Motorola Solutions Global Data Processing Addendum

This Data Processing Addendum, including its Schedules and Annexes ("DPA") forms part of the underlying Motorola Solutions Customer Agreement ("Agreement") to reflect the parties' agreement with regard to the Processing of Customer Data which may include Personal Data. In the event of a conflict between this DPA, the Agreement or any Schedule, Annex or other addenda to the Agreement, including a prior DPA, this DPA must prevail.

1. Definitions.

All capitalized terms not defined herein must have the meaning set forth in the Agreement. To the extent the Agreement provides definitions for the terms defined in this Section 1, the definitions of this Section 1 will apply to this DPA and the definitions of the Agreement will apply to the Agreement. All lower case 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.

"Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.

"**Customer Data**" means data including images, text, videos, and audio, that are provided to Motorola 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 comprised of Personal Information, or Third Party Data.

"Customer Contact Data" means data Motorola collects from Customer for contact purposes, including, without limitation, contract fulfillment, marketing, advertising, licensing, and sales activities.

"Data" means collectively Motorola Data and Customer Data, including any Personal Data included therein.

"Data Protection Laws and Policies" means all applicable corporate, state and local, federal and international laws, standards, guidelines, policies, regulations and procedures applicable to Supplier or Motorola pertaining to data security, confidentiality, privacy, and breach notification, as amended, including without limitation the European Union General Data Protection Regulation (GDPR), and the UK Data Protection Act 2018.

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

"GDPR" means European Union General Data Protection Regulation 2016/679.

“Metadata” means data that describes other data.

“Motorola Data” means data provided by Motorola and made available to Customer in connection with the provision of Products and Services.

“Personal Data” or **“Personal Information”** means any information relating to an identified or identifiable natural person transmitted to Motorola 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.

“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.

“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.

“Security Incident” means an incident that compromises or is suspected to compromise the security, confidentiality, integrity or availability of Motorola Data, Customer Data or Personal Data. For the avoidance of doubt, “suspected to compromise” means a determination by Motorola based on specific and articulable facts and circumstances, taken together with rational inferences from those facts, that an act or omission may likely result in a breach of security, confidentiality, availability or integrity with respect to the Motorola Data, Customer Data or Personal Data. .

“**Service Use Data**” means data generated about the use of the Products and Services through Customer’s use or Motorola’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 **Schedule 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” or “Service Provider” means other processors engaged by Motorola to Process Customer Data which may include Personal Data.

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

“Users” means Customer’s employees, contractors, agents, customers and end-users who are authorized to use the Services to access or receive Data. Motorola or customer (as determined by Motorola) will be responsible for all User identification and password change management.

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 Motorola is the Processor who may engage Sub-processors pursuant to the requirements of **Section 6** entitled “Sub-processors” below.

2.2. Motorola’s Processing of Customer Data. Motorola and Customer agree that Motorola 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 Motorola 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 Motorola 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 Motorola that Customer’s instructions, including appointment of Motorola as a Processor or Sub-processor, have been authorized by the relevant Controller. Customer Data may be processed by Motorola at any of its global locations and/or disclosed to Sub-processors. It is Customer’s responsibility to notify Authorized Users of Motorola’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 Motorola that it has complied with the terms of this provision.

2.2.1. **Additional Products and Services.** In the event, Customer purchases additional Products and Services that integrate with the previously purchased Products and Services, Customer Data may be processed at additional locations around the world and by Sub-processors utilized in

connection with the additional Products and Services. Identification of Sub-processors utilized by Motorola Solutions can be found at Motorola Sub-Processors or Annex III attached hereto.

2.3. Details of Processing. The subject-matter of Processing of Personal Data by Motorola hereunder, the duration of the Processing, the categories of Data Subjects and types of Personal Data are set forth on **Schedule 2, Annex I** to this DPA.

2.4. Disclosure of Processed Data. Motorola must not disclose to or share any Customer Data with any third party except to Motorola'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, Motorola 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, Motorola retains the right to comply with applicable law. Motorola 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 (i) the lawfulness of any transfer of Personal Data to Motorola, (ii) the accuracy, quality, and legality of Personal Data provided to Motorola; (iii) the means by which Customer acquired Personal Data, and (iv) 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 Motorola to the minimum necessary for Motorola to perform in accordance with the Agreement. 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 Motorola shall not be liable for any Security Incident arising from Customer's breach of this requirement.

