



Mavenir New Supplier  
**Information and Forms Packet**

**NOT** All Forms May Apply

Please Follow the Instructions and Checklist Page

For Queries, please contact your assigned Procurement Representative or

if no one is assigned email to: [**GlobalProcurement@mavenir.com**](mailto:GlobalProcurement@mavenir.com)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Changes** | **Procurement Member** | **Approved By** |
| 1.0 | January 1, 2021 | Original Document | Sharon Rabinovitz | Ralf Mueller |
| 1.1 | January 20, 2021 | Styling & formatting changes | Yulia Zavorina | Sharon Rabinovitz |

Copyright © Mavenir 2021. All rights reserved. This document is protected by international copyright law and may not be reprinted, reproduced, copied or utilized in whole or in part by any means including electronic, mechanical, or other means without the prior written consent of Mavenir.

Reference: Document Name

Version: 1.0

Status: [DocStatus]

Release Date: 8-Nov-17

**Copyright © Mavenir 2017**

Commercial in Confidence

Commercial in Confidence

Whilst reasonable care has been taken by Mavenir to ensure the information contained herein is reasonably accurate, Mavenir shall not, under any circumstances be liable for any loss or damage (direct or consequential) suffered by any party as a result of the contents of this publication or the reliance of any party thereon or any inaccuracy or omission therein. The information in this document is therefore provided on an “as is” basis without warranty and is subject to change without further notice and cannot be construed as a commitment by Mavenir.

The products mentioned in this document are identified by the names, trademarks, service marks and logos of their respective companies or organizations and may not be used in any advertising or publicity or in any other way whatsoever without the prior written consent of.

Instructions and Checklist

|  |  |
| --- | --- |
| **Section** | **Notes** |
| Part 1 New Supplier Form | Mandatory for all New Suppliers |
| Part 2 Form W-9 | Tax ID Form applicable for US Companies or Individuals ONLY |
| Part 3 Form W-8 BEN-E | Tax ID Form applicable for Non-US Companies |
| Part 4 Form W-8 | Tax ID Form applicable for Non-US Companies - Individuals ONLY |
| Part 5 Mutual NDA | Applicable for Corp-to-Corp arrangements |
| Part 6 Contract Terms | Case by Case Templates to be provided by Procurement |
| Part 7 Conflict of Interest Questionnaire | Conflict of Interest Check |
| Part 8 GDPR | Applicable to all Companies processing and holding the personal data of data subjects residing in the European Union |

# New Supplier Form

**Instructions**

A Supplier record cannot be created unless all details and documentation are provided. You are **required** to complete the forms and return all documentation to [**GlobalProcurement@mavenir.com**](mailto:GlobalProcurement@mavenir.com)

## Bank Documentation

Bank details must be provided on either a

* Logo document
* Official bank letter
* Check sample
* Invoice sample

## W8 or W9

* **For US Legal Entity** – please provide a correctly filled out [W-9](https://www.irs.gov/pub/irs-pdf/fw9.pdf) Form. Form must be signed and name on form and invoice must match (original form is required).
* **For non-US Entity** – please provide a correctly filled out [W-8](https://www.irs.gov/pub/irs-pdf/fw8ben.pdf) Form for Individual or [W-8BEN-E](https://www.irs.gov/pub/irs-pdf/fw8bene.pdf) for Entity. Form must be signed and name on form and invoice must match (original form is required).

## GDPR (General Data Protection Regulation)

Applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company’s location. More information can be found at this link<https://www.eugdpr.org/>

* Is your company in full compliance with GDPR? **Select an answer**   Yes No
* You must provide a copy of the company’s GDPR Statement**.**

## HSE Certificate

* For **UK Legal Entity** **ONLY** – please provide HSE Certificate.

## If applicable

* Copy of Mavenir Signed Agreement / Statement of Work
* Diversity Certification if applicable

|  |  |  |
| --- | --- | --- |
| **Classification** | **Certificate Number** | **Expiration Date** |
| **Hub Zone** |  |  |
| **Minority Owned** |  |  |
| **Woman Owned** |  |  |
| **Veteran Owned** |  |  |
| **Other** |  |  |
| **Not Applicable** |  |  |

