Digital eMobility Services Master Agreement

December 2021 - Global

1. Subject Matter and Scope

1.1. **Digital eMobility Services Master Agreement.** This Digital Services Master Agreement ("**DeSMA**"), together with the Acceptable Use Policy, the Data Privacy Terms, and the Transaction Documents (collectively, the "eMobility Service Agreement") which is agreed between the Siemens entity ("**we**", "**us**", or "**our**") and the contracting person or entity ("you" or "**your**") indicated in the Order Form, governs your use of certain Services provided to you by us from time to time on or in relation to a cloud-based Platform subject to mutual agreement on respective Order Forms.

1.2. **Definitions.** Capitalized terms used in this document shall have the meaning ascribed to them in Section 15 or elsewhere in this document.

1.3. **Contract Formation.** We are only obliged to provide you with Services if we accept your Order Form for such Services. Each Order Form, upon acceptance by us, shall be binding on the Parties.

1.4. **Out of Scope.** The Services always exclude (i) the provision of any software or services that are not specified by Siemens in the Transaction Documents, even if they interoperate with the Services; (ii) the transmission of data or software to and from the exit of the wide area network of the data centers used by us to provide the respective Service; and (iii) any hardware intended for the connection of devices, systems, or other equipment to the Platform other than explicitly specified in the Transaction Documents. Unless otherwise stipulated in the applicable Transaction Documents you are responsible for securing and maintaining an internet connection and suitable connectivity to the Services at your own expense.

2. Provision of Services

2.1. **Service Standards.** We provide the Services materially in accordance with the features and functionalities set out in the Transaction Documents. We will use commercially reasonable efforts to make the Services available to you subject to operational requirements including maintenance and security. Unless otherwise stipulated in a Transaction Document, a Service is available to you if its user interface is accessible by login at the exit of the wide area network of the data center used by us to provide the Service.

If a Transaction Document contains service level commitments, such service level commitments exclude downtime resulting directly or indirectly from any Service Level Exclusions.

2.2. **Security.** Unless otherwise stipulated in the Transaction Documents, the following shall apply with regard to security: We maintain a formal security program that is designed to protect against threats or hazards to the security of Your Content. Providers of our cloud infrastructure are required to (i) implement and maintain a security program that complies, inter alia, with ISO 27001 or a successor standard (if any) that is substantially equivalent to ISO 27001 and that is designed to provide at least the same risk management and security controls as evidenced by the certification of the providers under ISO 27001 and (ii) have the adequacy of their security measures annually verified by independent auditors. The Platform (i) employs firewalls, anti-malware, intrusion detection/prevention systems (IDS/IPS), and corresponding management processes designed to protect service delivery from malware and (ii) is operated under a security governance model aligned with ISO 27001. This Section contains Siemens' entire obligation regarding the security of Your Content, the Platform, and the Services.

2.3. **Changes to the Services.** We provide Services in a multi-user environment and must therefore reserve the right to modify and discontinue Services. We may modify a Service at any time without degrading its functionality or security features. For current subscriptions, we may degrade the functionality of a Service or discontinue a Service only in case of (i) legal requirements; (ii) changes in the Services imposed by Siemens' subcontractors; (iii) the termination or change of our relationship with a provider of software and/or services used by us which are material for the provision of such Service; (iv) lack of customer acceptance; and/or (v) security risks. We will notify you of any material degradation of functionality or the discontinuation of a Service and the effective date at least 90 days prior to such change, and you may terminate the modified Service 30 days prior to the change effective date. In the event of such termination or discontinuation of a Service, we will refund any prepaid amounts for the applicable Service on a pro-rata basis for the remaining Subscription Term. We do not maintain prior versions of a Service.

2.4. **Changes to the eMobility Service Agreement.** The terms of the eMobility Service Agreement published at the date of an Order Form shall apply until the end of the Subscription Term for the Services agreed in such Order Form and to all Services subsequently ordered and designated as related Services in an Order Form. Any change to the eMobility Service Agreement will only apply from the beginning of a renewed subscription, unless a change during a current Subscription Term is required as a result of a change of Laws or permitted in a Transaction Document or in order to reflect any changes in the Services agreed with or imposed by Siemens' subcontractors (including changes in Third Party or open source software or their license terms) or when we introduce new features, supplements, enhancements, capabilities or Services (e.g. that were not previously included with the subscription, but added for no additional fee). Should a change during a Subscription Term have a material adverse effect on your rights, obligations, or use of the Services, you may terminate the affected Service

within 30 days following our notice. In case of such termination, we will refund any prepaid amounts for the applicable Service on a pro-rata basis for the remaining Subscription Term.

2.5. **Adaptions to fees**

The fees during any renewed Subscription Term will be the same as during the immediately prior Subscription Term, unless we notify you of a change of fees or new fees (collectively referred to as "Fee Change") at least 90 days prior to the end of the then-current Subscription Term, in which case the communicated Fee Change will be effective upon subscription renewal.

During a running Subscription Term, we may conduct a Fee Change due to and to the extent required to reflect: (i) changes in the quality or functionalities of the Services; (ii) material changes in market conditions; (iii)general increases in wages or other employment costs; and/or (iv) changes in procurement costs due to price changes made by our suppliers, in each case to the extent that the changes affect our provision of the agreed Services. We will notify you of any Fee Change at least 90 days in advance of the effective date of the Fee Change.

2.6. **Subcontractors, Location of Data Centers.** To support the rendering of the Services, we may use personnel and resources in various countries, including subcontractors. The locations of data centers used by us for the storage of Your Content at rest are set out in Transaction Documents.

2.7. **Monitoring of Usage.** Without limiting any of our rights in Section 5.1 and 5.2, Siemens or Siemens' subcontractors may monitor Users' usage of Services for Siemens' internal purposes, including: (i) for security and availability reasons; (ii) to ensure compliance with the eMobility Service Agreement; (iii) to detect, prevent, and suspend any use of Services exceeding the permitted use under the eMobility Service Agreement, and otherwise as necessary for payment and billing purposes (also in relation to Third Parties); (iv) to provide you with reports on Users' use of the Services; and (v) to offer you, in accordance with any applicable legal requirements, other products or services that are not yet part of the Services. You will not block or interfere with our monitoring, but may use encryption technology or firewalls to help keep Your Content confidential. We may also use usage information on an aggregated basis to improve the Services, other Siemens products and services, and Siemens' subcontractors' services.

2.8. **Data Privacy**. Each Party shall comply with all applicable data privacy laws and regulations governing the protection of personal data in relation to their respective performance under the eMobility Service Agreement**.** In case Your Content contains personal data and we process the personal data on your behalf acting as your processor, our Data Privacy Terms apply to your use of the relevant Services.

3. Use of Services

3.1. **Use Rights.** We grant you the non-transferable, non-sub-licensable, time-limited and revocable right to access, use and have used the Services for your internal purposes as an end-user, subject to the limitations set out in the eMobility Service Agreement. In any case, Services on the Platform may only be accessed by Users (including Third Parties) via your Account using access Credentials provided by you, by Siemens at your request, or by a Third Party authorized by you. Unless otherwise agreed, the number of permitted Users for a Service shall be on a named-User basis. Access may be reassigned between uniquely identified individual Users over time, but not so frequently as to enable sharing by multiple Users.

3.2. **Value-Add Customers.** If the applicable Transaction Document offers you the option to create subtenants for your customers for your purposes, we grant you in addition to the rights granted in Section 3.1 the non-transferable, non-sublicensable, time-limited, and revocable right to permit your customers (each, a "Value Add Customer") and their Users to access and use the Services under a subtenant that you establish in your Account for each Value-Add Customer (each, a "Value Add Subaccount").

Your Value-Add Customers' Users who access the Services are also your Users. Your provision of Services to Value-Add Customers other than your Affiliates requires a written contract with your Value-Add Customers ("Value Add Contract"). You will ensure that the Value-Add Contracts are consistent with and not less protective of Siemens than the eMobility Service Agreement. Your Value Add Contracts shall contain, at a minimum, the full substance of the terms as set out in the ("**eMobility Minimum Terms**"). You shall remain responsible for the enforceability and enforcement of the Value Add Contracts and their compliance with Laws. Whether you use the eMobility Minimum Terms verbatim or substantially equivalent language of your own, you shall, in any case, ensure and be fully responsible that Value Add Customers and their Users comply with the eMobility Minimum Terms. You will immediately notify us of any non-compliance of Value Add Customers and/ or their Users with the eMobility Minimum Terms and of any related enforcement action you take against a Value-Add Customer and/or their Users.

