



AUTRONICA

ANNEXES FOR SUBSCRIPTION SERVICES

Autronica Fire and Security

Valid from 22 December 2020

ANNEX IV - Data Processing and Transfer Agreement

This DPTA shall apply to the use of Portal, Software and Support Services provided by Autronica Contract (the “Contract”), as of the Effective Date, entered into between the aforementioned parties and to which this DPTA is incorporated by reference. Autronica Fire and Security AS shall act as a Data Processor and the Customer as a Data Controller.

Except as expressly supplemented by this DPTA with respect to the subject matter hereunder, the terms of the Contract shall continue unchanged and shall apply with full force and effect as to the matters addressed therein.

1. DEFINITIONS

Capitalized terms in this DPTA shall have the meanings ascribed to such terms under clause 1.2 (or in other locations throughout this DPTA or the Contract), and, if not otherwise defined, shall have their ordinary and customary meanings.

The following definitions are applicable to this DPTA:

- “Data Privacy Laws”** means applicable national, federal, state and provincial laws relating to data privacy, the protection of Personal Information or data, and the cross-border transfer of Personal Information or data, including, without limitation, the General Data Protection Regulation (“GDPR”) and any European Union law or regulation that may be enacted to implement or replace GDPR.
- “Data Subject”** means an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- “Incident”** means any actual or reasonably suspected incident of accidental or unlawful destruction or accidental loss, alteration, unauthorized or accidental disclosure of or access to the Personal Information.
- “Personal Information”** means any information or data provided to Autronica or subcontractors, by the Data Controller or its agents, subcontractors or customers, in connection with the Contract that relate to any identified or identifiable natural person, or, to the extent of a conflict with applicable law, that is subject to any Data Privacy Laws.

2. SUBJECT MATTER OF THIS DPTA

This DPTA applies exclusively to the hosting and managing activities provided by the Data Processor to the Data Controller to store Personal Information related to the Portal and related Services as described in the Contract.

An overview of the categories of Personal Information, the types of Data Subjects and purposes for which the Personal Information are being processed is provided in Appendix 1 to this DPTA.

3. DURATION AND TERMINATION

This DPTA shall come into effect on the Effective Date and shall remain valid as long as the Contract is not terminated or does not expire.

Termination or expiration of this DPTA shall not discharge the Data Processor from its confidentiality obligations pursuant to article 6 of the Appendix II to the Contract.

The Data Processor shall process Personal Information until the date of termination or expiration of the Contract, unless instructed otherwise by the Data Controller, or until such data is returned or destroyed on instruction of the Data Controller, pursuant to clause 12 of this DPTA. Data Controller's instructions, to the extent that they seek additional Services or expenditure by Data Processor, are subject to additional fees to be negotiated in good faith by the parties.

4. DATA CONTROLLER AND DATA PROCESSOR OBLIGATIONS

Both parties shall comply with all applicable Data Privacy Laws and promptly notify each other in writing if one believes that collecting or processing Personal Information pursuant to this DPTA or the Contract infringes Data Privacy Laws;

The Data Processor will only process the Personal Information on documented instructions of the Data Controller, or as set forth in the Contract or this DPTA, in such manner as - and to the extent that - this is appropriate for the provision of the Services described in the Contract, except as required to comply with a legal obligation to which the Data Processor is subject.

The parties have entered into the Contract in order to benefit from the expertise of the Data Processor in securing and processing the Personal Information for the purposes set out in Appendix 2. The Data Processor shall be allowed to exercise its own discretion in the selection and use of such means as it considers necessary to pursue those purposes, subject to the requirements of this DPTA.

