DATA PROCESSING AGREEMENT (GLOBAL)

Last modified: September 2023

This Data Processing Agreement, including its Schedules and Annexes ("DPA") is entered into by between Avigilon Corporation, a wholly-owned subsidiary of Motorola Solutions, Inc., ("Motorola Solutions") on behalf of itself and its affiliates and subsidiaries ("Avigilon") and you (the "Customer") and reflects the parties' agreement with regard to the Processing of Customer Data which may include Personal Data pursuant to Customer's agreement with Avigilon (the"Agreement") and with an authorized reseller of Avigilon. In the event of a conflict between this DPA, the Agreement or any Schedule, Annex or other addenda to the Agreement, this DPA must prevail.

When Customer renews or purchases new equipment or software licenses ("Products") or related services ("Services"), the then-current DPA must apply and must not change during the applicable term of the Agreement ("Term"). When Avigilon provides new features or supplements to the Products or Services, Avigilon may provide additional terms or make updates to this DPA that must apply to Customer's use of those new features or supplements.

1. Definitions.

All capitalized terms not defined herein must have the meaning set forth in the Agreement. All lowercase terms not defined in this DPA must have the meaning as set within Article 4 of the GDPR if defined therein, regardless of whether GDPR applies.

"Avigilon Data" means data owned by Avigilon and made available to Customer in connection with the Products and Services.

"Customer Contact Data" means data Avigilon collects from Customer, its Authorized Users, and their end users for business contact purposes, including without limitation marketing, advertising, licensing, and sales purposes.

"**Customer Data**" means data including images, text, videos, and audio, that are provided to Avigilon by, through, or on behalf of Customer and its Authorized Users or their end users, through the use of the Products and Services. Customer Data does not include Customer Contact Data, Service Use Data other than that portion composed of Personal Information, or Third-Party Data.

"Data Protection Laws" means all data protection laws and regulations applicable to a Party with respect to the Processing of Personal Data under the Agreement.

"Data Subjects" means the identified or identifiable person to whom Personal Data relates.

"Metadata" means data that describes other data.

"Personal Data" or**"Personal Information"** means any information relating to an identified or identifiable natural person transmitted to Avigilon by, through, or on behalf of Customer and its Authorized Users or their end users as part of Customer Data. 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.

"Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller. Processors act on behalf of the relevant controller and under their authority. In doing so, they serve the controller's interests rather than their own.

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

"Security Incident" means an incident leading to the accidental or unlawful destruction, loss, alteration or disclosure of, or access to Customer Data, which may include Personal Data, while processed by Avigilon.

"**Service Use Data**" means data generated about the use of the Products and Services through Customer's use or Avigilon's support of the Products and Services, which may include Metadata, Personal Data, product performance and error information, activity logs, and date and time of use.

“Standard Contractual Clauses” means the clauses attached hereto as **Appendix 1** as established by the European Commission’s decision (C(2021) 3972 of 4 June 2021) on Standard Contractual Clauses for the transfer of personal data to processor established in third countries which do not ensure an adequate level of data protection.

“Sub-processor” means other processors engaged by Avigilon to Process Customer Data which may include Personal Data.

“Third-Party Data” means information obtained by Avigilon from publicly available sources or its Third-Party content providers and made available to Customer through the Products or Services.

2. Processing of Customer Data

- **2.1 Roles of the Parties**. The Parties agree that with regard to the Processing of Personal Data hereunder, Customer is the Controller and Avigilon is the Processor who may engage Sub-processors pursuant to the requirements of **Section 6** entitled “Sub-processors” below.
- **2.2 Avigilon’s Processing of Customer Data**. Avigilon and Customer agree that Avigilon may only use and Process Customer Data, including the Personal Information embedded in Service Use Data, in accordance with Customer’s documented instructions for the following purposes: (i) to perform Services and provide Products under the Agreement; (ii) analyze Customer Data to operate, maintain, manage, and improve Avigilon products and services; and (iii) create new products and services. Customer agrees that its Agreement (including this DPA), along with the Product and Service Documentation and Customer’s use and configuration of features in the Products and Services, are Customer’s complete and final documented instructions to Avigilon for the processing of Customer Data. Any additional or alternate instructions must be agreed to according to the process for amending Customer’s Agreement. Customer represents and warrants to Avigilon that Customer’s instructions, including appointment of Avigilon as a Processor or sub-processor, have been authorized by the relevant controller. Customer Data may be processed by Avigilon at any of its global locations and/or disclosed to Sub-processors. It is Customer’s responsibility to notify Authorized Users of Avigilon’s collection and use of Customer Data, and to obtain any required consents, provide all necessary notices, and meet any other applicable legal requirements with respect to such collection and use. Customer represents and warrants to Avigilon that it has complied with the terms of this provision.