3.3. **Credentials.** You shall: (i) carefully store access Credentials and security tokens and protect them from unauthorized access; (ii) not gain access to the Services by any means other than your Account or other means permitted by us; (iii) not circumvent or disclose the authentication or security of your Account, the Platform or any host, network, or account related to the Platform; (iv) not use a false identity or Credentials of another person to gain access to your Account, the Platform, or the Services; and (v) ensure that any Credentials are used only by the individual who was granted the Credentials. We may change access Credentials if we determine in our reasonable discretion that a change is necessary.

3.4. **Responsibility for Users and Other Persons.** You are responsible for all activities that occur under your Account and any use of the Services by any User, your employees, or any Third Party to whom you facilitate or permit access to the Services and all liabilities or other consequences arising therefrom as if these were your own acts. This does not apply to the extent damage or a breach is caused by our violation of the eMobility Service Agreement. You will ensure that all Users, your employees, and any Third Party to whom you facilitate or permit access to the Services comply with your obligations under the eMobility Service Agreement. Should you become aware of any violation of your obligations under the eMobility Service Agreement you will immediately terminate the relevant person's access to the Services. You acknowledge and agree that Your Users who submit declarations, notifications, or orders to us act on your behalf and have the legal authority to bind you.

3.5. **Obligations when Using Services.** You are responsible that your use of the Services complies with the Laws at all times. Insofar the following is not included in the Services you ordered from us, you shall (i) obtain at your own expense any rights, consents, and permits from vendors of software, hardware and services used by you in connection with the Services which are necessary for Siemens and its subcontractors to provide the Services and (ii) always keep up to date any software that we provide to you as part of the Services by installing updates and patches as they become available. If the installation of updates and patches is part of our Services, you agree that we may install the updates and patches remotely at our professional discretion. You shall remain responsible for the security of your systems and of on-premises hardware and software. You agree that we are only supporting you in operating your charging infrastructure within the agreed Services You recognize that you are the responsible charge point operator according to the legal, economic and actual circumstances.

3.6. **Your Content.** You are responsible for the development, content, management, use, and quality of Your Content and the means by which you acquire and share Your Content. This includes: (i) the technical operation of Your Content including compatibility of any calls you make to a Service with the Platform APIs; (ii) the transfer or copying of Your Content to data centers outside your country of residence in compliance with Laws; (iii) taking steps to maintain legally required or otherwise appropriate security and protection, including backup and archiving, of Your Content; (iv) any document retention or archiving obligations resulting from Laws or company policies; and (v) ensuring that Your Content can be used by Siemens and its business partners as permitted under this eMobility Service Agreement without violating Laws or rights of others. You shall properly handle any notices and claims sent to you claiming that Your Content violates Third Party's rights or Laws. We will not delete any of Your Content during the Subscription Term unless such deletion is required by a governmental body, to avoid or limit the liability of Siemens or any Third Party, or to protect the security of Siemens' systems.

3.7. **Information Obligations.** You will provide information or other materials related to Your Content that we reasonably request to verify your compliance with the eMobility Service Agreement. If you become aware of any of the following actual or potential events you shall promptly provide us with reasonable information and assistance regarding their mitigation and resolution: (i) unauthorized use of your Account and/or Credentials; (ii) loss or theft of your Account information and/or Credentials; (iii) circumstances or incidents affecting the security of the Platform or Services; or (iv) measures by authorities or court decisions specifically relating to your use of Services or the Platform which may affect the Platform or the Services.

3.8. **Limited Reliance.** You acknowledge and agree that (i) our Services are not designed to be used for the operation of or within a High Risk System if the functioning of the High Risk System is dependent on the proper functioning of the Services and (ii) the outcome from any processing of data through the use of the Services is beyond our control. You are responsible for the use and interpretation of the outcome from such processing and any reliance on such outcome.

3.9. **Notification Services.** Some of our applications offer you the usage of Notifications Services. You may only use the Notification Service to send notifications to recipients who have agreed to receive such notice. You may not use the Notification Service for safety relevant events. Notifications may be blocked, delayed or prevented from being delivered by destinations servers and other reasons outside of our control. There is no warranty that Notification Service will be uninterrupted, secure or error free or that notifications will reach their intended destination during any stated timeframe.

4. Fees, Payment Terms and Taxes

4.1. **General.** You agree to pay all applicable fees specified for the Services and, at the then-current price, all fees for use of Services exceeding the agreed usage or authorizations to us or any person or legal entity appointed by us. Any change of our fees will only apply from the beginning of a renewed subscription. Unless otherwise specified (including but not limited to quotations, Order Forms), fees are due upon receipt of the invoice and payable at no extra cost for us or any person or legal entity appointed by us and without any deduction within 30 days of the invoice date using one of the payment methods we support. Any overdue payment shall accrue interest at the lower of (i) the rate of 2 % per month or (ii) the highest rate legally permitted.

4.2. **Taxes.** All prices and payments relating to the Services are exclusive of any applicable taxes, customs and import duties, levies, and charges of any kind whatsoever, unless otherwise specified (including but not limited to quotations, Order Forms). Any such taxes, customs and import duties, levies, and

charges that may be imposed on or paid by us shall be borne or reimbursed by you. Any sums to be paid to us or any person or legal entity appointed by us shall be net of any applicable taxes, duties and levies that might be levied or withheld on payments made by you to us or any person or legal entity appointed by us . Should any such taxes, duties or levies be levied or withheld by you on payments due to us, then you shall gross up the net payments to us by such an amount necessary to ensure that we receive a net amount equal to the full amount invoiced. In any case, you are obligated to provide us or any person or legal entity appointed by us promptly with the official tax receipt, which confirms the tax payment on our behalf.

5. Proprietary Rights

5.1. **Rights in Your Content.** We will not acquire any rights, title, or interest in or to Your Content, except as granted under the eMobility Service Agreement. Siemens and its business partners have a worldwide, non-exclusive, transferable, sub-licensable, royalty-free right to use, host, store, transmit, display, modify, and reproduce Your Content for the purpose of providing the Services.

5.2. **Rights in Collected Data:** You acknowledge that Collected Data may include copies made by the Services from certain parts of Your Content for use in accordance with the applicable Transaction Documents.

During and after the Subscription Term, Siemens and its business partners may use Collected Data for Siemens internal purposes (e.g. development and improvement of products and services). On an aggregated basis with other data and in a form that does not identify you and your Users, Siemens shall own and be free to make Collected Data publicly available to you and others (e.g. for information and industry trends, benchmarking data). Use of Collected Data in accordance with this Sections will be at Siemens' risk.

5.3. **Rights in the Platform, Services, Feedback.** All rights, title and interest in and to the Platform and the Services, including any know-how and any part and improvement thereof, and all intellectual property rights in or to the foregoing shall remain wholly vested in Siemens, its business partners, and/or licensors. You grant Siemens a worldwide, perpetual, irrevocable, unlimited, transferable, sub-licensable, fully paid, royalty-free license to use any suggestion, recommendation, feature request, or other feedback provided by you or on your behalf related to the Services and/or the Platform.

6. Limited Warranty

6.1. **Conformance with Service Standards.** We warrant that the Services will be provided as set forth in Section 2.1. If Services fail to perform as warranted hereunder, to the extent permissible under Applicable Law, our sole obligation and your exclusive remedy will be (i) to use commercially reasonable efforts to restore the non-conforming Service so that it conforms to the warranty, or (ii) if such restoration would not be commercially reasonable, to terminate the non-conforming Service and refund any prepaid amounts for such Service on a pro-rata basis for the remaining Subscription Term.

6.2. **LIMITATIONS.** SECTION 6.1 SETS OUT THE EXCLUSIVE WARRANTY FROM US AND IT REPLACES ALL OTHER EXPRESS OR IMPLIED WARRANTIES OR CONDITIONS, INCLUDING ANY WARRANTY OR CONDITIONS OF NON-INFRINGEMENT, OR ANY EXPRESS OR IMPLIED WARRANTY OR CONDITIONS OF MERCHANTABILITY, QUALITY AND/OR FITNESS FOR A PARTICULAR PURPOSE, COURSE OF DEALING, OR USAGE OF TRADE. WITHOUT LIMITING THE FOREGOING, SIEMENS DOES NOT WARRANT THAT THE SERVICES WILL BE FAIL-SAFE, FAULT-TOLERANT, UNINTERRUPTED, ERROR FREE, FREE OF HARMFUL COMPONENTS, OR THAT ANY CONTENT, INCLUDING YOUR CONTENT, OR THIRD PARTY SOFTWARE WILL BE SECURE OR NOT OTHERWISE LOST OR DAMAGED. THIS SECTION 6.2 DOES NOT APPLY TO THE EXTENT PROHIBITED BY APPLICABLE LAW.