## Supplier Details

|  |  |
| --- | --- |
| Supplier Full Name: |  |
| Supplier Registration Number: |  |
| VAT number: |  |
| GST #: (applicable for India) |  |
| Income Tax PAN # (applicable for India) |  |
| Address: |  |
| City: |  |
| State: |  |
| County: (For US only) |  |
| Country: |  |
| Postal Code/ZIP: |  |
| Phone Number: |  |
| Supplier Contact Person: |  |
| Contact E-mail address: |  |
| E-mail address for Purchase Orders: |  |
| E-mail address for Remittance Advise: |  |
| Supplier Service / Occupation: |  |
| Scope of Services: |  |
| Agreement Effective Date: |  |
| Agreement End Date: |  |
| Initial Term (Duration): |  |
| Payment Terms (altered according to contract) | **NET 90 Days** |
| Mavenir Focal Point: |  |

## 

## Banking Details

|  |  |
| --- | --- |
| Bank Name: |  |
| Account Name: |  |
| Account Number: |  |
| Swift No: |  |
| IBAN Number: |  |
| Routing Number/ABA (USA/Canada):  Sort Code (UK):  IFSC Number (India): |  |
| Invoice Currency: |  |
| Payment Currency: |  |

# 

# Form W9



# Form W8 BEN-E

# 

# Form W8



# Mutual NDA



# Contract Terms

# Conflict of Interest Questionnaire

**Supplier Certification and Questionnaire**

(“Supplier”) is entering into or has entered into a business relationship with **Mavenir Systems, Inc**. (“**Mavenir**” or any of its affiliates) and hereby certifies and agrees that the following information is true and accurate:

|  |  |  |  |
| --- | --- | --- | --- |
| 1. | Supplier’s full Legal Name and Address |  | |
| 2. | Supplier’s Legal Place of Incorporation |  | |
| 3. | General information about Supplier  (Owners, Stake Holders, Company Size, Competitors, Market etc.) |  | |
| 4. | Scope of Activity with Mavenir |  | |
| 5. | Do you compete with Mavenir in any way? |  | |
| 6. | Are you aware of:  a. any business or personal relationship your company (or any of its owners, shareholders, directors, or employees) has had with Mavenir (other than the specific scope of activity in Question 4) or with any of Mavenir’s customers, owners, shareholders, directors, officers or employees or any of their family members?  b. business or personal relationship your company (or any of its owners, shareholders, directors, or employees) currently has with Mavenir (other than the specific scope of activity in Question 4) or with any of Mavenir’s customers, owners, shareholders, directors, officers or employees or any of their family members?  c. Any business or personal relationship your company (or any of its owners, shareholders, directors, or employees) may have with Mavenir (other than the specific scope of activity in Question 4) or with any of Mavenir’s customers, owners, shareholders, directors, officers or employees or any of their family members? |  | |
|  | |
|  | |
| 7. | Are you owned by a Government Entity or a Government Official? |  | |
| 8. | Do you require your employees to post a bond with financial or other penalties upon leaving your employ? |  | |
| Company Name:  By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Name:  Title:  Date: | | | |

# GDPR Data Privacy Addendum

**GDPR**

**Data Privacy Addendum**

**WHEREAS,** **Mavenir Systems, Inc**. (“**Mavenir**”) has engaged \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (“**Vendor**”) to provide \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ services and other offerings as set forth in that certain \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Agreement (“**Agreement**”) effective as of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_, 20\_\_ as may be amended or superseded (“**Agreement**”); and

**WHEREAS,** the **EU General Data Protection Regulation** will impose additional compliance obligations upon **Mavenir Systems, Inc**. (“**Mavenir**”) and \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (“**Vendor**”), including in relation to Mavenir’s contracts with service providers that process Personal Data on its behalf; and