For avoidance of doubt, so long as not specifically identifying the Customer, “Customer Data,” as defined in the Agreement, shall not include, and Avigilon shall be free to use, share and leverage security threat intelligence and mitigation data generally, including without limitation, Third-Party threat vectors and IP addresses, file hash information, domain names, malware signatures and information, information obtained from Third-Party sources, indicators of compromise, and tactics, techniques, and procedures used, learned or developed in the course of providing Services.

- **2.3 Details of Processing**. The subject-matter of Processing of Personal Data by Avigilon hereunder, the duration of the Processing, the categories of Data Subjects and types of Personal Data are set forth on **Annex I** to this DPA.
- **2.4 Disclosure of Processed Data**. Avigilon must not disclose to or share any Customer Data with any Third-Party except to Avigilon’s Sub-processors, suppliers and channel partners as necessary to provide the Products and Services unless permitted under this Agreement, authorized by Customer or required by law. In the event a government or supervisory authority demands access to Customer Data, to the extent allowable by law, Avigilon must provide Customer with notice of receipt of the demand to provide sufficient time for Customer to seek appropriate relief in the relevant jurisdiction. In all circumstances, Avigilon retains the right to comply with applicable law. Avigilon must ensure that its personnel are subject to a duty of confidentiality, and will contractually obligate its sub-processors to a duty of confidentiality, with respect to the handling of Customer Data and any Personal Data contained in Service Use Data.
- **2.5 Customer’s Obligations.** Customer is solely responsible for its compliance with all Data Protection Laws and establishing and maintaining its own policies and procedures to ensure such compliance. Customer must not use the Products and Services in a manner that would violate applicable Data Protection Laws. Customer must have sole responsibility for (a) the lawfulness of any transfer of Personal Data to Avigilon, (b) the accuracy, quality, and legality of Personal Data provided to Avigilon; (c) the means by which Customer acquired Personal Data, and (d) the provision of any required notices to, and obtaining any necessary acknowledgements, authorizations or consents from Data Subjects. Customer takes full responsibility to keep the amount of Personal Data provided to Avigilon to the minimum necessary for Avigilon to perform in accordance with the Agreement. Customer must be solely responsible for its compliance with applicable Data Protection Laws. Customer agrees that it has implemented administrative, physical and technical safeguards for Customer’s environment and operations that are no less rigorous than accepted industry practices and

shall ensure that all such safeguards comply with applicable data protection and privacy laws. Customer agrees that Avigilon shall not be liable for any Security Incident arising from Customer's breach of this requirement.

- **2.6 Customer Indemnity**. Customer will defend, indemnify, and hold Avigilon and its subcontractors, subsidiaries and other affiliates harmless from and against any and all damages, losses, liabilities, and expenses (including reasonable fees and expenses of attorneys) arising from any actual or threatened third-party claim, demand, action, or proceeding arising from or related to Customer's failure to comply with its obligations under this Agreement and/or applicable Data Protection Laws. Avigilon will give Customer prompt, written notice of any claim subject to the foregoing indemnity. Avigilon will, at its own expense, cooperate with Customer in its defense or settlement of the claim.

3. Service Use Data. Except to the extent that it is Personal Information, Customer understands and agrees that Avigilon may collect and use Service Use Data for its own purposes, provided that such purposes are compliant with applicable Data Protection Laws. Service Use Data may be processed by Avigilon at any of its global locations and/or disclosed to Sub-processors.

4. Third-Party Data and Avigilon Data. Avigilon Data and Third-Party Data may be available to Customer through the Products and Services. Customer and its Authorized Users may use the Avigilon Data and Third-Party Data as permitted by Avigilon and the applicable third-party data provider, as described in the Agreement. Unless expressly permitted in the Agreement, Customer must not, and must ensure its Authorized Users must not: (a) use the Avigilon Data or Third-Party Data for any purpose other than Customer's internal business purposes or disclose the data to third parties; (b) "white label" such data or otherwise misrepresent its source or ownership, or resell, distribute, sublicense, or commercially exploit the data in any manner; (c) use such data in violation of applicable laws ; (d) use such data for activities or purposes where reliance upon the data could lead to death, injury, or property damage; (e) remove, obscure, alter, or falsify any marks or proprietary rights notices indicating the source, origin, or ownership of the data; or (f) modify such data or combine it with Customer Data or other data or use the data to build databases. Additional restrictions may be set forth in the Agreement. Any rights granted to Customer or Authorized Users with respect to Avigilon Data or Third-Party Data must immediately terminate upon termination or expiration of the Agreement. Further, Avigilon or the applicable Third-Party Data provider may suspend, change, or terminate Customer's or any Authorized User's access to Avigilon Data or Third-Party Data if Avigilon or such Third-Party Data provider believes Customer's or the Authorized User's use of the data violates the Agreement, applicable law or by Avigilon's agreement with the applicable Third-Party Data provider. Upon termination