7. Indemnification

7.1. **Intellectual Property Infringement.** If a Third Party asserts a claim against you that the Services infringe such Third Party's patent or copyright, we will defend you against or, at our option, settle such claim and pay amounts (including costs) finally awarded by a court of competent jurisdiction against you or included in a settlement approved by us.

7.1.1. Notices. You will give us written notice of such claim without undue delay, allow us to control the defense and settlement, and reasonably cooperate with us in this regard. Your failure to provide such notice or cooperation will release us from our obligations under this Section 7.1 if, and to the extent, we are materially prejudiced by such failure.

7.1.2. Exceptions. Our obligations in this Section 7.1 shall not apply to the extent that any such infringement claims arise from: (i) your failure to use the most current version of the Services or a defect correction or patch made available by us; (ii) the combination, operation, or use of the Services in conjunction with any of Your Content or with any Third Party software, equipment, materials, services or products; (iii) an adjustment or configuration of the Services not made by us; (iv) any use of the Services following our notification to you to discontinue such use; or (v) our compliance with designs, plans, or specifications provided to us by you or on your behalf.

7.1.3. Injunction. If a permanent injunction is obtained against you due to an infringement pursuant to Section 7.1, then we will, at our sole discretion: (i) obtain for you the right to continue using the Services; (ii) replace or modify the Services so that they no longer infringe the relevant intellectual property right; or (iii) if neither of the remedies in (i) or (ii) are commercially reasonable, grant you a pro-rata refund of amounts prepaid by you for use of the affected Services, and you shall immediately cease to use the affected Services. We may decide to provide the remedies specified in this Section prior to the issuance of a permanent injunction.

7.1.4. Sole and Exclusive Remedy. To the extent permissible under Applicable Law, this Section 7.1 represents the sole and exclusive remedy available to you against Siemens for infringement of intellectual property rights under the eMobility Service Agreement.

7.2. **Indemnity by You.** You will indemnify Siemens, our suppliers and contractors, and each of their respective employees, officers, directors, and representatives from and against, and, at Siemens' option, defend Siemens from, any claims, damages, liabilities, losses, costs and expenses (including reasonable attorney's fees) arising from or in connection with: (i) Your Content; (ii) any violation of Laws or rights of others by your use of the Services; (iii) any breach by you of the eMobility Service Agreement; (iv) operation, combination, or use of the Services in conjunction with any of Your Content and/or in conjunction with any Third Party software, materials, or services; (v) an adjustment or configuration of the Services made by you or a Third Party to which you facilitate or permit access to the Services, including Users; (vi) our compliance with designs, plans, or specifications provided to us by you or on your behalf; (vii) any claims by any User or any Third Party to which you facilitate or permit access to the Services; (viii) your use of Siemens' trademarks, designations, and logos in breach of the authorization granted to you in a Transaction Document; and (ix) the use of a Service for the operation of or within a High Risk System, if the functioning of a High Risk System depends on the proper functioning of a Service or a Service caused a High Risk System to fail. Section 7.1.1 shall apply mutatis mutandis.

8. Limitation of Liability

8.1. **Limitation.** Except for our obligation under Section 7, Siemens' entire liability for all claims, damages, and indemnities arising out of or related to the eMobility Service Agreement, regardless of the form of action, whether in contract, tort (including negligence) or otherwise, will not exceed, in the aggregate, the fees paid to us by you during the 12 months preceding the date on which the claim arose for the specific Service giving rise to the claim.

8.2. **Disclaimer.** In no event will Siemens be liable for any amounts for loss of production, interruption of operations, contractual claims against you by any Third Party, damage to property, loss or corruption of Your Content or other data, loss of use, loss of interest, income, profit or savings, costs associated with data recovery or re-creation, or indirect, incidental, consequential, exemplary, punitive, or special damages, even if Siemens has been advised of the possibility of such damages in advance, and all such damages are expressly disclaimed.

8.3. **Limitation on Claims.** Any claims against Siemens shall be brought no later than 12 months after the event giving rise to the respective claim. Thereafter all claims arising out of that event against Siemens shall be barred.

8.4. **Scope of Limitations and Exclusions.** The limitation and exclusion in this Section 8 shall not apply: (i) to the extent that liability cannot be limited or excluded according to Applicable Law; (ii) in cases of willful misconduct and gross negligence; (iii) in cases of bodily injuries or death caused by our negligence; and (iv) in cases of fraud or fraudulent misrepresentation. In cases of gross negligence, liability is limited to the amount of foreseeable loss that would have been prevented through the exercise of due care.

8.5. **Beneficiaries.** Any limitations and exclusions of liability shall also apply to the benefit of any employees, officers, directors, representatives, suppliers, subcontractors, and any person used by Siemens in performing any of our obligations.

9. Temporary Suspension

9.1. **Our right to Suspend.** We may suspend or limit Users' use of a Service, or portion thereof, immediately if we reasonably determine that there is a material breach of your obligations or a security incident or threat to the security of the Platform in connection with your access to or use of Services; or if such suspension or limitation is required by Laws, a court decision, or a request from a governmental body. Breaches for failure to pay fees within 10 days after receipt of a reminder or failure to comply with Sections 3 or 12 constitute material breaches. In addition, we may throttle or terminate computing jobs that we determine degrade the performance of the Services or any component of the Services.

9.2. **Effect of Temporary Suspension.** Your obligation to pay fees remains unaffected. If you can reasonably remedy the cause of the suspension or limitation, we will notify you of the actions that you must take to reinstate the Services. The suspension or limitation will be lifted as soon as the reason for such suspension or limitation no longer exists. Our right to terminate pursuant to Section 10 and all other rights and remedies we may have remain unaffected.

10. Termination

10.1. **Termination for Convenience.** The Subscription Term and any renewal of a Subscription Term will be specified in the Transaction Documents and/or the Order Form. A Service may not be terminated for convenience during the Subscription Term.

10.2. **Termination for Cause.** Either Party may terminate a Service for cause in the event of the other Party's material breach if such breach remains uncured for a period of 30 days from receipt of notice specifying the breach by the other Party. Only the Service affected by the material breach may be terminated. Events that entitle us to terminate a Service and/or the eMobility Service Agreement for cause include: (i) acts or omissions that entitle us to a suspension or limitation pursuant to Section 9 that remain uncured for a continuous period of 60 days; (ii) our obligation to comply with Laws or requests of a governmental body; (iii) a change in control of you or your Affiliates that, according to our reasonable opinion, adversely

affects our position, rights, or interests; and (iv) your ceasing to operate in the ordinary course, making an assignment for the benefit of creditors or similar disposition of your assets, or becoming the subject of any bankruptcy, reorganization, liquidation, dissolution, or similar proceeding.

10.3. **Effect of Termination.** On termination of a Service for any reason, subject to Section 10.4, you shall immediately: (i) cease using the affected Service; and (ii) return or, if instructed by us, destroy or delete all Materials relating to the affected Service. Termination of the eMobility Service Agreement shall be deemed as termination of all Services. Except as otherwise set out in the eMobility Service Agreement, you must pay to us all fees due at the time of termination and all fees paid by you to us are non-refundable. In case of termination for cause by you in accordance with Section 10.2, we will refund a reasonable portion of any prepaid amounts for the applicable Service for the remaining Subscription Term. Any terms and conditions of the eMobility Service Agreement, which by their nature should survive a termination or expiry, shall survive and continue in full force and effect after such termination or expiry.

10.4. **Post-Termination Phase.** After termination of a Service, we will remove Your Content that is associated with such Service from the Platform, unless otherwise provided under the eMobility Service Agreement or agreed in writing. However, upon your request made within 30 days following the termination date, we will assist you in transitioning certain parts of Your Content to an alternate technology for additional fees and under separately agreed terms, to the same extent that we make such services generally available to all our customers. You acknowledge that some of Your Content may be retained by us as part of our disaster recovery backup of the Platform until deletion of such files in accordance with our policies.

11. Confidentiality, Compelled Disclosure

11.1. **Confidentiality Obligations.** Each Party shall treat Confidential Information disclosed by the other Party or its Affiliates as confidential, only use it in connection with the Services or as otherwise permitted under the eMobility Service Agreement (i.e. in the respective Transaction Documents), and not disclose such Confidential Information to anyone except to those Users, employees, Affiliates, business partners and advisors, and the respective employees of such Affiliates, business partners and advisors who need to know that information for implementation of the eMobility Service Agreement and who are bound to appropriate confidentiality obligations or as explicitly specified in the respective Transaction Documents.

