth on Data Protection Laws with any Sub Processor that will process Personal Data and b) ensure that each such written agreement contains terms that are no less protective of Personal Data than those contained in this DPA and (c) be liable for the acts and omissions of its Sub Processors to the same extent that Company would be liable if it were performing the Services of each of those Sub Processors directly under the terms of this DPA.

5.5 The Company, in providing the Services shall transfer Personal Data outside of EEA. Company ensures that Company will comply with any requirements (such as Standard Contractual Clauses and any other legal transfer mechanism) under Data Protection Laws with regard to such Personal Data Transfers.

6. Data Subject Rights

6.1 Taking into account the nature of the processing, Company shall assist Partner by implementing appropriate technical and organizational measures, insofar as this is possible, for the fulfilment of Partner's obligations, as reasonably understood by Partner, to respond to requests to exercise Data Subject rights under Data Protection Laws.

6.2 Company shall promptly notify Partner if receives a request from a Data Subject under any Data Protection Laws in respect of Personal Data.

6.3 Company shall ensure Partner , that Company does not respond to that request except on the documented instructions of or as required by Applicable Laws to which Company is subject, in which case Company shall to the extent permitted by Applicable Laws inform Partner of that legal requirement before Company responds to the request.

7. Personal Data Breach

7.1 Company shall notify Partner without undue delay upon Company becoming aware of a Personal Data Breach affecting Personal Data, providing Partner with sufficient information to allow Partner to meet any obligations to report or inform Data Subjects of the Personal Data Breach under Data Protection Laws.

7.2 Such notification shall as a minimum and as available to Company as follows:

- Describe the nature of the Personal Data Breach, the categories and numbers of Persons concerned, and the categories and amount of Personal Data records concerned;
- Describe the likely consequences of the Personal Data Breach;
- Description of the possible consequences of the security compromise;
- Description of the measures that the responsible party intends to take or has taken to address the security compromise;
- Recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the security compromise;
- If known to the responsible party, the identity of the unauthorized person who may have accessed or acquired the Personal Data.
- Describe the measures taken or proposed to be taken to address the Personal Data Breach.

7.3 Company shall co-operate with Partner and take such reasonable commercial steps as are directed by the Partner to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

Company shall provide reasonable assistance to Partner with any data protection assessments, which Partner reasonably considers to be required under Data Protection Laws and prior consultations with Data Protection Supervisor Authorities, which Partner reasonably considers to be required under Data Protection Laws, in each case solely in relation to Processing of Personal Data by, and taking into account the nature of the Processing and information available to Company.

9. Deletion or return of Personal Data

9.1 Subject to sections 9.2 and 9.3 Company shall promptly and in any event within 90 days of the date of termination of any Services involving the Processing of Personal Data (the "**Termination Date**"), delete and procure the deletion of all copies of those Personal Data.

9.2 Subject to section 9.3, Partner may in its absolute discretion by written notice to Company within 15 days of the Termination Date require Company to (a) return a complete copy of all Personal Data to Partner by secure file transfer in such format as is reasonably notified by Partner to Company; and (b) delete and procure the deletion of all other copies of Personal Data Processed . Company shall comply with any such written request within 90 days of the Termination Date.

9.3 Company may retain Personal Data to the extent required by Applicable Laws and only to the extent and for such period as required by Applicable Laws.

10. Audit rights

Upon prior written request by the Partner, Company agrees to provide Partner within reasonable time with: (a) a summary of a recent audit report demonstrating Company's compliance with its obligations under this DPA after redacting any confidential and/or commercially sensitive information where appropriate, and (b) confirmation that the audit has not revealed any material vulnerability in Company's systems, or to the extent that any such vulnerability was detected and Company has appropriately remedied such vulnerability. If the above measures are not reasonably sufficient to confirm compliance with the provisions of Data Protection Laws relevant to the Services and their use by the Company, or if they reveal material compliance or security vulnerability issues, then, subject to the strictest confidentiality obligations, Company allows Partner to request an audit of Company's data protection framework by an external independent auditor, which shall be jointly selected by the Parties. The external independent auditor cannot be a competitor of the Company, and the Parties will mutually agree upon the scope, timing, and duration of the audit. Company will make available to Partner the result of the audit of its data protection framework.

11. General Terms

11.1 The Parties to this DPA hereby submit to the choice of jurisdiction stipulated in the Agreement with respect to any disputes or claims howsoever arising under this DPA, including disputes regarding its existence, validity or termination or the consequences of its nullity; and

11.2 This DPA and all non-contractual or other obligations arising out of or in connection with it are governed by the laws of the country or territory stipulated for this purpose in the Agreement.

11.3 With regards to the subject matter of this DPA in the event of inconsistencies between the provisions of this DPA and any other agreements between the parties, including the Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the Parties) agreements entered into or purported to be entered into after the date of this DPA, the provisions of this DPA shall prevail.