of Customer's rights to use of any Avigilon Data or Third-Party Data, Customer and all Authorized Users must immediately discontinue use of such data, delete all copies of such data, and certify such deletion to Avigilon. Notwithstanding any provision of the Agreement to the contrary, Avigilon has no liability for Third-Party Data or Avigilon Data available through the Products and Services. Avigilon and its Third-Party Data providers reserve all rights in and to Avigilon Data and Third-Party Data not expressly granted in the Agreement.

5. Avigilon as a Controller or Joint Controller. In all instances where Avigilon acts as a Controller it must comply with the applicable provisions of the Privacy Statement located at https://www.avigilon.com/about…, as may be updated from time to time. Avigilon holds all Customer Contact Data as a Controller and must Process such Customer Contact Data in accordance with the Avigilon Privacy Statement. In instances where Avigilon is acting as a Joint Controller with Customer, the Parties must enter into a separate addendum to the Agreement to allocate the respective roles as joint controllers.

6. Sub-processors.

- **6.1 Use of Sub-processors**. Customer agrees that Avigilon may engage Sub-processors who in turn may engage Sub-processors to Process Personal Data in accordance with the DPA. A current list of Sub-processors is set forth at **Annex III**. When engaging Sub-processors, Avigilon must enter into agreements with the Sub-processors to bind them to obligations which are substantially similar or more stringent than those set out in this DPA.
- **6.2 Changes to Sub-processing**. The Customer hereby consents to Avigilon engaging Sub-processors to process Customer Data provided that: (i) Avigilon must use its reasonable endeavors to provide at least 10 days' prior notice of the addition or removal of any Sub-processor, which may be given by posting details of such addition or removal at a URL provided to Customer in **Annex III** hereto; (ii) Avigilon imposes data protection terms on any Sub-processor it appoints that protect the Customer Data to the same standard provided for by this Agreement; and (iii) Avigilon remains fully liable for any breach of this clause that is caused by an act, error or omission of its Sub-processor(s). The Customer may object to Avigilon's appointment or replacement of a Sub-processor prior to its appointment or replacement, provided such objection is based on reasonable grounds relating to data protection. In such event, Avigilon will either appoint or replace the Sub-processor or, if in Avigilon's discretion this is not feasible, the Customer may terminate this Agreement and receive a pro-rata refund of any prepaid service or support fees as full satisfaction of any claim arising out of such termination.

- **6.3 Data Subject Requests.** Avigilon must, to the extent legally permitted, promptly notify Customer if it receives a request from a Data Subject, including without limitation requests for access to, correction, amendment, transport or deletion of such Data Subject's Personal Data and, to the extent applicable, Avigilon must provide Customer with commercially reasonable cooperation and assistance in relation to any complaint, notice, or communication from a Data Subject. Customer must respond to and resolve promptly all requests from Data Subjects which Avigilon provides to Customer. Customer must be responsible for any reasonable costs arising from Avigilon's provision of such assistance under this Section.

7. Data Transfers. Avigilon agrees that it must not make transfers of Personal Data under this Agreement from one jurisdiction to another unless such transfers are performed in compliance with this Agreement and applicable Data Protection Laws. Avigilon agrees to enter into appropriate agreements with its affiliates and Sub-processors, which will permit Avigilon to transfer Personal Data to its affiliates and Sub-processors. Avigilon agrees to amend as necessary its agreement with Customer to permit transfer of Personal Data from Avigilon to Customer. Avigilon also agrees to assist the Customer in entering into agreements with its affiliates and Sub-processors if required by applicable Data Protection Laws for necessary transfers. To the extent Avigilon is a Processor or Sub-processor of Personal Data subject to the General Data Protection Regulation, (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of Personal Data and on the free movement of such data ("GDPR"), and repealing Directive 95/46/EC, the Standard Contractual Clauses set forth in Schedule 1 hereto must apply to data transfers.