11.2. **Compelled Disclosure**. We will not disclose Confidential Information and/or any of Your Content to any Third Party except (i) as instructed by you, (ii) as permitted in the eMobility Service Agreement, or (iii) as required by Laws or governmental order. Should any Third Party (including governmental bodies) contact us with a request to disclose Confidential Information or any of Your Content, we will redirect such Third Party to request that data directly from you and may provide your basic contact information unless we are prohibited from doing so by Laws or governmental order. If we are compelled to disclose Confidential Information or any of Your Content to any Third Party, we will promptly notify you and provide a copy of the request unless we are prohibited from doing so by Laws or governmental order. We may further disclose Confidential Information or Your Content to Third Parties in order to report to them potential violations of Laws in connection with your use of the Services.

12. Export Control and Sanctions Compliance

12.1. **Export and Sanctions Laws.** You agree to comply with all applicable sanctions, embargoes and (re-)export control regulations, and, in any event, with those of the European Union, the United States of America and the jurisdiction in which the Services are made available to you (collectively "**Export Regulations**").

12.2. **Your Obligations.** In particular, you shall not, unless permitted by the Export Regulations or respective governmental licenses or approvals, (i) access or use the Services from any location prohibited by or subject to comprehensive sanctions (currently Cuba, Iran, North Korea, Syria, and the Crimea region of Ukraine) or license requirements according to the Export Regulations; (ii) grant access, transfer or otherwise make available to any individual or entity designated on a sanctioned party list of the Export Regulations; (iii) use the Services for any purpose prohibited by the Export Regulations (e.g. use in connection with armaments, nuclear technology or weapons); (iv) upload to the Services platform any content unless it is non-controlled (e.g. in the EU: AL = N; in the U.S.: ECCN = N or EAR99).

12.3. **Your Users.** You shall provide any individual or entity to whom you grant access, transfer or otherwise make available the Services (collectively "**User(s)**") with all information necessary to ensure compliance with the Export Regulations. You shall (i) be responsible for the use of the Services by any User; (ii) procure to pass on all of your obligations under this eMobility Service Agreement to each User; (iii) ensure that all Users comply with your obligations under this eMobility Service Agreement. Should you become aware of any violation of your obligations under this eMobility Service Agreement, you shall immediately terminate the relevant User's access to the Services.

12.4. **Information Requirements.** If required to enable authorities or Siemens to conduct export control checks, you, upon request by us, shall promptly provide us with all information pertaining to User(s), the intended use and the location of the use of the Services.

12.5. **Indemnity by You.** You shall indemnify and hold harmless Siemens from and against any claim, proceeding, action, fine,

loss, cost and damages arising out of or relating to any noncompliance with Export Regulations by you and/or User(s), and you shall compensate Siemens for all losses and expenses resulting thereof.

12.6. **Right to Withhold Performance.** We shall not be obligated to perform under the eMobility Service Agreement if such performance is prevented by any impediments arising out of national or international foreign trade or customs requirements or any embargoes or other sanctions. You acknowledge that Siemens may be obliged under the Export Regulations to limit or suspend access by you and/or Users to the Services.

13. Limitations for Free of Charge Services, Trials, Beta

13.1. **Provision of Services.** Where we enable you to access and use Services free of charge, e.g., certain free online support services, services for testing and evaluation purposes, "trial" services, "pre-release", "beta", or "preview" versions (such Services collectively "**Free of Charge Services**"), the limitations under this Section 13 apply in addition to any additional limitations in the eMobility Service Agreement, including Sections 6.2 and 8.

13.2. **Change, Limitation, Suspension.** We may change, limit, or discontinue any Free of Charge Service and your access to and use of any Free of Charge Service in our sole discretion. Your Content may be deleted upon the expiration or discontinuation of the Free of Charge Service, unless specific migration to the related paid Services is available and agreed.

13.3. **Service Standards and Limited Use Right.** Free of Charge Services for testing or evaluation and any "pre-release", "beta", or "preview" versions may only be used for the purpose of evaluating their functionality and to provide feedback to Siemens. Such Free of Charge Services may not comply with the normal security standards as per Section 2.2, their performance and availability may be lower than paid Services, personal data may not be processed, and productive use is at your own risk.

13.4. **Warranty and Liability.** Except to the extent prohibited by Applicable Law, Free of Charge Services are provided "as is" without warranties of any kind and in the then-current version made available by us from time to time without support and availability commitments. We are not obliged to offer post-termination assistance. Siemens' entire liability for all claims, damages, and indemnities arising out of or related to your use of a Free of Charge Service will not exceed, in the aggregate, the amount of EUR 1,000.00 (or the equivalent amount in local currency).

14. General Provisions

14.1. **Assignment.** The eMobility Service Agreement will extend to and be binding upon the successors and permitted assignees of the Parties. We may assign the eMobility Service Agreement or any right granted thereunder or individual orders to any of our Affiliates that assume our obligations. You shall not assign the eMobility Service Agreement, in whole or in part, or any of the rights granted thereunder without our prior written consent.

14.2. **Set-off, Retention.** You may only set off claims or assert a right of retention with regard to claims that are uncontested by us, are ready for decision, or have been confirmed by final court judgment.

14.3. **Force Majeure.** Neither Party shall be liable for any failure or delay in its performance under the eMobility Service Agreement due to any cause beyond its reasonable control, including acts of God, earthquake, fire, flood, embargo, riot, sabotage, attacks on IT systems by Third Parties (e.g., hacker attacks), labor shortage or dispute, acts or omissions of civil or military authorities, war, or terrorism (**"Force Majeure Event"**).

14.4. **Dispute Resolution.** All disputes arising out of or in connection with the eMobility Service Agreement, including the formation, interpretation, amendment, breach, or termination thereof, shall be finally settled as set forth in the table below.

If the Siemens entity named in the Order Form is in:	**Any dispute arising out of or in connection with the eMobility Service Agreement shall be:**
a country in North or South America, with the exception of Brazil	finally resolved by binding arbitration in accordance with the Rules of Arbitration of the International Chamber of Commerce ("ICC Rules"). The seat of arbitration shall be New York, NY, USA.
Brazil	subject to the jurisdiction and venue of the Court of Sao Caetano do SulSP, Brazil.
A Country in Asia or Australia/Oceania, with the exception of Japan	finally resolved by binding arbitration in accordance with ICC Rules. The seat of arbitration shall be Singapore.
Japan	finally resolved by binding arbitration in accordance with ICC Rules. The seat of arbitration shall be Singapore.
A country not covered by the above	finally resolved by binding arbitration in accordance with ICC Rules. The seat of arbitration shall be Zurich, Switzerland.

In the event that a dispute is subject to arbitration as described in the table above, arbitrators shall be appointed in accordance with the applicable ICC Rules; the language to be used in the arbitration shall be English and any orders for the production or disclosure of documents shall be limited to the documents on which each Party specifically relies in its submission(s). Nothing in this section 14.4 shall restrict the right of the Parties to seek interim relief intended to preserve the status quo or interim measures in any court of competent jurisdiction.

14.5. **Applicable Law.** The eMobility Service Agreement shall be governed by and construed in accordance with the laws set forth in the table below (without giving effect to any choice-of-law rules that may require the application of the law of another jurisdiction. The UN Convention on Contracts for the International Sale of Goods shall not apply.

If the Siemens entity named in the Order Form is in:	**The applicable law shall be:**
a country in North or South America, with the exception of Brazil	the Laws of the state of New York, USA
Brazil	The laws of Brazil
A Country in Asia or Australia/Oceania, with the exception of Japan	The laws of Singapore
Japan	The Laws of Japan
A country not covered by the above	The laws of Switzerland

14.6. **Notices.** We may provide notice to you under the eMobility Service Agreement by: (i) posting a notice on your Account or (ii) sending a message to the email address provided to us as part of the ordering process for an Order Form or then associated with your Account. It is your responsibility to regularly visit your Account and to keep your email address current. If you do not comply with such obligation or if your receipt of a notice fails because of technical issues related to equipment or services which are under your or your subcontractors' control, notices shall be deemed to have been provided to you 2 days following the date of such notice. Notices to us shall be sent to the email address provided in the respective Order Form and/or Transaction Documents. Notwithstanding the foregoing, notices of claims or notices regarding disputes shall always be sent by facsimile or postal mail to the contact addresses provided in the respective Order Form and/ or Transaction Documents.

14.7. **Validity and Enforceability.** If any provision of the eMobility Service Agreement is held to be invalid, illegal or unenforceable, the validity, legality, and enforceability of the remaining provisions will not in any way be affected or impaired, and such provision will be deemed to be restated to reflect the original intentions of the Parties as nearly as possible in accordance with Applicable Law.

14.8. **Publicity.** Except as may be required by Applicable Law, neither Party shall issue a press release in connection with the subject matter hereof without the prior written consent of the other Party, which shall not be unreasonably withheld. Notwithstanding the foregoing, the Parties shall have the limited right to disclose the terms of the eMobility Service Agreement to their bona fide financial, tax, and legal advisors subject to appropriate confidentiality obligations.