5. DATA CONTROLLER OBLIGATIONS

The Data Controller shall:

- a) warrant that it has all necessary rights to provide the Personal Information to the Data Processor for the Processing to be performed in relation to the use of the Portal, Software and related Services. To the extent required by Data Privacy Laws, Data Controller is responsible for ensuring that it provides such Personal Information to Autronica based on an appropriate legal basis allowing lawful processing activities, including any necessary Data Subject consents to this Processing are obtained, and for ensuring that a record of such consents is maintained. Should such a consent be revoked by the Data Subject, the Data Controller is responsible for communicating the fact of such revocation to the Data Processor;
- b) provide any and all natural persons from whom it collects Personal Information with the relevant privacy notice, based on the Autronica Privacy Notice displayed in the Portal;
- a) request the Data Processor to purge Personal Information when required by the Data Controller or any Data Subject whom it collects Personal Information, unless the Data Processor is otherwise required to retain the Personal Information by applicable law; and

- c) immediately advise the Data Processor in writing if it receives or learns of any: (i) complaint or allegation indicating a violation of Data Privacy Laws regarding Personal Information; (ii) request from one or more individuals seeking to access, correct, or delete Personal Information; (iii) inquiry or complaint from one or more individuals relating to the collection, processing, use, or transfer of Personal Information; and (iv) any regulatory request for, subpoena, search warrant, or other legal, regulatory, administrative, or governmental process seeking Personal Information (collectively, "Data Privacy Matters").

6. DATA PROCESSOR OBLIGATIONS

The Data Processor shall:

- a) only process Personal Information, or transfer Personal Information to authorized third parties, in performance of its obligations under the Contract, in accordance with the Data Controller's instructions or as set forth in this DPTA, or to comply with legal obligations.;
- b) not share, transfer, disclose or provide access to Personal Information for any third party except to provide access to the Portal and to provide the Services covered by the Contract or as required by law. This provision does not preclude Data Processor from using subcontractors to provide the Services, so long as if the Data Processor does share, transfer, disclose or provide access to Personal Information to a third party, it shall do so in accordance with the provisions of clause 8 of this DPTA; and
- c) take commercially reasonable steps to ensure the reliability of its employees, agents, representatives, subcontractors, subcontractor employees, or any other person used by it (collectively, "Data Processor Personnel") who have access to the Personal Information, ensure that such access is on a need-to-know basis, and ensure that Data Processor Personnel are obligated to maintain the confidentiality of Personal Information, such as through a confidentiality agreement or by application of relevant law or regulation.

7. DATA CONTROLLER ASSISTANCE

The Data Processor shall:

- a) provide such information, assistance and cooperation as the Data Controller may reasonably require from time to time to demonstrate Data Processor's compliance with Data Privacy Laws;
- b) assist the Data Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Data Controller's obligation to respond to requests for exercising the Data Subject's rights under the Data Privacy Laws;
- c) assist the Data Controller in ensuring compliance with and demonstrate the measures it has taken to comply with the obligations pursuant to clause 10 (Security Measures), data protection impact assessment and prior consultations with supervisory authorities required under Article 36 of the GDPR taking into account the nature of processing and the information available to the Data Processor; and
- d) in case it learns of any complaint, request, allegation, or inquiry, shall provide assistance to the Data Controller, fully cooperate with it in investigating the matter, including but not limited to, providing the relevant information to it, preparing a response, implementing a remedy, and/or cooperating in the conduct of and defending against any claim, court or regulatory proceedings. The Data Controller shall be responsible for communicating with individuals regarding their Personal Information in connection with such Data Privacy Matters unless the Data Controller authorizes the Data Processor to do so on its behalf. The Data Processor shall use commercially and legally reasonable efforts to limit the nature and scope of the required disclosure to the minimum amount of Personal Information required

to comply with applicable law. Unless prevented by applicable law, the Data Processor shall provide the Data Controller with advance written notice of any such Data Privacy Matters sufficient to allow the Data Controller to contest legal, regulatory, administrative, or other governmental processes.

If any of the required assistance involves a time and expenditure beyond that required to provide the Services, Data Processor and Data Controller will negotiate in good faith reasonable compensation for Data Processor's time and expenditure. If the parties cannot agree, they shall use the dispute resolution provisions contained in the Contract.

8. CONTRACTING WITH SUB-PROCESSORS

The Data Processor shall not subcontract any of the Services or any other Processing of Personal Information to any third party without two weeks' prior written notice to the Data Controller. During this time, the Data Controller shall be entitled to object, but only in good faith and upon justification. The Data Processor shall then have 60 days to select an alternative subcontractor. The Data Processor may switch without providing advance notice in the case of an emergency, but in such circumstance will provide notice promptly and allow for a two weeks' period for Data Controller to object.