**NOW, THEREFORE,** on this \_\_ day of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_, for good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1. **Order of Precedence**
2. This Addendum shall apply in relation to all Processing of Personal Data.
3. In case of any conflict between this Data Processing Addendum and the Agreement, this Data Processing Addendum shall prevail with regard to the Processing of Personal Data.
4. **Definitions**
5. ***“Applicable Law”*** means all applicable European Union (“EU”) or national laws and regulations relating to the privacy, confidentiality, security and protection of Personal Data, including, without limitation: the European Union (“EU”) General Data Protection Regulation 2016/679 (“GDPR”), with effect from 25 May 2018, and EU Member State laws supplementing the GDPR; the EU Directive 2002/58/EC (“e-Privacy Directive”), as replaced from time to time, and EU Member State laws implementing the e-Privacy Directive, including laws regulating the use of cookies and other tracking means as well as unsolicited e-mail communications.
6. ***“Data Security Measures”*** means technical and organizational measures that are aimed at ensuring a level of security of Personal Data that is appropriate to the risk of the Processing, including protecting Personal Data against accidental or unlawful loss, misuse, unauthorized access, disclosure, alteration, destruction, and all other forms of unlawful Processing, including measures to ensure the confidentiality of Personal Data.
7. ***“Data Subject”*** means an identified or identifiable natural person to which the Personal Data pertain.
8. ***“Instructions”*** means this Addendum and any further written agreement or documentation through which the Data Controller instructs the Data Processor to perform specific Processing of Personal Data.
9. ***“Personal Data”*** means any information provided by Mavenir to Vendor under the Agreement relating to a Data Subject who is located in the European Union who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person**.**
10. ***“Sub-Processor”*** means the entity engaged by the Data Processor or any further Sub-Processor to Process Personal Data on behalf and under the authority of the Data Controller.
11. **“*Data Controller*”, “*Data Processor*”*,* “*Personal Data Breach*”, “*Process*”, “*Processed*”, and “*Processing*”** shall have the meaning ascribed to them in the GDPR.
12. **Roles and Responsibilities of the Parties**
13. The Parties acknowledge and agree that **Mavenir** is acting as a Data Controller and has the sole and exclusive authority to determine the purposes and means of the Processing of Personal Data Processed under this Addendum, and **Vendor** is acting as a Data Processor on behalf and under the Instructions of **Mavenir**.
14. **Obligations of Vendor**

**Vendor** agrees and warrants to:

1. Process Personal Data disclosed to it by **Mavenir** only on behalf of and in accordance with the Instructions of the Data Controller, unless **Vendor** is otherwise required by Applicable Law, in which case **Vendor** shall inform **Mavenir** of that legal requirement before Processing the Personal Data, unless informing **Mavenir** is prohibited by law on important grounds of public interest**. Vendor** shall immediately inform **Mavenir** if, in **Vendor’s** opinion, an Instruction provided infringes Applicable Law.
2. Ensure that any person authorized by **Vendor** to Process Personal Data in the context of the Services is only granted access to Personal Data on a need-to-know basis, is subject to a duly enforceable contractual or statutory confidentiality obligation, and only processes Personal Data in accordance with the Instructions of the Data Controller.
3. Inform **Mavenir** promptly and without undue delay of any formal requests from Data Subjects exercising their rights of access, correction or erasure of their Personal Data, their right to restrict or to object to the Processing as well as their right to data portability, and not respond to such requests, unless instructed by **Mavenir** in writing to do so.Taking into account the nature of the Processing of Personal Data, **Vendor** shall assist **Mavenir**, by appropriate technical and organizational measures, insofar as possible, in fulfilling **Mavenir’s** obligations to respond to a Data Subject’s request to exercise their rights with respect to their Personal Data.
4. Assist **Mavenir** in complying with its obligations under Applicable Law, in particular **Mavenir’s** obligation to implement appropriate Data Security Measures, to carry out a data protection impact assessment, and to consult the competent supervisory authority.
5. Maintain internal record(s) of Processing activities, copies of which shall be provided to **Mavenir** by **Vendor** or to supervisory authorities upon request.
6. **Data Transfers**
7. **Vendor** shall not transfer Personal Data protected under this Agreement to a jurisdiction for which the **European Commission** has not issued an adequacy decision without the prior written authorization of **Mavenir**, and provided that appropriate safeguards have been implemented for the transfer of Personal Data in accordance with Applicable Law and the Annex to this Addendum. Vendor agrees to inform **Mavenir** of any legal requirement applicable to Vendor according to which theVendor isrequired to transfer Personal Data outside of the EEA, unless that law prohibits such information on important grounds of public interest.
8. **Sub-Processing**
9. **Vendor** shall not share, transfer, disclose, make available or otherwise provide access to any Personal Data to any third party, or contract any of its rights or obligations concerning Personal Data, unless **Mavenir** has authorized **Vendor** to do so in writing. Where **Vendor**,with the consent of **Mavenir,** provides access to Personal Data to a third party, **Vendor** shall enter into a written agreement with each such third party that imposes obligations on the third party that are the same as those imposed on **Vendor** under this Addendum. **Vendor** shall only retain third parties that are capable of appropriately protecting the privacy, confidentiality and security of the Personal Data.
10. **Compliance with Applicable Laws**
11. **Vendor** shall comply with all Applicable Laws.
12. **Vendor** shall enter into any further data Processing agreement reasonably requested by **Mavenir** for purposes of compliance with Applicable Law.
13. **Data Security**
14. **Vendor** shall develop, maintain, and implement a comprehensive written information security program that shall include appropriate administrative, technical, physical, organizational, and operational safeguards and other security measures designed to (i) ensure the security and confidentiality of Personal Data; (ii) protect against any anticipated threats or hazards to the security and integrity of Personal Data; and (iii) protect against any Personal Data Breach, including, as appropriate:
15. The pseudonymisation and encryption of the Personal Data
16. The ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services
17. The ability to restore the availability and access to the Personal Data in a timely manner in the event of a physical or technical incident; and
18. A process for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures adopted pursuant to this provision for ensuring the security of the Processing.
19. Promptly upon the expiration or earlier termination of the Master Agreement, or such earlier time as **Mavenir** requests, **Vendor** shall return to **Mavenir** or its designee, or at **Mavenir’s** request,securely destroy or render unreadable or undecipherable if return is not reasonably feasible or desirable to **Mavenir** (which decision shall be based solely on **Mavenir’s** written statement), each and every original and copy in every media of all Personal Data in **Vendor’s**, its affiliates’ or their respective subcontractors’ possession, custody or control. In the event applicable law does not permit **Vendor** to comply with the delivery or destruction of the Personal Data, **Vendor** warrants that it shall ensure the confidentiality of the Personal Data and that it shall not use or disclose any Personal Data after termination of this Addendum.
20. **Data Breach Notification**
21. **Vendor** shall immediately inform Mavenir in writing of any Personal Data Breach of which **Vendor** becomes aware, but in no case longer than twenty-four **(24)** hours after it becomes aware of the Personal Data Breach. The notification to Mavenir shall include all available information regarding such Personal Data Breach, including information on:
22. The nature of the Personal Data Breach including where possible, the categories and approximate number of affected Data Subjects and the categories and approximate number of affected Personal Data records
23. The likely consequences of the Personal Data Breach; and
24. The measures taken or proposed to be taken to address the Personal Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