8. Security. Avigilon must implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk posed by the Processing of Personal Data, taking into account the costs of implementation; the nature, scope, context, and purposes of the Processing; and the risk of varying likelihood and severity of harm to the data subjects. The appropriate technical and organizational measures implemented by Avigilon are set forth in **Annex II.** In assessing the appropriate level of security, Avigilon must weigh the risks presented by Processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise Processed.

9. Security Incident Notification. If Avigilon becomes aware of a Security Incident, then Avigilon must (a) notify Customer of the Security Incident without undue delay, (b) investigate the Security Incident and apprise Customer of the details of the Security Incident and (c) take commercially reasonable steps to stop any ongoing

loss of Personal Data due to the Security Incident if in the control of Avigilon. Notification of a Security Incident must not be construed as an acknowledgement or admission by Avigilon of any fault or liability in connection with the Security Incident. Avigilon must make reasonable efforts to assist Customer in fulfilling Customer's obligations under Data Protection Laws to notify the relevant supervisory authority and Data Subjects about such incident.

10. Data Retention and Deletion. Except for anonymized Customer Data, as described above, or as otherwise provided under the Agreement, Avigilon deletes all Customer Data ninety (90) days following termination or expiration of the Agreement unless otherwise required to comply with applicable law. Notwithstanding the foregoing, Avigilon will retain the Customer Data for at least thirty (30) days following such termination or expiration to accommodate a request by Customer for the Customer Data. If, within such thirty (30) day period, Customer requests (in writing), Avigilon will make Customer Data available to Customer for export or download for a period of thirty (30) days. Avigilon has no obligation to retain such Customer Data beyond such thirty (30) day period. Subject to Section 12.4 regarding CJIS Data, Avigilon may delete any Service Use Data upon termination or expiration of the Agreement.

11. Audit Rights

- **11.1 Periodic Audit.** Avigilon will allow Customer to perform an audit of reasonable scope and duration of Avigilon operations relevant to the Products and Services purchased under the Agreement, at Customer's sole expense, for verification of compliance with the technical and organizational measures set forth in **Annex II** if (a) Avigilon notifies Customer of a Security Incident that results in actual compromise to the Products and/or Services purchased; or (b) if Customer reasonably believes Avigilon is not in compliance with its security commitments under this DPA, or (c) if such audit is legally required by the Data Protection Laws. Any audit must be conducted in accordance with the procedures set forth in **Section 11.3** of this DPA and may not be conducted more than one time per year. If any such audit requires access to confidential information of Avigilon's other customers, suppliers or agents, such portion of the audit may only be conducted by Customer's nationally recognized independent third-party auditors in accordance with the procedures set forth in **Section 11.3** of this DPA. Unless mandated by GDPR or otherwise mandated by law or court order, no audits are allowed within a data center for security and compliance reasons. Avigilon must, in no circumstances, provide Customer with the ability to audit any portion of its software, products, and services which would be reasonably expected to compromise the confidentiality of any third-party's information or Personal Data.

- **11.2 Satisfaction of Audit Request.** Upon receipt of a written request to audit, and subject to Customer's agreement, Avigilon may satisfy such audit request by providing Customer with a confidential copy of Avigilon's applicable most recent third-party security review performed by a nationally recognized independent third-party auditor, such as a SOC2 Type II report or ISO 27001 certification, in order that Customer may reasonably verify Avigilon's compliance with industry standards.
- **11.3 Audit Process.** Customer must provide at least sixty days (60) days prior written notice to Avigilon of a request to conduct the audit described in **Section 11.1**. All audits must be conducted during normal business hours, at applicable locations or remotely, as designated by Avigilon. Audit locations, if not remote will generally be those location(s) where Customer Data is accessed, or Processed. The audit must not unreasonably interfere with Avigilon's day to day operations. An audit must be conducted at Customer's sole cost and expense and subject to the terms of the confidentiality obligations set forth in the Agreement. Before the commencement of any such audit, Avigilon and Customer must mutually agree upon the time, and duration of the audit. Avigilon must provide reasonable cooperation with the audit, including providing the appointed auditor a right to review, but not copy, Avigilon security information or materials provided such auditor has executed an appropriate non-disclosure agreement. Avigilon's policy is to share methodology and executive summary information, not raw data or private information. Customer must, at no charge, provide to Avigilon a full copy of all findings of the audit.

12. Regulation Specific Terms

GDPR. To the extent Avigilon is a Processor or Sub-processor of Personal Data subject to the GDPR (as defined in Section 7 herein), the Standard Contractual Clauses set forth in **Schedule 1** hereto must apply.