11.4 Should any provision of this DPA be 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.

11.5 This DPA, including any schedules and exhibits hereto, constitute the entire Agreement between Company and Partner and supersedes all previous agreements by and between Company and Partner relating to the subject matter hereof.

SCHEDULE A. PROCESSING OF PERSONAL DATA

Subject Matter of the Processing

Company will Process Personal Data to provide the NEC UNIVERGE BLUE Services, which may include Unified Communications, Voice over Internet Protocol (VoIP) telecommunications services, video conferencing and webinar, hosted Contact Center, file sync and share, email, email backup, email archiving, file storage, file backup, and other communications services, as described in the Agreement and the Schedules and Exhibits incorporated therein. The provision of the Services includes not only the delivery of the Services themselves, but also the operation of the administrative portal through which the Services are managed as well as related processes and activities.

Purpose of the Processing

Company will Process Personal Data for the purpose of providing the NEC UNIVERGE BLUE Services and any associated tools and services, including technical support or other support services.

Nature of the Processing

In providing the Services, Company (and its Sub-Processors to which Personal Data may be disclosed or otherwise transmitted) will transmit, receive, store, encrypt and/or copy Personal Data.

Types of Personal Data

Company will Process any Personal Data that Partner transmits, receives, stores, encrypts and/or copy in their use of the Services. In addition, Company will Process any Personal Data that is included (a) as metadata (such as user names, email addresses, IP addresses and the like) in any communications or files that Company Processes in its delivery of the and/or (b) within the Company portal.

Categories of Data Subjects

Company will Process Personal Metadata relating to any users, senders or recipients of communications or files through the Services, as well as individuals identified as authorized contacts, administrators or other roles within the administrative portal through which the Services are managed. In addition, Company will Process Personal Data regarding any data subjects regarding whom Partner transmits, receives, stores, encrypts and/or copy Personal Data in their use of the Services.

Duration of the Processing

Company will Process Personal Data only for as long as necessary to provide the Services or as otherwise permitted under the Agreement.

SCHEDULE B. DATA SECURITY MEASURES

Company will, as a minimum, implement the following types of security measures:

1. Physical access control

Technical and organizational measures designed to prevent unauthorized persons from gaining access to the data processing systems available in premises and facilities (including databases, application servers and related hardware), where Personal Data are processed, including:

- Establishing security areas and restriction of access paths;
- Establishing access authorizations for employees and third parties;
- Access control system (ID reader, magnetic card, chip card);
- Key management and card-keys procedures;
- Door locking (electric door openers, for example);
- Security staff;
- Surveillance facilities, video/CCTV monitor, and alarm system;
- Securing decentralized data processing equipment and personal computers.

2. Virtual access control

Technical and organizational measures designed to prevent data processing systems from being used by unauthorized persons, including:

- User identification and authentication procedures;
- ID/password security procedures (e.g., special characters, minimum length, change of password);
- Automatic blocking (e.g., password or timeout);
- Monitoring of break-in-attempts and automatic turn-off of the user ID upon several erroneous passwords attempts;
- Encryption of archived data media.

3. Data access control

Technical and organizational measures designed to ensure that persons entitled to use a data processing system gain access only to such Personal Data in accordance with their access rights, and that Personal Data cannot be read, copied, modified or deleted without authorization, including:

- Internal policies and procedures;
- Control authorization schemes;
- Differentiated access rights (profiles, roles, transactions and objects);
- Monitoring and logging of accesses;
- Disciplinary action against employees who access personal data without authorization;
- Reports of access;
- Access procedure;
- Change procedure;
- Deletion procedure;
- Encryption.

4. Disclosure control

Technical and organizational measures designed to ensure that Personal Data cannot be read, copied, modified or deleted without authorization during electronic transmission, transport or storage on storage media (manual or electronic), and that it can be verified to which companies or other legal entities Personal Data are disclosed, including:

- Encryption/tunneling;
- Logging;
- Transport security.

5. Entry control

Technical and organizational measures designed to monitor whether data have been entered, changed or removed (deleted), and by whom, from data processing systems, including:

- Logging and reporting systems;
- Audit trails and documentation.

6. Control of instructions

Technical and organizational measures designed to ensure that Personal Data are processed solely in accordance with the instructions of Partner, including:

- The terms of, and performance by Company of its obligations under the Agreement;
- Formal commissioning (request form);

7. Availability control

Technical and organizational measures designed to ensure that Personal Data are protected against accidental destruction or loss (physical/logical), including:

- Backup procedures;
- Mirroring of hard disks (e.g., RAID technology);
- Uninterruptible power supply (UPS);
- Remote storage;
- Anti-virus/firewall systems;
- Disaster recovery plan.

8. Separation control

Technical and organizational measures designed to ensure that Personal Data collected for different purposes can be processed separately, including:

- Separation of databases;
- "Internal client" concept / limitation of use;
- Segregation of functions (production/testing).