14.9. **Entire Agreement.** The eMobility Service Agreement constitutes the full and complete statement of the terms agreed between the Parties with respect to the subject matter thereof and supersedes any previous or contemporaneous agreements, understandings, or communications, whether written or verbal, relating to its subject matter. The reference to a document that refers to another document shall be deemed to also include such other document, unless otherwise stated therein. Subject to Section 2.4, the eMobility Service Agreement may not be varied other than in writing executed by the duly authorized representatives of both Parties or via an online mechanism, if so provided explicitly for such purpose by us. No other terms and conditions shall apply.

14.10. **Order of Precedence**. In the event of a conflict or inconsistency the documents prevail in the following descending order: (i) Order Form; (ii) Transaction Documents; (iii) the Data Privacy Terms (Exhibit 2); (iv) the Acceptable Use Policy (Exhibit 1); and (v) this document at hand. If a document is provided in different languages, the English language version of that document prevails.

14.11. **Independent Contractors.** For all purposes, the Parties will be deemed to be independent contractors, and nothing contained in the eMobility Service Agreement will be deemed to constitute a joint venture, partnership, employer-employee relationship or other agency relationship. Neither Party is, nor will either Party hold itself out to be, vested with any power or right to contractually bind or act on behalf of the other Party.

15. Definitions

15.1. "**Acceptable Use Policy**" means the document listed in Exhibit 1.

15.2. "**Account**" means one or more web-based accounts, individually or collectively, enabling access to and use of certain Services provided on the Platform through a unique URL (i.e. web-address) assigned by Siemens, including any subtenants established under the Account.

15.3. "**Affiliate**" means a corporation or other legal entity, directly or indirectly, owned or controlled by, or owning or controlling or under common control with one of the Parties where "control" shall mean to have, directly or indirectly, the power to direct or cause the direction of the management and policies of a corporation or other entity.

15.4. "**Applicable Law**" means the law specified in Section 14.5.

15.5. "**Application**" means software that is deployed on the Platform and/or interoperates with the Platform via Platform APIs.

15.6. **"Available" and "Availability"** for cloud-based-application mean: The respective Service is Available if at least 4 out of 5 times within a 5-minutes interval (where logins are performed every minute) the user interface is accessible at the exit of the wide area network of the data center used by us. Such interval measurements shall be performed by us evenly distributed 288 times a day.

15.7. "**Confidential Information**" means any information disclosed by a Party or its Affiliate to the other Party under or in connection with the eMobility Service Agreement and which is – when disclosed – identified as "Confidential" or consists of information that, by its nature or context, is sufficient to put the receiving Party on notice of its confidential nature. In addition, any information and materials obtained by you in connection with the eMobility Service Agreement or your receipt of Services, including the performance and availability of the Services, the Platform, information regarding Siemens' or our business partners' business strategies and practices, methodologies, trade secrets, know-how, pricing, technology, software, application programming interfaces, application programming interface signatures, product plans, and information regarding Siemens' employees, clients, vendors and consultants, are deemed to be our Confidential Information. Confidential Information does not include information that: (i) is generally available to the public without breach of the eMobility Service Agreement and without any wrongdoing; (ii) is or becomes available to the recipient from a source other than the Party who discloses the Confidential Information, provided that the recipient has no reason to believe that such source is itself bound by a confidentiality obligation or that such source has obtained the information through any wrongful or tortious conduct; (iii) was lawfully in the recipient's possession prior to receipt from the other Party without a corresponding obligation of confidentiality; (iv) is independently developed by the recipient without the use of, or reference to, Confidential Information; or (v) has been released by the disclosing Party for non-confidential use e.g. in a Transaction Document.

15.8. **"Credentials**" are access Credentials and security tokens as well as RFID-cards.

15.9. **"Collected Data"** means any information, code in any form, or data collected (i) by the cloud based applications or / and (ii) used for other related services we provide to you as specified in the applicable Transactions Documents. You acknowledge that Collected Data may include copies made by our applications of portions of Your Content for use in accordance with the eMobility Service Agreement..

15.10. "**Data Privacy Terms**" means the document listed in Exhibit 2.

15.11. "**High Risk System**" means a device or system that requires enhanced safety functionalities such as fail-safe or fault-tolerant features to maintain a safe state where it is reasonably foreseeable that failure of the device or system could lead directly to death, personal injury, or catastrophic property damage. Without limitation, High Risk Systems may be required in critical infrastructure, direct health support devices, aircraft, train, boat, or vehicle navigation or communication systems, air traffic control, weapons systems, nuclear facilities, power plants, medical systems and facilities, and transportation facilities.

15.12. "**Laws**" means any law, rule, regulation, norm, or directive including, without limitation, industry or company specific regulations, co-determination rights of the works council, data privacy, telecommunication, energy law, IT security law, export control, sanctions, and regulation pertaining to the protection of classified information.

15.13. "**Material**" means any software, sample code, scripts, libraries, software development kits, technology, documentation, and other proprietary material or information made available to you by or on behalf of us in relation to our provision of Services.

15.14. **"Monthly Uptime Percentage"** meant the percentage of a Service being Available in average during a Month, based on our Availability measurements. Monthly Uptime Percentage excludes downtime resulting directly or indirectly from any Service Level Exclusions.

15.15. **"Month"** means a calendar month.

15.16. "**Order Form**" means a document, electronic form, or online instrument provided by Siemens for the ordering of Services.

15.17. "**Platform APIs**" means Siemens' application programming interfaces that are integrated with the Platform or the Services. Platform APIs are part of the Platform and the Services.

15.18. **"Party**" means you or us, depending on the context.

15.19. "**Platform**" means a cloud-based platform solution on which the Services are provided. Platform may include Siemens' operating system MindSphere as well as other Siemens branded cloud-based solutions that underlie the Services.

15.20. **"Services"** means (i) the cloud services and related services as described in the Transaction Documents and (ii) Materials.

15.21. "**Siemens**" means Siemens AG (Germany) and its Affiliates.

15.22. **"Service Level Exclusions"** mean unavailability, suspension or termination of the Services, or any other performance issues affecting the Services: (i) caused by factors

outside of our reasonable control, including any Force Majeure Event; (ii) that result from any actions or inactions of you or any Third Party; (iii) that result from your equipment, software or other technology and/or Third Party equipment, software or other technology (other than Third Party equipment within our direct control); (iv) that result from any planned maintenance, (v) arising from our suspension or termination of the Services in accordance with the eMobility Service Agreement.

15.23. "**Transaction Documents**" means the documents which describe and/or further govern the Services and which are referenced in the Order Form.

15.24. "**Subscription Term**" means the period for which a Service is agreed as specified in the Order Form.

15.25. "**Third Party**" means any person or legal entity other than you or Siemens. Third Party includes your Affiliates.

15.26. "**User**" means an individual who has access Credentials to your Account, including individuals of Third Parties, or who is otherwise authorized by you to access your Account. Access to your Account includes access to any subtenant that you establish under your Account, to any Application associated with your Account, to Your Content, and/or the Services.

15.27. "**Your Content**" means any information, program, software, Application, code in any form, script, library, or data that is entered, uploaded onto, or stored on the Platform in connection with your or any User's use of Services under your Account. Your Content excludes the Services and the Platform.

EXHIBIT 1:

Acceptable Use Policy

This Acceptable Use Policy ("**Policy**") sets out terms with which you must comply when using our Services.

1. **Definitions**

Capitalized terms shall have the meaning given to them in the terms governing the Services.

2. **No Illegal, Harmful, or Offensive Use of Your Content**

You shall not use, or encourage, promote, facilitate, or instruct others to use, the Services for any illegal, harmful, or offensive use. Your Content must not be illegal, harmful, or offensive. In particular, your use of the Services, Your Content and your use of Your Content shall not:

(i) be in violation of any Laws or rights of others;

(ii) be harmful to others, or Siemens' operations or reputation, including by offering or disseminating fraudulent goods, services, schemes, or promotions, make-money-fast schemes, ponzi or pyramid schemes, phishing, farming, or other deceptive practices;

(iii) enter, store or send hyperlinks, enable access to external websites or datafeeds, including embedded widgets or other means of access, in or as part of Your Content, for which you have no authorization or which are illegal;

(iv) be defamatory, obscene, abusive, invasive of privacy, or otherwise objectionable;

(v) subject Siemens or its business partners to liability.