13. Avigilon Contact. If Customer believes that Avigilon is not adhering to its privacy or security obligations hereunder, Customer must contact the Motorola Data Protection Officer at Motorola Solutions, Inc., 500 W. Monroe St., Chicago, IL USA 60661 – 3618 or at privacy1@motorolasolutions.com.

Schedule 1

STANDARD CONTRACTUAL CLAUSES

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

- (i) The natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and
- (ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer') have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

- (i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;
- (ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);
- (iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);
- (iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);
- (v) Clause 13;
- (vi) Clause 15.1(c), (d) and (e);
- (vii) Clause 16(e);
- (viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure

compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or

proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a Third-Party on documented instructions from the data exporter. In addition, the data may only be disclosed to a Third-Party located outside the European Union (4) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the Third-Party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(a) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(b) the Third-Party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(c) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(d) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least [*Specify time period*] prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

OPTION 2: GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an

agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [*Specify time period*] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (8) The Parties agree that, by complying with this Clause, the data importer fulfills its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfill its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

- (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;
- (ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer’s responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

- (i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;
- (ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;
- (iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in

practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfill its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three:, if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

- (i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or
- (ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

- (i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;
- (ii) the data importer is in substantial or persistent breach of these Clauses; or
- (iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to

which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Denmark.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Denmark.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

1.

Name: …

Address: …

Contact person's name, position and contact details: …

Activities relevant to the data transferred under these Clauses: …

Role (controller/processor): Controller

2.

…

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

1.

Name: Motorola Solutions, Inc.

Address:500 W. Monroe St., Chicago, IL 60661 USA

Contact person's name, position and contact details: Irene Amu, DPO, Privacy1@MotorolaSolutions.com

Activities relevant to the data transferred under these Clauses: Provision of services related to video security and/or access control system in Controller's premises.

Role (controller/processor): Processor

2.

…

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Data subjects include the data exporter's representatives and end-users including employees, contractors, collaborators, and customers of the data exporter. Data subjects may also include individuals attempting to communicate or transfer personal information to users of the services provided by data importer. Avigilon acknowledges that, depending on Customer's use of the Online Service, Customer may elect to include personal data from any of the following types of data subjects in the Customer Data:

- Employees, contractors, and temporary workers (current, former, prospective) of data exporter;
- Dependents of the above;

- Data exporter’s collaborators/contact persons (natural persons) or employees, contractors or temporary workers of legal entity collaborators/contact persons (current, prospective, former);
- Users (e.g., customers, clients, patients, visitors, etc.) and other data subjects that are users of data exporter’s services;
- Partners, stakeholders or individuals who actively collaborate, communicate or otherwise interact with employees of the data exporter and/or use communication tools such as apps and websites provided by the data exporter;
- Stakeholders or individuals who passively interact with data exporter (e.g., because they are the subject of an investigation, research or mentioned in documents or correspondence from or to the data exporter);
- Minors; or
- Professionals with professional privilege (e.g., doctors, lawyers, notaries, religious workers, etc.).

Categories of personal data transferred

Customer’s use of the Products and Services, Customer may elect to include personal data from any of the following categories in the Customer Data:

- Basic personal data (for example place of birth, street name, and house number (address), postal code, city of residence, country of residence, mobile phone number, first name, last name, initials, email address, gender, date of birth), including basic personal data about family members and children;
- Authentication data (for example user name, password or PIN code, security question, audit trail);
- Contact information (for example addresses, email, phone numbers, social media identifiers; emergency contact details);
- Unique identification numbers and signatures (for example Social Security number, bank account number, passport and ID card number, driver’s license number and vehicle registration data, IP addresses, employee number, student number, patient number, signature, unique identifier in tracking cookies or similar technology);
- Pseudonymous identifiers;
- Financial and insurance information (for example insurance number, bank account name and number, credit card name and number, invoice number, income, type of assurance, payment behavior, creditworthiness);

