SIEMENS

Data Privacy Terms for Data Services

Mobility Customer Services, October 2019

1. Purpose, scope and term

1.1. These Data Privacy Terms ("**DPT**") apply to all Services that involve the Processing of Personal Data by Siemens acting as Processor or Subprocessor. The DPT describe the parties´ data protection related rights and obligations with respect to these Services. All other rights and obligations shall be exclusively governed by the respective Contract.

1.2. The DPT shall have the same term as the respective Contract.

2. Details of the provided processing activities

2.1. The details of the Processing services provided by Siemens, including the scope, duration, nature and purpose of the Processing, the types of Personal Data processed and the categories of affected data subjects, are specified in Attachment 1 to these DPT.

2.2. Siemens will Process Personal Data in accordance with the terms of the Contract (including these DPT) or as otherwise permitted by the Customer.

2.3. Siemens shall be entitled to disclose or to entitle its Subprocessors to disclose Personal Data to comply with applicable laws and/or governmental orders. In case of such a request, unless legally prohibited from doing so, Siemens or the Subprocessor will attempt to redirect the governmental agency or regulatory body to the Customer and provide the Customer with reasonable notice of such disclosure request.

3. Instruction rights

3.1. As Processor, Siemens will only act upon the Customer's documented instructions. These DPT and the Contract constitute the Customer's complete and final instructions for the Processing of Personal Data by Siemens.

3.2. Any additional or alternate instructions must be agreed between the Customer and Siemens in writing and may be subject to additional costs.

3.3. Siemens shall inform the Customer if, in the opinion of Siemens, an instruction infringes Applicable Data Protection Law. Siemens shall, however, not be obligated to perform any legal examination of the Customer's instructions.

4. Technical and organizational measures

Siemens will implement the technical and organizational measures described in Attachment 2 to these DPT in order to protect the Personal Data. The Customer hereby confirms that the level of security provided is appropriate to the risk inherent with the Processing by Siemens on the Customer's behalf. The Customer understands and agrees that the technical and organizational measures are subject to technical progress and development. In that regard, Siemens shall have the right to implement adequate alternative measures as long as the security level of the measures is maintained.

5. Confidentiality of the Processing

Siemens will ensure that personnel who are involved with the Processing of Personal Data under the DPT have committed themselves to confidentiality.

6. Subprocessors

6.1. The Customer hereby allows Siemens to employ Subprocessors. A current list of Subprocessors commissioned by Siemens is contained in Attachment 1 to these DPT. The Customer hereby agrees to the employment of these Subprocessors.

6.2. Siemens may remove or add new Subprocessors at any time. Siemens will obtain Customer's approval to engage new Subprocessors in accordance with the following process: (i) Siemens shall publish new Subprocessors on the Railigent Platform Website or otherwise notify the Customer at least twenty (20) days before authorizing any new Subprocessor to access the Customer's Personal Data; new Subprocessors shall be published on the 15th of each calendar month; (ii) if the Customer raises no reasonable objections to Siemens in writing within this twenty (20) day period, then this shall be taken as an approval of the new Subprocessor by the Customer; and (iii) in the event the Customer objects to a new Subprocessor, Siemens shall have the right to terminate the affected Services with ten (10) days' notice. Instead of terminating the Service, Siemens shall have the right to (a) continue the Service without the engagement of the Subprocessor which the Customer objected to, (b) take sufficient steps to address the concerns raised in the Customer's objection, or (c) in agreement with the Customer, cease to provide (temporarily or permanently), the particular aspect of the Service that would involve use of the Subprocessor. The Customer´s approval must not be unreasonably withheld.

6.3. Siemens shall be entitled to perform Emergency Replacements of Subprocessors. In such a case, Siemens shall inform the Customer of the Emergency Replacements without undue delay and the approval process as described in Section 6.2 shall apply after the Customer´s receipt of the notification.

6.4. In case of any commissioning of Subprocessors, Siemens shall enter into an agreement with such Subprocessor imposing appropriate contractual obligations on the Subprocessor that are no less protective than the obligations in these DPT.

7. Transfers to Non-EEA Recipients

7.1. In case Transfers to Non-EEA Recipients relate to Personal Data originating from a Controller located within the EEA or Switzerland, Siemens shall implement the Transfer Safeguards identified per Subprocessor in the list of Subprocessors available on the Railigent Platform Website or (where applicable) otherwise notified to the Customer. It is the Customer's responsibility to assess whether the respective Transfer Safeguards implemented suffice for the Customer to comply with Applicable Data Protection Law.