**Vendor** shall promptly take all necessary and advisable corrective actions and shall cooperate fully with **Mavenir** in all reasonable and lawful efforts to prevent, mitigate or rectify such Breach. **Vendor** shall provide such assistance as required to enable **Mavenir** to satisfy **Mavenir**’s obligation to notify the relevant supervisory authority and Data Subjects of a Personal Data Breach under Articles 33 and 34 of the GDPR. The content of any filings, communications, notices, press releases or reports related to any Personal Data Breach must be approved by **Mavenir** prior to any publication or communication thereof. **Vendor** shall be responsible for the costs and expenses associated with the performance of its obligations described in this paragraph unless the Personal Data Breach is caused by the acts or omissions of **Mavenir** or its affiliates.

1. **Audit**

**Vendor** shall make available to **Mavenir** all information necessary to demonstrate compliance with the obligations set forth in this Addendum and allow for and contribute to audits, including inspections, conducted by **Mavenir** or another auditor mandated by **Mavenir**.

1. **Liability**

**Vendor** agrees to indemnify and hold **Mavenir** harmless from and against any losses that it may incur or that arise out of or in connection with a third-party claim relating to (i) any violation of this Addendum, and (ii) **Vendor**’s negligence, gross negligence, bad faith, fraudulent acts or omissions, or intentional or wilful misconduct. In no event shall **Vendor**’s liability be excluded or limited for a violation of its obligations under this Addendum.

1. **Governing Law**

If the Agreement is governed by the laws of a country that is a member of the European Union, then this Addendum shall be governed by the laws of the jurisdiction specified in the Agreement. In all other cases, this Addendum shall be governed by the laws of England.

**IN WITNESS WHEREOF**, the parties acknowledge their agreement to the foregoing by due execution of the Addendum by their duly authorized representatives.

|  |  |
| --- | --- |
| Name: **Mavenir Systems, Inc.**  By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Name:  Title: | Name:  By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Name:  Title: |

## EU Standard Contractual Clauses

**ANNEX**

**EU STANDARD CONTRACTUAL CLAUSES**

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

**Between**

**Mavenir Systems, Inc.** (“**Data Exporter**”)

And

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (“**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.