- Commercial Information (for example history of purchases, special offers, subscription information, payment history);
- Biometric Information (for example DNA, fingerprints and iris scans);
- Location data (for example, Cell ID, geo-location network data, location by start call/end of the call. Location data derived from use of wifi access points);
- Photos, video, and audio;
- Internet activity (for example browsing history, search history, reading, television viewing, radio listening activities);
- Device identification (for example IMEI-number, SIM card number, MAC address);
- Profiling (for example based on observed criminal or anti-social behavior or pseudonymous profiles based on visited URLs, click streams, browsing logs, IP-addresses, domains, apps installed, or profiles based on marketing preferences);
- HR and recruitment data (for example declaration of employment status, recruitment information (such as curriculum vitae, employment history, education history details), job and position data, including worked hours, assessments and salary, work permit details, availability, terms of employment, tax details, payment details, insurance details and location, and organizations);
- Education data (for example education history, current education, grades and results, highest degree achieved, learning disability);
- Citizenship and residency information (for example citizenship, naturalization status, marital status, nationality, immigration status, passport data, details of residency or work permit);
- Information processed for the performance of a task carried out in the public interest or in the exercise of an official authority;
- Special categories of data (for example racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, data concerning a natural person’s sex life or sexual orientation, or data relating to criminal convictions or offences); or
- Any other personal data identified in Article 4 of the GDPR.

Sensitive data transferred *(if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for*

instance strict purpose limitation, access restrictions (including access only for staff having followed specialized training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

…

***The frequency of the transfer** (e.g. whether the data is transferred on a one-off or continuous basis).*

Data may be transferred on a continuous basis during the term of the Agreement or other agreement to which this DPA applies.

Nature of the processing

The nature, scope and purpose of processing personal data is to carry out performance of Avigilon's obligations with respect to provision of the Products and Services purchased under the Agreement. The data importer utilizes a global network of data centers and management/support facilities, and processing may take place in any jurisdiction where data importer or its sub-processors utilize such facilities.

Purpose(s) of the data transfer and further processing

The nature, scope and purpose of processing personal data is to carry out performance of Avigilon's obligations with respect to provision of the Products and Services purchased under the Agreement. The data importer utilizes a global network of data centers and management/support facilities, and processing may take place in any jurisdiction where data importer or its sub-processors utilize such facilities

***The period for which the personal data will be retained,** or, if that is not possible, the criteria used to determine that period*

Data retention is governed by Section 10 of this Data Processing Agreement

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

Transfers to sub-processors will only be for carrying out the performance of Avigilon's obligations with respect to provision of the Products and Services purchased under the Agreement. The duration of the processing will be for the term of the Agreement. The data importer utilizes a global network of data centers and management/support facilities, and processing may take place in any jurisdiction where data importer or its sub-processors utilize such facilities.

C. COMPETENT SUPERVISORY AUTHORITY

The Danish Data Protection Agency

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

[Examples of possible measures:

Measures of pseudonymisation and encryption of personal data

Where technically feasible and when not impacting services provided:

- Avigilon minimizes the data it collects to information it believes is necessary to communicate, provide, and support products and services and information necessary to comply with legal obligations.
- Avigilon encrypts data in transit and at rest.
- Avigilon pseudonymizes and limits administrative accounts that have access to reverse pseudonymisation.

Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services

In order to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services, Avigilon Information Protection policy mandates the institutionalization of information protection throughout solution development and operational lifecycles. Avigilon maintains dedicated security teams for its internal information security and its products and services. Its security practices and policies are integral to its business and mandatory for all Avigilon employees and contractors The Avigilon Chief Information Security Officer maintains responsibility and executive

oversight for such policies, including formal governance, revision management, personnel education and compliance. Avigilon generally aligns to the NIST Cybersecurity Framework as well as ISO 27001.

Some of the system configuration is under the control of the customer.

Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident

Security Incident Procedures Avigilon maintains a global incident response plan to address any physical or technical incident in an expeditious manner. Avigilon maintains a record of security breaches with a description of the breach, the time period, the consequences of the breach, the name of the reporter, and to whom the breach was reported, and the procedure for recovering data. For each security breach that is a Security Incident, notification will be made in accordance with the Security Incident Notification section of this DPA.

Business Continuity and Disaster Preparedness Avigilon maintains business continuity and disaster preparedness plans for critical functions and systems within Avigilon's control that support the Products and Services purchased under the Agreement in order to avoid services disruptions and minimize recovery risks.

Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing

Avigilon periodically evaluates its processes and systems to ensure continued compliance with obligations imposed by law, regulation or contract with respect to the confidentiality, integrity, availability, and security of Customer Data, including personal information. Avigilon documents the results of these evaluations and any remediation activities taken in response to such evaluations. Avigilon periodically has Third-Party assessments performed against applicable industry standards, such as ISO 27001, 27017, 27018 and 27701.

Measures for user identification and authorisation

Identification and Authentication**.** Avigilon uses industry standard practices to identify and authenticate users who attempt to access Avigilon information systems. Where authentication mechanisms are based on passwords, Avigilon requires that the passwords are at least eight characters long and are changed regularly. Avigilon uses industry standard password protection practices, including practices designed to maintain the confidentiality and integrity of passwords when they are assigned and distributed, and during storage.