Notwithstanding the foregoing, the Data Controller agrees and acknowledges that the Data Processor subcontracts the hosting services to a third party hosting provider, to the extent appropriate agreement is concluded with said subcontractor, which might include the EU Standard Contractual Clauses or any other contractual arrangements, ascribed in clause 13.

The Data Processor shall ensure that the sub-processor is bound by the same data protection obligations of the Data Processor under this DPTA, shall supervise compliance thereof, and must in particular impose on its sub-processors the obligation to implement appropriate technical and organizational measures in such a manner that the processing will meet the requirements of the relevant Data Privacy Laws.

In any case, the Data Processor shall remain fully liable for the performance of any such subprocessor that fails to fulfil its obligations under this DPTA as pertaining to the Services.

9. AUDIT

Upon Data Controller's request and subject to at least 30 days' prior notice given to the Data Processor, the Data Processor shall provide the Data Controller with a detailed audit report carried out by the Data Processor or a third party, selected by the Data Processor, in order to demonstrate compliance with the provisions of this Contract and this DPTA.

In case of serious doubts regarding the accuracy of such audit report, the Data Controller shall be entitled to carry out, or have carried out by a third party who has entered into a confidentiality agreement with the Data Processor, at its own expenses, audits of the Data Processor's policies, processes and documentation, as these relate to the Personal Information to verify Data Processor compliance with its obligations under the Contract and this DPTA. The Data Processor shall cooperate with such audits.

10. SECURITY MEASURES

Taking into account the state of the art, the type of Personal Information, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of the Data Subjects, without prejudice to any other security standards agreed upon by the parties, the Data Processor shall implement appropriate technical and organisational measures to ensure a level of security of the processing of Personal Information appropriate to the risk. These measures are further described in Appendix 2.

The parties acknowledge that security requirements are constantly changing and that effective security requires frequent evaluation and regular improvements of outdated security measures. The Data

Processor will therefore evaluate the measures as implemented in accordance with this clause 10 on an on-going basis and will modify these measures in order to maintain compliance with the requirements set out in this clause. The parties will negotiate in good faith the costs, if any, to implement material changes required by specific updated security requirements set forth in applicable data protection law or by data protection authorities of competent jurisdiction.

11. INFORMATION OBLIGATIONS AND INCIDENT MANAGEMENT

When the Data Processor becomes aware of an Incident that impacts the Processing of the Personal Information that is the subject of this DPTA and the Contract, it shall promptly and, whenever possible, within 48 hours, notify the Data Controller about the Incident, shall cooperate with the Data Controller and shall follow the Data Controller's instructions with regard to such Incidents, except where prohibited by law or where the Incident involves the data of multiple data controllers. If the Incident involves the Personal Information of multiple data controllers, Data Processor shall take reasonable measures to investigate, inform the data controllers, and remediate the issue. When the Data Processor is not able to provide the notice within 48 hours, it shall provide the Data Controller with an explanation for the delay that it will be allowed to share with regulators.

The Data Processor shall at all times have in place written incident response procedures.

Any notifications made to the Data Controller pursuant to this clause 11.2 shall be addressed to the employee of the Data Controller whose contact details are provided in clause 14.4 of this DPTA, and shall contain:

- a) a description of the nature of the Incident, including where possible the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Information records concerned;
- b) the name and contact details of the Data Processor's data protection officer or another contact point where more information can be obtained;
- c) a description of the likely consequences of the Incident; and
- d) a description of the measures taken or proposed to be taken by the Data Processor to address the Incident including, where appropriate, measures to mitigate its possible adverse effects.

12. RETURNING OR DESTRUCTION OF PERSONAL INFORMATION

Upon termination of this DPTA or upon the Data Controller's written request, the Data Processor shall, at the discretion of the Data Controller, either delete, destroy or return all Personal Information to the Data Controller and destroy or return any existing copies, except (i) such Personal Information is required by the Data Processor to discharge its obligations under this DPTA and/or the Contract or under applicable law; or (ii) return or destruction is prohibited by applicable law.