3. **No violation of use restrictions**

You shall not:

(i) copy, sell, resell, license, transfer, assign, sublicense, rent, lease, or otherwise make available the Services or the Platform in whole or in part to any Third Party (unless permitted otherwise by us or required by Laws);

(ii) translate, disassemble, decompile, reverse engineer or otherwise modify, tamper with, repair or attempt to discover the source code of any software contained in the Services or the Platform (unless permitted otherwise by us or required by Laws);

(iii) create derivative works of, or based on, any parts of the Services or the Platform;

(iv) change or remove any notices or notations from the Services or the Platform that refer to intellectual property rights or brand names;

(v) imitate the "look and feel" of any of Siemens' website or other user interface, nor the branding, color combinations, fonts, graphic designs, product icons or other elements associated with Siemens;

(vi) upload to the Platform any of Your Content that is subject to a license that, as a condition of use, access, and/or modification of such content, requires that any Siemens' or Siemens' business partners' software or service provided by Siemens and interacting with or hosted alongside Your Content: (a) are disclosed or distributed in source code form; (b) are licensed to recipients for the purpose of making derivative works; (c) are licensed at no charge; (d) are not used for commercial purposes; or (e) are otherwise encumbered in any manner; and

(vii) access the Services from any location prohibited by or subject to sanctions or license requirements according to applicable sanctions and/or (re-)export control regulations, including those of the European Union, the United States of America and/or any other applicable country/-ies;

(viii) grant access, transfer or otherwise make available to any individual or entity designated on any applicable sanctioned party list;

(ix) use the Services for any purpose prohibited by applicable export control regulations; and

(x) upload to the Services platform any content unless its is non-controlled (e.g. in the EU: AL = N; in the U.S.: ECCN = N or EAR99").

4. **No Abusive Use**

You shall not do any of the following:

(i) use the Services in a way intended to avoid or work around any use limitations and restrictions placed on such Services, such as access and storage restrictions or to avoid incurring fees;

(ii) access or use the Services for the purpose of conducting a performance test, building a competitive product or service or copying its features or user interface or use the Services in the operation of a business process outsourcing or other outsourcing or a time-sharing service;

(iii) interfere with the proper functioning of any of Siemens' systems, including any overload of a system by mail bombing, news bombing, broadcast attacks, or flooding techniques;

(iv) engage in any activity or modification or attempt to modify the Platform or the Services in such a way as to negatively impact on the performance of the Platform or the Services.

5. **No Security Violations**

You shall not use the Services in a way that results in, permits, assists or facilitates any action that constitutes a threat to the security of the Platform or the Services. You shall in particular:

(i) before accessing the Services, during use, and when transferring Your Content, take all reasonable precautions against security attacks on your system, on-site hardware, software or services that you use to connect to and/or access the Platform, including appropriate measures to prevent viruses, trojan horses or other programs that may damage software;

(ii) not interfere with or disrupt the integrity or performance of the Services or other equipment or networks connected to the Platform, and in particular not transmit any of Your Content containing viruses, trojan horses, or other programs that may damage software;

(iii) not use the Services in a way that could damage, disable, overburden, impair or compromise any of Siemens' systems or their security or interfere with other Users of the Platform;

(iv) not perform any penetration test of or on the Services or the Platform without obtaining our express prior written consent; and

(v) not connect devices to the Services that do not comply with industry standard security policies (e.g., password protection, virus protection, update and patch level).

6. **Reporting**

If you become aware of any violation of this Policy, you will immediately notify us and provide us with assistance, as requested by us, to stop, mitigate or remedy the violation.

SIEMENS

Data Privacy Terms

September 2021

The Data Privacy Terms ("**DPT**") are agreed between the Siemens entity ("**we**", "**us**", or "**our**") and the customer ("**you**" or "**your**") named in the Agreement.

1. Scope and compliance with laws

1.1. The DPT and the DPT Exhibits shall apply to Services provided under the Agreement that involve the Processing of Personal Data by us acting as Processor or Subprocessor for you. The DPT are incorporated into the Agreement, in the event of conflicts, the DPT Exhibits prevail over the DPT which prevails over the remainder of the Agreement.

1.2. The DPT describe your and our data protection related rights and obligations with regard to the Services captured by the DPT. All other rights and obligations shall be exclusively governed by the other parts of the Agreement.

1.3. When providing the Services, we will comply with all data protection laws and regulations directly applicable to our provision of the Services, including security breach notification law. However, we are not responsible for compliance with any data protection laws or regulations applicable to you or your industry that are not generally applicable to Processors. You shall comply with all laws and regulations applicable to your use of the Services, including Applicable Data Protection Law, and ensure that we and our Subprocessor are allowed to provide the Services as described in the DPT.

2. Details of the processing, Instructions

2.1. The details of the Processing operations provided by us, including the scope, the nature and purpose of the Processing, the types of Personal Data Processed and the categories of affected Data Subjects, are specified in the DPT Exhibits.

2.2. We will Process Personal Data only in accordance with your documented instructions. You agree that the Agreement (including the DPT and the DPT Exhibits), along with your use and configuration of features in the Services (where available), are your complete and final documented instructions to us for the processing of Personal Data. Any additional or alternate instructions must be agreed between you and us in writing.

3. Technical and organizational measures

3.1. We will implement appropriate technical and organizational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed. The technical and organizational measures implemented are described in the DPT Security Exhibit.

3.2. You understand and agree that the technical and organizational measures are subject to technical progress and development. In that regard, we shall have the right to implement adequate alternative measures as long as the security level of the measures is maintained.

3.3. You are responsible for implementing and maintaining privacy protections and security measures for components that you provide or control, such as implementing physical and system access control measures for your own premises, assets and IT-systems or configuring the Services to your individual requirements.

4. Confidentiality of the processing

We will ensure that personnel who are engaged in the Processing of Personal Data (i) are under an obligation to maintain the confidentiality of such data, (ii) will process such data only as described in this DPA or on your documented instructions and (iii) receive adequate privacy and security trainings.

5. Subprocessors

5.1. You hereby approve the engagement of Subprocessors by us. A current list of Subprocessors commissioned by us is available in the DPT Exhibits.

5.2. We may remove or add new Subprocessors at any time. If required by Applicable Data Protection Law, we will obtain your approval to engage new Subprocessors in accordance with the following process: (i) we shall notify you with at least 30 days' prior notice before authorizing any new Subprocessor to access your Personal Data; (ii) if you raise no reasonable objections that include an explanation of the grounds for non-approval in writing within this 30 day period, then this shall be taken as an approval of the new Subprocessor; (iii) if you raise reasonable objections, we will - before authorizing the Subprocessor to access your Personal Data - use reasonable efforts to (a) recommend a change to your configuration or use of the Services to avoid Processing of Personal Data by the objected-to new Subprocessor or (b) propose other measures that address the concerns raised in your objection; (iv) if the proposed changes or measures cannot eliminate the grounds for non-approval, you may terminate the affected Service without penalty with 14 days' written notice following our response to your objection. If you do not terminate the affected Service within the 14-day period, this shall be taken as an approval of the Subprocessor by you.

5.3. In case of any commissioning of Subprocessors, we shall enter into an agreement with such Subprocessor imposing appropriate contractual obligations on the Subprocessor that are no less protective than the obligations in this DPT. We remain responsible for any acts or omissions of our Subprocessors in the same manner as for our own acts and omissions hereunder.

6. Transfers to Non-EEA Recipients

6.1. In case Transfers to Non-EEA Recipients relate to Personal Data originating from a Controller located within the EEA, Switzerland, or the United Kingdom, we shall implement the Transfer Safeguards identified per Subprocessor in the DPT Exhibits. It is your responsibility to assess whether the respective Transfer Safeguards implemented suffice for you and your Further Controllers to comply with Applicable Data Protection Law. If you believe that the Transfer Safeguards identified do not suffice to meet your requirements under Applicable Data Protection Law, you shall notify us and the parties to agree to cooperate in good faith to find and implement alternative safeguards.

6.2. The following shall apply if a Transfer Safeguard is based on the Standard Contractual Clauses: We enter into such Standard Contractual Clauses with the relevant Subprocessor. Customer and Further Controllers (if any) shall become a data exporter under the Standard Contractual Clauses as follows: (i) the Standard Contractual Clauses shall contain the right for Customer and Further Controllers to join the Standard Contractual Clauses as data exporter ("Accession Mechanism"); or (ii) We enter into the Standard Contractual Clauses with the Subprocessor acting as data importer on behalf of the Customer and Further Controllers acting as data exporters ("Mandate Mechanism").

6.3. The following shall apply if a Transfer Safeguard is based on BCR-P: We shall contractually bind such Subprocessor to comply with the BCR-P with regard to the Personal Data Processed under this DPT.

7. Personal Data Breach

In the event of any Personal Data Breach, we shall notify you of such breach without undue delay after we become aware of it. We shall (i) reasonably cooperate with you in the investigation of such event; (ii) provide reasonable support in assisting you in your security breach notification obligations under Applicable Data Protection Law (if applicable); and (iii) initiate respective and reasonable remedy measures.