Access Policy and Administration. Avigilon maintains a record of security privileges of individuals having access to Customer Data. including personal information. Avigilon maintains appropriate processes for requesting, approving and administering accounts and access privileges in connection with the Processing of Customer Data. Only authorized personnel may grant, alter or cancel authorized access to data and resources. Where an individual has access to systems containing Customer Data, the individuals are assigned separate, unique identifiers. Avigilon deactivates authentication credentials on a periodic basis.

Measures for the protection of data during transmission

Data is generally encrypted during transmission within the Avigilon managed environments. Encryption in transit is also generally required of any sub-processors. Further, protection of data in transit is also achieved through the access controls, physical and environmental security, and personnel security described throughout this Annex II.

Measures for the protection of data during storage

Data is generally encrypted during storage within the Avigilon managed environments. Encryption in storage is also generally required of any sub-processors. Further, protection of data in storage is also achieved through the access controls, physical and environmental security, and personnel security described throughout this Annex II.

Measures for ensuring physical security of locations at which personal data are processed

Avigilon maintains appropriate physical and environment security controls to prevent unauthorized access to Customer Data, including personal information. This includes appropriate physical entry controls to Avigilon facilities such as card-controlled entry points, and a staffed reception desk to protect against unauthorized entry. Access to controlled areas within a facility will be limited by job role and subject to authorized approval. Use of an access badge to enter a controlled area will be logged and such logs will be retained in accordance with Avigilon policy. Avigilon revokes personnel access to Avigilon facilities and controlled areas upon separation of employment in accordance with Avigilon policies. Avigilon policies impose industry standard workstation, device and media controls designed to further protect Customer Data, including personal information.

Measures for ensuring personnel security

Access to Customer Data. Avigilon maintains processes for authorizing and supervising its employees, and contractors with respect to monitoring access to Customer Data. Avigilon requires its employees, contractors and agents who have, or may be expected to have, access to Customer Data to comply with the provisions of the Agreement, including this Annex and any other applicable agreements binding upon Avigilon.

Security and Privacy Awareness. Avigilon must ensure that its employees and contractors remain aware of industry standard security and privacy practices, and their responsibilities for protecting Customer Data and Personal Data. This must include, but not be limited to, protection against malicious software, password protection, and management, and use of workstations and computer system accounts. Avigilon requires periodic Information security training, privacy training, and business ethics training for all employees and contract resources

Sanction Policy. Avigilon maintains a sanction policy to address violations of Avigilon's internal security requirements as well as those imposed by law, regulation, or contract.

Background Checks. Avigilon follows its standard mandatory employment verification requirements for all new hires. In accordance with Avigilon internal policy, these requirements must be periodically reviewed and include, but may not be limited to, criminal background checks, proof of identity validation and any additional checks as deemed necessary by Avigilon.

Measures for ensuring events logging

Avigilon maintains policies requiring continuous monitoring and event logging on all production information resources. Application audit trail logs must be captured on all production Avigilon information resources. Audit trail logs of production Avigilon information resources are regularly reviewed and appropriate remedial actions are taken when necessary.

Measures for ensuring system configuration, including default configuration

Measures for internal IT and IT security governance and management

The Motorola Solutions Enterprise Information Security organization is structured as follows: Governance/ Risk/ Compliance, Threat Intelligence & Vulnerability Management, Detection, Protection, and Response. Avigilon assesses organization's effectiveness annually via external assessors who report and share the assessment findings with Avigilon Audit Services who tracks any identified remediations. For more

information, please see the Avigilon Trust Center at https://www.motorolasolutions.com/en_us/about/trust-center/security.html

Measures for certification/assurance of processes and products

Avigilon performs internal Secure Application Review and Secure Design Review security audits and Production Readiness Review security readiness reviews prior to service release. Where appropriate, privacy assessments are performed for Avigilon's products and services. A risk register is created as a result of internal audits with assignments tasked to appropriate personnel. Security audits are performed annually with additional audits as needed. Additional privacy assessments, including updated data maps, occur when material changes are made to the products or services. Further, Avigilon Solution has achieved AICPA SOC2 Type 2 reporting and ISO/IEC 27001:2013 certification for many of its development and support operations.

Measures for ensuring data minimisation

Avigilon policies require processing of all personal information in accordance with applicable law, including when that law requires data minimisation. Further, Avigilon conducts privacy assessments of its products and services and evaluates if those products and services support the principles of processing, such as data minimisation, as set forth in Article 5 of the GDPR.