7.2. The following shall apply if a Transfer Safeguard is based on the EU Model Contract: Siemens enters into such EU Model Contract with the relevant Subprocessor. Such EU Model Contract shall contain the right for the Customer to accede to the EU Model Contract. The Customer hereby accedes to the EU Model Contracts as a data exporter with current Subprocessors and agrees that the Customer's approval of future Subprocessors in accordance with Section 6.2 shall be deemed as declaration of accession to the EU Model Contract with the relevant future Subprocessor. Besides the Customer will ensure that also any further recipients of the Services will accede to the EU Model Contract as data exporters. The respective accession is hereby approved. Any applicable requirement for receipt of the accession statement by Siemens or the respective Suprocessors is hereby waived.

7.3. The following shall apply if a Transfer Safeguard is based on the Privacy Shield or Binding Corporate Rules for Processors in the sense of art. 47 GDPR: Siemens shall contractually bind a Privacy Shield-certified Subprocessor to comply with the Privacy Shield principles or the Binding Corporate Rules, as the case may be, with regard to the Personal Data processed under these DPT.

8. Rectification and erasure

8.1. Siemens shall, at its discretion, either (i) provide the Customer with the ability to rectify or delete Personal Data via the functionalities of the Services, or (ii) rectify or delete Personal Data as instructed by the Customer.

8.2. After termination of the DPT and unless otherwise agreed between the parties, Siemens will delete, destroy or anonymize any Customer's Personal Data processed by Siemens as Processor in accordance with the provisions of the Contract, unless Siemens is required to retain such data in accordance with Laws.

SIEMENS

9. Personal Data Breach

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

10. Further notifications and support

10.1. Siemens shall notify the Customer without undue delay of (i) complaints or requests of data subjects whose Personal Data are processed pursuant to these DPT (e.g. regarding the rectification, erasure and restrictions of Processing of Personal Data) or (ii) orders or requests by a competent data protection authority or court which relate to the Processing of Personal Data under these DPT.

10.2. At the Customer's request, Siemens shall reasonably support the Customer in (i) dealing with complaints, requests or orders described in Section 10.1 above (especially in fulfilling the Customer's obligation to respond to requests for exercising the data subject's rights) or (ii) fulfilling any of the Customer's further obligations as Controller under Applicable Data Protection Law (such as the obligation to conduct a data protection impact assessment). Such support shall be compensated by the Customer on a time and material basis.

11. Audits

11.1. The Customer shall have the right to audit, by appropriate means - in accordance with Sections 11.2 and 11.3 below - Siemens and its Subprocessors' compliance with the data protection obligations hereunder annually (in particular with respect to the implemented technical and organizational measures), unless additional audits are necessary under Applicable Data Protection Law; such audit being limited to information and data Processing systems that are relevant for the provision of the Services provided to Company.

11.2. Siemens and its Subprocessors may use (internal or external) auditors to perform audits to verify compliance with the data protection obligations hereunder, especially the requirement to implement technical and organizational measures. Each audit will result in the generation of an audit report (e.g. as Service Organization Controls 1, Type 2 reports and Service Organization Controls 2, Type 2 reports). Upon the Customer's request, Siemens shall provide such relevant Audit Reports and, if necessary, other information and documents (together "**Audit Reports**") to the Customer.

11.3. In case the Customer can demonstrate that the Audit Reports provided are not reasonably sufficient to allow the Customer to comply with applicable audit requirements and obligations under Applicable Data Protection Law, the Customer shall specify the further information, documentation or support required. Siemens shall render such information, documentation or support within a reasonable period of time at the Customer's expense.

11.4. The Audit Reports and any further information and documentation provided during an audit shall constitute Confidential Information of Siemens. In case audits relate to Siemens' Subprocessors, Siemens may require the Customer to enter into non-disclosure agreements directly with the respective Subprocessor before issuing Audit Reports and any further information or documentation.

12. Data privacy contact person

12.1 The Customer informs Siemens, prior to or promptly after the signature of the Contract, of the name and the contact details of a contact person in the Customer´s organization for data privacy matters. The Customer will notify Siemens without delay in writing (including per e-mail) of any changes in respect of such contact person.

12.2 All notifications and communication from Siemens to the Customer in connection with these DPT may be directed to such contact person, unless expressly agreed otherwise. Any such notifications or communication must be in writing (including per e-mail).