8. Data subject rights, Our assistance

8.1. We shall, to the extent legally permitted, promptly notify you if we receive a request from a Data Subject to exercise their Data Subject's rights (such as the right to access, rectification, erasure or restriction of Processing).

8.2. Taking into account the nature of the Processing and the information available to us, we shall reasonably assist you (i) in the fulfilment of your obligation to respond to requests for exercising Data Subject's rights or (ii) to comply with its obligations under Applicable Data Protection Law. Any such additional assistance shall be mutually agreed between the parties.

9. Audits

9.1. You shall have the right to audit, by appropriate means - in accordance with Sections 9.2 to 9.5 below - our and our Subprocessors' compliance with the data protection obligations hereunder annually (in particular in regard to the technical and organizational measures implemented). Such audits shall be limited to information and data processing systems that are relevant for the provision of the Services provided to you.

9.2. We and our Subprocessors may use (internal or external) auditors to perform audits to verify compliance with the data protection obligations hereunder. Each audit will result in the generation of an audit report ("**Audit Report**"). Upon your request, we shall provide such relevant Audit Reports for the Services concerned.

9.3. If required under Applicable Data Protection Law, we will allow for additional audits, including onsite audits at our facilities and premises by you or an independent, accredited third party audit firm, during regular business hours, with reasonable advance notice to us. You are responsible for your costs and fees related to such audit.

9.4. The Audit Reports and any further information and documentation provided during an audit shall constitute confidential information and may only be provided to Further Controllers pursuant to confidentiality obligations substantially equivalent to the confidentiality obligations contained elsewhere in the Agreement. In case audits relate to Subprocessors, we may require you and Further Controllers to enter into non-disclosure agreements directly with the respective Subprocessor before issuing Audit Reports and any further information or documentation to you or Further Controllers.

10. Single point of contact and liability

10.1. You shall serve as a single point of contact for us, also with regard to Further Controllers under the terms of this DPT.

10.2. In case this DPT or any of the Transfer Safeguards in Section 6 (such as Standard Contractual Clauses) provide rights to Controllers (including Controllers other than you) in relation to us and/or our Subprocessors, you shall exercise these rights by contacting us directly, in your own name and/or on behalf of the respective Controller. We shall be entitled to refuse any requests, instructions or claims provided directly by a Controller other than you.

10.3. In case the DPT or any of the Transfer Safeguards contain notification obligations vis-a-vis Controllers, we shall be discharged of our obligation to notify a Controller when we have provided such notice to you.

10.4. Without prejudice to the statutory rights of Data Subjects, limitations of liability contained in the Agreement shall also apply to our and our Subprocessors' liability (taken together in the aggregate vis-à-vis you and your Further Controllers) under the DPT (and any of the Transfer Safeguards specified in Section 6).

10.5. You shall be responsible to ensure that the limitations contained in Sections 10.1 to 10.4 above are enforceable by us and our Subprocessors vis-à-vis your Further Controllers.

11. Notices

11.1. We may provide notice to you under the DPT by: (i) posting a notice as described in the Agreement or (ii) sending a message to the email address provided to us as part of the ordering process for an Service.

11.2. Notices concerning Subprocessors under section 5 of the DPT may additionally be given by granting you access to a website that lists all current Subprocessors and provides you with a mechanism to obtain notice of any new Subprocessor.

11.3. It is your responsibility to keep your contact information for notices current.

12. Term and termination

The DPT shall have the same terms as the Agreement. Upon termination of the DPT, unless otherwise agreed between the parties in the Agreement, we shall erase all Personal Data made available to us or obtained or generated by us on your behalf in connection with the Services.

13. **Definitions**

13.1. "**Agreement**" means the commercial agreement on the provision of the Services between you and us referencing the DPT.

13.2. "**Applicable Data Protection Law**" means all applicable law pertaining to the Processing of Personal Data hereunder.

13.3. "**Binding Corporate Rules for Processor**" or "**BCR-P**" shall mean Binding Corporate Rules for Processors approved in accordance with Article 47 of the General Data Protection Regulation (EU) 2016/679.

13.4. "**Controller**" means the natural or legal person which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

13.5. "**Country with an Adequacy Decision**" shall mean a country outside the EEA where the European Commission has decided that the country ensures an adequate level of protection with respect to Personal Data.

13.6. "**Data Subject**" means an identified or identifiable natural person.

13.7. "**DPT**" shall mean this Data Privacy Terms.

13.8. "**DPT Exhibits**" shall mean the documents which describe the scope, the nature and purpose of the Processing, the types of Personal Data Processed, the categories of affected Data Subjects and technical and organizational measures and which are referenced in the Agreement.

13.9. "**EEA**" shall mean the European Economic Area.

13.10. "**Further Controller**" shall mean any third party (such as an affiliated company of you) acting as Controller which is entitled to use or receive Offerings under the terms of the Agreement.

13.11. "**Personal Data**" means information that relates, directly or indirectly, to a Data Subject, including without limitation, names, email addresses, postal addresses, identification numbers, location data, online identifiers or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person. Personal Data, for the purposes of this DPT, includes only such Personal Data entered by you or any Further Controller into or derived from the use of the Services or that is accessed by us in the context of providing the Services.

13.12. "**Personal Data Breach**" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data Processed under the terms of this DPT.

13.13. "**Processor**" means a natural or legal person, public authority, agency or any other body which Processes Personal Data on behalf of a Controller.

13.14. "**Process**" or **Processing**" means any operation or set of operations which is performed upon Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, access to, transfer, and disposal.

13.15. "**Services**" shall mean the services under the Agreement provided by us acting in its role as Processor, including cloud, hosting and support services.

13.16. "**Standard Contractual Clauses**" means the Standard Contractual Clauses for the Transfer of Personal Data to Processors Established in Third Countries pursuant to Commission Decision 2010/87/EU of 5 February 2010 or any successor document issued by the European Commission.

13.17. "**Subprocessor**" shall mean any further Processor engaged by us that has access to Personal Data.

13.18. "**Special Categories of Personal Data**" shall mean information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, social security measures, administrative or criminal proceedings and sanctions, or genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

13.19. "**Transfer Safeguards**" shall mean (i) an adequacy decision in the meaning of Article 45 of the General Data Protection Regulation (EU) 2016/679 or (ii) appropriate safeguards as required by Article 46 of the General Data Protection Regulation (EU) 2016/679.

13.20. **"Transfers to Non-EEA Recipients"** shall mean (i) the Processing of Personal Data outside the EEA or a Country with an Adequacy Decision or (ii) any accesses to Personal Data from outside the EEA or a Country with an Adequacy Decision by us or any of our Subprocessors.

SIEMENS

DPT Exhibits - Description of the Processing Operations

The parties may provide further details in the Transaction Documents if required for a particular Service.

Processing operations

We and our Subprocessors will Process Personal Data to provide the Services, including as applicable:

- Internet accessible e-mobility services made available by us ("Cloud Services");
- Administration, management, maintenance and support services ("Support Services");

Data Subjects

The Personal Data Processed concerns the following categories of Data Subjects:
Data Subjects include:

- Users accessing our E-Mobility cloud solutions
- E-Drivers using your charging stations

Categories of data

The Personal Data Processed concerns the following categories of personal data:

- Contact information, including full name, company, telephone number and e-mail address, mail address
- E-Driver's RFID number
- Charging station status, including charging logs, boot notifications, serial number, MAC address.
- Charge Data Record including charging transaction details such as RFID-card, location, kWh consumption, start date, end date
- Further Personal Data that is stored by You or Your users in the Cloud Services

Special Categories of Personal Data (if appropriate)

The Services are not intended for the processing of Special Categories of Personal Data and you and your Further Controllers shall not transfer, directly or indirectly, any such sensitive personal data to us.