Measures for ensuring data quality

Avigilon policies require processing of all personal information in accordance with applicable law, including when that law requires ensuring the quality and accuracy of data. Further, Avigilon conducts privacy assessments of its products and services and evaluates if those products and services support the principles of processing, such as ensuring data quality, as set forth in Article 5 of the GDPR.

Measures for ensuring limited data retention

Avigilon maintains a data retention policy that provides a retention schedule outlining storage periods for personal data. The schedule is based on business needs and provides sufficient information to identify all records and to implement disposal decisions in line with the schedule. The policy is periodically reviewed and updated.

Measures for ensuring accountability

To ensure compliance with the principle of accountability, Avigilon maintains a Privacy Program which generally aligns its activities to both the Nymity Privacy Management and Accountability Framework and NIST Privacy Framework. The Privacy Program is audited annually by Motorola Solutions Audit Services.

Measures for allowing data portability and ensuring erasure

When subject to a data subject request to move, copy or transfer their personal data, Avigilon will provide personal data in a structured, commonly used and machine readable format. Where possible and if an individual requests it, Avigilon can directly transmit the personal information to another organization.

For transfers to (sub-) processors*, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter.*

Processor contracts with its sub-processors in a manner that allows for it to be compliant with its obligations to Controller. With respect to Processor's affiliated companies located around the globe, Processor has BCRs in place. With respect to third-party vendors, Processor contracts appropriately-including SCCs when appropriate, and performs a security assessment prior to disclosing any customer data to the vendor.

ANNEX III

LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors:

AVIGILON ALTA

Name and Services (Name and registered address of Supplier entity or subcontractor, with brief description of corresponding Services)	**Location/ Transfers (Location where entity will Process the Personal Data. Indicate where and from whom**	**Mechanism (Agreed mechanism for ensuring any transfer is compliant with Data Protection Laws)**

	transferred, where relevant)	
Microsoft Azure (Cloud Platform)	EU	N/A
Elastic (cloud Services storage for JSON documents)	EU	N/A
Google Ireland Ltd (Ava Security cloud)	US, EU, UK, CA, AU,	SCCs
OpenPath Security, Inc. (an MSI company)	US, EU	SCCs
Amazon Web Services EMEA	US	SCCs
Freshworks Inc.	US	SCCs
Wasabi.com	US, EU, AU, CA	SCCs or similar applicable contracting mechanism as needed
Digital Ocean	US, EU, UK, CA, SG	SCCs or similar applicable contracting mechanism as needed
Mixpanel, Inc.	US, EU	SCCs
Bugfender	US, EU	SCCs
Bugsnag	US, EU	SCCs
Avigilon Corporation (an MSI company)	US/CA/EU	SCCs
Avigilon USA Corporation (an MSI company)	US/EU	SCCs
Millicast	US	SCCs
Netsuite	US	SCCs

Hubspot	US	SCCs
Locize	EU	N/A
Mouseflow	US	SCCs
LiveKit	US	SCC's

AVIGILON UNITY

Name and Services (Name and registered address of Supplier entity or subcontractor, with brief description of corresponding Services)	**Location/ Transfers (Location where entity will Process the Personal Data. Indicate where and from whom transferred, where relevant)**	**Mechanism (Agreed mechanism for ensuring any transfer is compliant with Data Protection Laws)**	**Applicable for Cloud Services Only**
Microsoft Corporation	US, Australia and Canada	Appropriate Contracting Mechanisms	Yes
Elastic	US, Australia and Canada	Appropriate Contracting Mechanisms	Yes
Google, Inc.	Worldwide	Appropriate Contracting Mechanisms	
Apple, Inc.	Worldwide	Appropriate Contracting	

		Mechanisms	
Motorola Solutions, Inc., including subsidiaries	Worldwide	Appropriate Contracting Mechanisms	
Flexera	US	Appropriate Contracting Mechanisms	
Whatsapp	Worldwide	Appropriate Contracting Mechanisms	
Twilio	US	Appropriate Contracting Mechanisms and BCR	Yes
PubNub	US	Appropriate Contracting Mechanisms	Yes
Salesforce	US	Appropriate Contracting Mechanisms and BCR	

Join the Conversation:

ABOUT US

PARTNERS

INVESTORS

NEWSROOM

TRAININGS

CAREERS

COMMUNITY

Privacy Statement Communication Preference Your California Privacy Choices

Cookie Preferences