1. **Definitions**

For the purposes of the clauses:

1. ‘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;
2. ‘the data exporter’ means the controller who transfers the personal data;
3. ‘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**;
4. ‘the sub-processor’ means any processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor 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;
5. ‘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;
6. ‘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.
7. **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. **Third-party beneficiary clause**
2. 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.
3. 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.
4. The data subject can enforce against the sub-processor 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 sub‑processor shall be limited to its own processing operations under the Clauses.
5. 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.
6. **Obligations of the data exporter**

The data exporter agrees and warrants:

1. 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;
2. 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;
3. that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;
4. 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;
5. that it will ensure compliance with the security measures;
6. 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**;
7. to forward any notification received from the data importer or any sub-processor 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;
8. 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 sub-processing 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;
9. that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub- processor 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
10. that it will ensure compliance with Clause 4(a) to (i).
11. **Obligations of the data importer**

The data importer agrees and warrants:

1. 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;
2. 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;
3. that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
4. that it will promptly notify the data exporter about:
5. 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;
6. any accidental or unauthorized access; and
7. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorized to do so;
8. 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;
9. 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;
10. to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, 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;
11. that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;
12. that the processing services by the sub-processor will be carried out in accordance with Clause 11;
13. to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.
14. **Liability**
15. 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 sub-processor is entitled to receive compensation from the data exporter for the damage suffered.
16. 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 sub-processor 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 sub-processor of its obligations in order to avoid its own liabilities.

1. 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 sub-processor 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 sub-processor agrees that the data subject may issue a claim against the data sub-processor 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 sub-processor shall be limited to its own processing operations under the Clauses.
2. **Mediation and jurisdiction**
3. 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:
4. to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
5. to refer the dispute to the courts in the Member State in which the data exporter is established.
6. 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.
7. **Cooperation with supervisory authorities**
8. 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.
9. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, 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.
10. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to Paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).
11. **Governing law**

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

1. **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.

1. **Sub-processing**
2. 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 sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses. Where the sub-processor 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 sub-processor’s obligations under such agreement.
3. The prior written contract between the data importer and the sub-processor 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 sub-processor shall be limited to its own processing operations under the Clauses.
4. The provisions relating to data protection aspects for sub-processing 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.
5. The data exporter shall keep a list of sub-processing 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.
6. **Obligation after the termination of personal data-processing services**
7. The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor 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, thedata importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
8. The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in Paragraph 1.

|  |  |
| --- | --- |
| **On behalf of the Data Exporter:**  Name: Ralf Mueller  Title: Head of Global Procurement  Address: 1700 International Pkwy., #200, Richardson, TX 75081 USA  By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **On behalf of the Data Importer:**  Name:  Title:  Address:  By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

## Appendix 1 to the Standard Contractual Clauses

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

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

**Data Exporter**

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

**Mavenir Systems, Inc.**

**Data Importer**

At the request and direction of Mavenir the Data Importer is operating as a Data Processor of data subject personal data.

**Data subjects**

Mavenir employees and contingent workers (contractors).

**Categories of data**

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

**Personal Information, CV**

**Special categories of data (if appropriate):**

There are no special categories of data applicable in this Addendum.

**Processing operations**

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

**Access**

|  |  |
| --- | --- |
| **On behalf of the Data Exporter:**  Name: Ralf Mueller  Title: Head of Global Procurement  By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | **On behalf of the Data Importer:**  Name:  Title:  By: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

## Appendix 2 to the Standard Contractual Clauses

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

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

Vendor agrees to implement the following technical and organisational security measures:

1. **Physical access control**

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

1. **Virtual access control**

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

* User identification and authentication procedures
* ID/password security procedures (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
* Creation of one master record per user, user master data procedures, per data processing environment
* Encryption and Pseudonymization.

1. **Data access control**

Technical and organizational measures 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 and Pseudonymization

1. **Disclosure control**

Technical and organizational measures 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:

* Logging
* Transport security
* Encryption and Pseudonymization.

1. **Entry control**

Technical and organizational measures 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.

1. **Control of instructions**

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

* Unambiguous wording of the contract
* Formal commissioning (request form)
* Criteria for selecting the processor.

1. **Availability control**

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

* Backup procedures
* Mirroring of hard disks
* Uninterruptible power supply
* Remote storage
* Anti-virus/firewall systems
* Disaster recovery plan.

1. **Separation control**

Technical and organizational measures 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)
* Procedures for storage, amendment, deletion, transmission of data for different purposes.

# 