Entities engaged in the storage of Your Content:

Entity Name	Country/Territory where Processing is Performed	Registered Address	Transfer to Non-EEA Recipients: Transfer Safeguards
Amazon Web Services, Inc. (AWS)	European Union	**2021 7th Avenue; Seattle, Washington 98121, USA**	Not applicable, no Transfers to Non-EEA Recipients
Microsoft Corporation	European Union	**One Microsoft Way Redmond WA, USA 98052**	Not applicable, no Transfers to Non-EEA Recipients

Entities engaged in the processing of Your Content for non-storage purposes:

Entity Name	Country/Territory where Processing is Performed	Registered Address	Transfer to Non-EEA Recipients: Transfer Safeguards
Digital Charging Solutions GmbH	Germany	**Brunnenstraße 19 – 21, 10110 Berlin, Germany**	Not applicable, no Transfers to Non-EEA Recipients
EVA Solution Group Oy	Finland	**Åkerlundinkatu 8, 33100 Tampere, Finland**	Not applicable, no Transfers to Non-EEA Recipients
Microsoft Corporation and its Subprocessors	List of Subprocessors and processing locations are indicated in the Microsoft at: https://www.microsoft.com/en-us/trust-center/privacy/data-access	**One Microsoft Way Redmond WA, USA 98052**	EU Model Contract
Siemens Aktiengesellschaft	Germany	**Werner-von-Siemens-Str. 1, 80333 Munich, Germany**	Not applicable, no Transfers to Non-EEA Recipients
Siemens Technology and Services PL	India	**84, Hosur Rd, Keonics, Electronic City, Bengaluru, Karnataka 560100; India**	EU Model Contract

Find a list of further entities engaged in the Processing of Your Content in the context of Digital Solutions for Depots offerings at: http://sie.ag/MindSphere_ListOfSubprocessors

SIEMENS

DPT Security Exhibit -

Technical and organisational measures

This document describes the technical and organizational measures ("TOMs") implemented by us. Some Services may be protected by different or additional technical and organizational security measures, as set forth in the respective Agreement. In all other cases, the following TOMs implemented by us and/or our Subprocessors shall apply. It is Customers own responsibility to implement measures in addition to the TOMs described below that fall in its own sphere of responsibility, such as implementing physical and system access control measures for your own premises and assets or configuring the Services to its individual requirements.

Scenario 1: The Services provided include Cloud Services hosted by us.

Scenario 2: The Services provided include Support Services via remote access tools provided and controlled by us.

Scenario 3: The Services provided include Support Services via remote access tools provided and controlled by you.

#	Measures	Scenario		
		1	2	3
1.	Physical and Environmental Security			
	We implement suitable measures to prevent unauthorized persons from gaining access to the data processing equipment (namely database and application servers and related hardware). This shall be accomplished by:			
	a) establishing security areas;	X	X	-
	b) protecting and restricting access paths;	X	X	-
	c) securing the decentralized data processing equipment and personal computers;	X	X	X
	d) establishing access authorizations for employees and third parties, including the respective documentation;	X	X	-
	e) all access to the data center where Personal Data is hosted will be logged, monitored, and tracked;	X	-	-
	f) the data center where Personal Data is hosted is secured by restricted access controls, and other appropriate security measures; and	X	-	-
	g) maintenance and inspection of supporting equipment in IT areas and data centers shall only be carried out by authorized personnel	X	X	-
2.	Access Control (IT-Systems and/or IT-Application)			
	2.1 We implement an authorization and authentication framework including, but not limited to, the following elements:			
	a) role-based access controls implemented;	X	X	X
	b) process to create, modify, and delete accounts implemented;	X	X	X[i]
	c) access to IT systems and applications is protected by authentication mechanisms;	X	X	X
	d) appropriate authentication methods are used based on the characteristics and technical options of the IT system or application;	X	X	X
	e) access to IT systems and applications shall require adequate authentication;	X	X	X
	f) all access to data (including personal data) is logged;	X	X	-
	g) authorization and logging measures for inbound and outbound network connections to IT systems and applications (including firewalls to allow or deny inbound network connections) implemented;	X	X	-
	h) privileged access rights to IT systems, applications, and network services are only granted to individuals who need it to accomplish their tasks (least-privilege principle);	X	X	X

SIEMENS

#	Measures	Scenario		
		1	2	3
	i) privileged access rights to IT systems and applications are documented and kept up to date;	X	X	X
	j) access rights to IT systems and applications are reviewed and updated on regular basis;	X	X	X
	k) password policy implemented, including requirements re. password complexity, minimum length and expiry after adequate period of time, no re-use of recently used passwords;	X	X	X
	l) IT systems and applications technically enforce password policy;	X	X	X
	m) access rights of employees and external personnel to IT systems and applications is removed immediately upon termination of employment or contract; and	X	X	X
	n) use of secure state-of-the-art authentication certificates.	X	X	-
	2.2 We implement a roles and responsibilities concept.	X	X	-
	2.3 IT systems and applications lock down automatically or terminate the session after exceeding a reasonable defined idle time limit.	X	X	-
	2.4 We maintain log-on procedures on IT systems with safeguards against suspicious login activity (e.g. against brute-force and password guessing attacks).	X	X	X[ii]
3.	Availability Control			
	3.1 We define, document and implement a backup concept for IT systems, including the following technical and organizational elements:			
	a) backups storage media is protected against unauthorized access and environmental threats (e.g., heat, humidity, fire);	X	-	-
	b) defined backup intervals; and	X	-	-
	c) the restoration of data from backups is tested regularly based on the criticality of the IT system or application.	X	-	-
	3.2 We store backups in a physical location different from the location where the productive system is hosted.	X	-	-
	3.3 We protect systems and applications against malicious software by implementing appropriate and state-of-the-art anti-malware solutions.	X	X	X
	3.4 IT systems and applications in non-production environments are logically or physically separated from IT systems and applications in production environments.	X	-	-
	3.5 Data centers in which Personal Data is stored or processed are protected against natural disasters, physical attacks or accidents.	X	-	-
	3.6 Supporting equipment in IT areas and data centers, such as cables, electricity, telecommunication facilities, water supply, or air conditioning systems are protected from disruptions and unauthorized manipulation.	X	-	-
4.	Operations Security			
	4.1 We maintain and implement an Information Security Framework reflecting the measures described herein which is regularly reviewed and updated.	X	X	X
	4.2 We log security-relevant events, such as user management activities (e.g., creation, deletion), failed logons, changes on the security configuration of the system on IT systems and applications.	X	X	X
	4.3 We continuously analyze the respective IT systems and applications log data for anomalies, irregularities, indicators of compromise and other suspicious activities.	X	X	X
	4.4 We scan and test IT systems and applications for security vulnerabilities on a regular basis.	X	X	X
	4.5 We implement and maintain a change management process for IT systems and applications.	X	X	X
	4.6 We maintain a process to update and implement vendor security fixes and updates on the respective IT systems and applications.	X	X	X
	4.7 We irretrievably erase data or physically destroy the data storage media before disposing or reusing of an IT system.	X	X	X
5.	Transmission Controls			
	5.1 We continuously and systematically monitor IT systems, applications and relevant network zones to detect malicious and abnormal network activity by;			

SIEMENS

#	Measures	Scenario		
		1	2	3
	a) Firewalls (e.g., stateful firewalls, application firewalls);	X	X	-
	b) Proxy servers;	X	X	-
	c) Intrusion Detection Systems (IDS) and/or Intrusion Prevention Systems (IPS);	X	X	-
	d) URL Filtering; and	X	-	-
	e) Security Information and Event Management (SIEM) systems.	X	X	-
	5.2 We document and updates network topologies and its security requirements on regular basis.	X	X	-
	5.3 We administer IT systems and applications by using state-of-the-art encrypted connections.	X	X	-
	5.4 We protect the integrity of content during transmission by state-of-the-art network protocols, such as TLS.	X	X	-
	5.5 We encrypt, or enable our customers to encrypt, customer data that is transmitted over public networks.	X	X	-
	5.6 We use secure Key Management Systems (KMS) to store secret keys in the cloud.	X	-	-
6.	Security Incidents			
	We maintain and implement an incident handling process, including but not limited to			
	a) records of security breaches;	X	X	X
	b) customer notification processes; and	X	X	X
	c) an incident response scheme to address the following at time of incident:(i) roles, responsibilities, and communication and contact strategies in the event of a compromise (ii) specific incident response procedures and (iii) coverage and responses of all critical system components.	X	X	X
7.	Asset Management, System Acquisition, Development and Maintenance			
	7.1 We implement an adequate security patching process that includes:			
	a) monitoring of components for potential weaknesses (CVEs);	X	X	-
	b) priority rating of fix;	X	X	-
	c) timely implementation of the fix; and	X	X	-
	d) download of patches from trustworthy sources.	X	X	-
	7.2 We identify and document information security requirements prior to the development and acquisition of new IT systems and applications as well as before making improvements to existing IT systems and applications.	X	X	-
	7.3 We establish a formal process to control and perform changes to developed applications.	X	X	-
	7.4 We plan and incorporate security tests into the System Development Life Cycle of IT systems and applications.	X	X	-
8.	Human Resource Security			
	8.1 We implement the following measures in the area of human resources security:			
	a) employees with access to Personal Data are bound by confidentiality obligations;	X	X	X
	b) employees with access to Personal Data are trained regularly regarding the applicable data protection laws and regulations	X	X	X
	8.2 We implement an offboarding process for our employees and external vendors.	X	X	X