Definitions

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

2. **„Contract"** means the agreement or the agreements between the Customer and Siemens on services involving the processing of Personal Data by Siemens for the Customer. Where the parties have entered into more than one agreement in the sense of this definition, the term „Contract" may refer to one or all of these agreements, as the case may be.

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

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

5. **„Customer"** means the other party to the Contract.

6. **„DPT"** means these Data Services Privacy Terms.

7. **„EEA"** means the European Economic Area.

8. **„Emergency Replacement"** refers to a short-term replacement of a Subprocessor which is necessary (i) due to an event outside of Siemens' reasonable control and (ii) in order to provide the Services without interruptions (such as if the Subprocessor unexpectedly ceases business, abruptly discontinues providing Services to Siemens, or breaches its contractual duties owed to Siemens).

9. **„EU Model Contract"** 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.

10. **„Personal Data"** means information that relates, directly or indirectly, to a data subject. Personal Data, for the purpose of these DPT, includes only such data entered by the Customer into or derived from the use of the Services.

11. **„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 these DPT.

12. **„Privacy Shield"** means - with regard to Controllers located within the EEA - the European Union / United States Privacy Shield arrangement and - with regard to Controllers located in Switzerland - the Switzerland / United States Privacy Shield arrangement.

13. **„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.

14. **„Processor"** means a legal person, which Processes Personal Data on behalf of a Controller.

15. **„Railigent Platform Website"** means the website referenced in the order Form or otherwise notified by Siemens to the Customer.

16. **„Services"** means the services performed under the Contract involving the Processing of Personal Data by Siemens acting as Processor or Subprocessor for the Customer as Controller.

17. **„Siemens"** means the Siemens entity being party to the Contract.

18. **„Subprocessor"** means any further Processor engaged by Siemens in the performance of the Services provided under these DPT that has access to Personal Data.

19. **„Transfers to Non-EEA Recipients"** means (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 Siemens or any of its Subprocessors.

20. **„Transfer Safeguards"** means (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.

21. Capitalized terms which are not defined in these DPT shall have the meaning given to them in the Contract.

SIEMENS

ATTACHMENT 2 TO THE DPT (DESCRIPTION OF DATA PROCESSING ACTIVITIES)

Processing operation

Siemens and its Subprocessors Process Personal Data for the following purposes:

- to provide the Services
- to provide storage and backup of Personal Data in data centers in connection with providing the Services (multi-tenant architecture).

Data Subjects

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

- Employees of the Customer and any further recipients of the Services
- Other natural persons whose Personal Data are Processed in connection with performing the Services

Categories of Personal Data

The Personal Data Processed fall in the following categories of Personal Data:

- Business-related contact data (e.g. address, telephone number and e-mail address)
- Device codes (e.g. IP addresses)
- System- and machine-logfiles
- In respect of video surveillance products (e.g. closed-circuit television / CCTV) or products with picture recording: video- and audio-recordings
- Other categories of Personal Data Processed in connection with the performance of the Services

Processing of Personal Data

The Personal Data Processed are subject to the following general categories of Processing:

- Performance of the Services specified in the respective scope description of the respective Contract, e.g.:
- Hotline- and support-services
- Back-up services
- Digital services for visualization, analysis and prediction of technical data in the mobility sector, e.g. app- and platform-offerings
- Operation and maintenance of CCTV-solutions

Where the performance of the Services includes the Processing of further categories of data subjects or further categories of Personal Data, the relevant information are set out in the scope description of the respective Contract.

Subprocessors

Name	Address	Transfer to Non-EEA Recipients: Transfer Safeguards
Amazon Web Services Inc. („AWS“)	2021 7th Ave, Seattle, Washington 98121, USA	Hosting in the EEA, no Transfers to Non-EEA Recipients
Atos Information Technology GmbH	Otto-Hahn-Ring 6 81739 München, Germany	Hosting in the EEA, no Transfers to Non-EEA Recipients
CloudCheckr	1-833-CLDCHCK 342 N. Goodman St Rochester, NY 14607, USA	Hosting in the EEA, no Transfers to Non-EEA Recipients
Teradata GmbH	Dachauer Str. 63 80335 Munich, Germany	Hosting in the EEA, no Transfers to Non-EEA Recipients
TIBCO Software Inc.	3303 Hillview Avenue - Palo Alto - California – 94304, USA	Hosting in the EEA, no Transfers to Non-EEA Recipients
COMPAREX AG	Blochstraße 1 04329 Leipzig, Germany	Hosting in the EEA, no Transfers to Non-EEA Recipients
Siemens Mobility GmbH (where “Siemens” as defined herein is another Siemens entity than Siemens Mobility GmbH)	Otto-Hahn-Ring 6 81739 Munich, Germany	Hosting in the EEA, no Transfers to Non-EEA Recipients