The Data Processor shall notify all third parties supporting its own processing of the Personal Information of the termination of the DPTA and shall ensure that all such third parties shall either destroy or return the Personal Information.

13. TRANSFER OF PERSONAL INFORMATION

The Data Processor shall be entitled to transfer, or permit the transfer of, Personal Information to a recipient located outside of the European Economic Area or Switzerland, subject to the provisions of clause 13.2 below. For the avoidance of doubt, the foregoing applies mutatis mutandis to accessing, and permitting the access to, Personal Information which is stored within the European Economic Area or Switzerland by a person located outside this area.

Before the transfer or access starts, the Data Processor will complete and sign adequate contractual arrangements for the transfer of Personal Information to processors established in third countries that do not offer adequate level of protection with regards to the rights and freedoms of the individuals.

Notwithstanding the foregoing, the Data Processor shall exchange such Personal Information with any of its Affiliated Companies, in accordance with the Autronica Binding Corporate Rules, as incorporated within Carrier Global Corporation group and available at <https://www.corporate.carrier.com/legal/privacy-notice/>.

14. MISCELLANEOUS

In the event of any inconsistency between the provisions of this DPTA and the provisions of the Contract, the provisions of this DPTA shall prevail.

This DPTA is governed by the laws of The Netherlands. Any disputes arising from or in connection with this DPTA shall be brought exclusively before the competent court of Amsterdam.

If the Data Privacy Laws shall be amended, both parties shall work together to make any required amendments to this DPTA. The Data Controller shall procure each Third Party to make those or comparable amendments.

Any notice provided under this DPTA must be sent to CarrierHQ_Compliance@carrier.com

APPENDIX 1. OVERVIEW OF THE PROCESSING ACTIVITIES

1. DATA SUBJECTS

Data Controller's employees or contractors and End-Users.

2. CATEGORIES OF DATA

The following Personal Information might be processed by the Data Processor, depending on which Personal Information the Data Controller shall enter into the Portal:

- With regards to Data Controller's employees or contractors:
 - Login details
 - First and Last Name
 - Email address
 - Role/function
- With regards to End-Users:
 - Site Name
 - Home address
 - Phone number

3. PROCESSING OPERATIONS

The Personal Information mentioned above will be subject to the following basic processing activities:

- Compute, Networking, Storage and Content Delivery;
- Technical Support to the Portal and related Products and Services, as described in the Contract.

APPENDIX 2. SECURITY MEASURES

1. DATA PROCESSOR'S RESPONSIBILITIES

The Data Processor shall maintain an information security program in collaboration with its subcontractor, where applicable, designed to:

- 1.1. Secure Personal Information of Data Subjects against accidental or unlawful loss, access or disclose;
- 1.2. Identify reasonably foreseeable and internal risks to security and unauthorized access to the network supporting the hosting of the Portal, Software or Remote Service;
- 1.3. Minimize security risks, including through risk assessment and regular testing;
- 1.4. Ensure appropriate level of protection with regards to the confidentiality, integrity and availability of the Personal Information.

2. PHYSICAL ACCESS CONTROLS AND SECURITY PROTECTIONS

- 2.1. Physical barrier controls are in place to prevent unauthorized entrance to the facilities where the Personal Information is hosted. The passage through these barriers requires either electronic access control validation or validation by human security personnel.
- 2.2. All access points of the facilities (other than the main entrance) are maintained in a secured (locked) state and monitored by video surveillance cameras. The facilities are covered by electronic intrusion detection systems, so that unauthorized access can be detected. Access of Data Processor Personnel is monitored and logged in security systems.
- 2.3. The Data Processor's subcontractor providing the hosting services is certified ISO 27001. The Data Processor shall evaluate, at least once a year, compliance of the subcontractor to this certification.

3. DATA PROCESSOR PERSONNEL'S ACCESS

- 3.1. The Data Processor shall provide access to the Personal Information only to those of its employees and contractors who have a legitimate business need for being granted such access. Such Data Processor Personnel have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.