SIEMENS

ATTACHMENT 2 TO THE DPT (TECHNICAL AND ORGANIZATIONAL MEASURES)

Description of the technical and organizational measures implemented in accordance with Section 4 of the DPT:

1. Physical Access Control

The following measures are implemented to protect premises, buildings or rooms where data processing systems processing Personal Data are located against unauthorized physical access:

a) Definition of security-relevant areas and physical barrier controls to prevent unauthorized entrance
b) Limitation and protection of physical access points
c) Protection of decentralized data processing facilities and personal computers
d) Assignment and documentation of access authorizations for employees and third parties
e) Legitimization requirements for authorized users

2. System Access Control

The following measures are implemented to protect systems used for providing digital services against unauthorized access or use:

a) Registration and de-registration of users according to a formal process allowing for allocation of access rights
b) Administration of secret authentication credentials of users
c) Regular checks of users´ access rights
d) Revocation or adjustment of access rights of external parties in case of termination or modification of the respective external business relationship with such parties
e) Obligatory use of secret authentication credentials
f) Checking and controlling access by means of an Access Control Policy
g) Definition of complementary security measures for access to or processing of Personal Data from a remote tele-workplace (*Telearbeitsplatz*) or a mobile end device
h) Information security guideline for dealing with suppliers which stipulates binding requirements in connection with access by suppliers to systems, data media or assets

3. Data Access Control

The following measures are implemented to ensure that authorized users of data processing systems gain access to the Personal Data only if they have a corresponding access right and that in the course of processing, using and storing Personal Data it is not read, copied, modified or removed without authorization:

a) Limitation and control of user access to networks and network services pursuant to an Access Control Policy
b) Assignment and revocation of user access to all systems and services according to a defined process
c) Limitation and control of privileged access rights
d) Segregation of environments for development, testing and operation in order to reduce the risk of unauthorized access or modification for the operation environment
e) Binding approval requirements or control procedures for removal of data media from the premises
f) Clearance checks of hardware and data media prior to disposal or re-use to verify that any sensitive data has clearly been removed
g) Agreements on information security requirements with suppliers which have access to Personal Data, may process it or provide IT-infrastructure components
h) Agreements with suppliers on requirements for dealing with information security risks related to the relevant supplier´s performance and the supply chain

4. Data Transmission Control

The following measures are implemented to procure that Personal Data is not read, copied, modified or removed without authorization during transmission or transfer:

a) Disposal of data media only after prior clearance check
b) Use of encryption methods in line with tried and tested, generally accepted practice
c) Administration of encryption keys throughout their lifetime
d) Transfer of Personal Data to external parties only with prior agreement on security requirements

5. Data Input Control

The following measures are implemented to follow up and verify ex post whether and by whom Personal Data have been entered, modified or removed from data processing systems used to provide digital services:

a) Electronic recording of the activities of users and system administrators, disturbances and information security incidents
b) Protection of the recorded information against unauthorized access and manipulation
c) Regular checks of the electronic records

6. Order Control

The following measures are implemented in order to ensure that Personal Data which is processed on the Customer´s behalf can only be processed in compliance with its instructions:

a) Definition of binding guidelines for work and organization processes for the processor´s employees in alignment (if applicable) with the Customer
b) Granting of opportunity for the Customer´s employees or agents in accordance with the DPT and upon request for auditing the processor´s compliance with the DPT

7. Availability Control

The following measures are implemented to protect Personal Data against accidental or unauthorized destruction or loss:

a) Monitoring of technical vulnerabilities
b) Protection against power breakdowns by means of redundant power supply systems and emergency power supply
c) Regular forecasts of the anticipated system performance required and future capacity requirements
d) Detection, precaution and rectification measures protecting against malware
e) Technical checks and tests in case of modifications of operation platforms with respect to potential negative effects on operations or security
f) Definition of an emergency or contingency plan

8. Data Separation Control

The following measures are implemented to control that Personal Data collected for different purposes can be processed separately:

a) Information services, user and information systems are segregated in different groups