2.6. Customer Indemnity. To the extent permitted by applicable law, Customer will defend, indemnify, and hold Motorola 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. Motorola will give Customer prompt, written notice of any claim

subject to the foregoing indemnity. Motorola 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 Motorola 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 Motorola at any of its global locations and/or disclosed to Sub-processors.

4. **Third Party Data and Motorola Data**. Motorola Data and Third Party Data may be available to Customer through the Products and Services. Customer and its Authorized Users may use the Motorola Data and Third Party Data as permitted by Motorola and the applicable Third Party Data provider, as described in the Agreement or applicable Addendum. Unless expressly permitted in the Agreement or applicable Addendum, Customer must not, and must ensure its Authorized Users must not: (a) use the Motorola 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 or applicable Addendum. Any rights granted to Customer or Authorized Users with respect to Motorola Data or Third Party Data must immediately terminate upon termination or expiration of the Agreement or applicable Addendum, Ordering Document, or the - Agreement. Further, Motorola or the applicable Third Party Data provider may suspend, change, or terminate Customer's or any Authorized User's access to Motorola Data or Third Party Data if Motorola 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 Motorola's agreement with the applicable Third Party Data provider. Upon termination of Customer's rights to use of any Motorola 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 Motorola. Notwithstanding any provision of the Agreement to the contrary, Motorola has no liability for Third Party Data or Motorola Data available through the Products and Services. Motorola and its Third Party Data providers reserve all rights in and to Motorola Data and Third Party Data not expressly granted in the Agreement, an Addendum or Ordering Document.

5. **Motorola as a Controller or Joint Controller.** In all instances where Motorola acts as a Controller it must comply with the applicable provisions of the Motorola Privacy Statement at Motorola Privacy Statement as each may be updated from time to time. Motorola holds all Customer Contact Data as a Controller and must Process such Customer Contact Data in accordance with the Motorola Privacy Statement. In

instances where Motorola 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 Motorola may engage Sub-processors who in turn may engage Sub-processors to Process Personal Data in accordance with the DPA. A list of Sub-processors is set forth at Motorola Sub-Processors or **Annex III,** if **Annex III** has been completed. When engaging Sub-processors, Motorola 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 Motorola engaging Sub-processors to process Customer Data provided that: (i) Motorola 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 Motorola Sub-Processors; (ii) Motorola imposes data protection terms on any Sub-processor it appoints that protect the Customer Data to the same standard provided for by this Addendum; and (iii) Motorola 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 Motorola'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 an event, Motorola will either appoint or replace the Sub-processor or, if in Motorola'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. Motorola 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, Motorola 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 Motorola provides to Customer. Customer must be responsible for any reasonable costs arising from Motorola's provision of such assistance under this Section.

7. Data Transfers. Motorola 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 Addendum and applicable Data Protection Laws. Motorola agrees to enter into appropriate agreements with its affiliates and Sub-processors, which will permit Motorola to transfer Personal Data to its affiliates and Sub-processors. Motorola agrees to amend as necessary its agreement with Customer to permit transfer of Personal Data from Motorola to Customer. Motorola 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.

8. **Security.** Motorola 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 Motorola are set forth in **Schedule 3.** In assessing the appropriate level of security, Motorola 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 Motorola becomes aware of a Security Incident, then Motorola must (i) notify Customer of the Security Incident without undue delay, (ii) investigate the Security Incident and apprise Customer of the details of the Security Incident and (iii) take commercially reasonable steps to stop any ongoing loss of Personal Data due to the Security Incident if in the control of Motorola. Notification of a Security Incident must not be construed as an acknowledgement or admission by Motorola of any fault or liability in connection with the Security Incident. Motorola 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. Notwithstanding the foregoing, If Motorola becomes aware of a Security Incident that involves Customer Data which is Personal Data, Motorola shall provide notice to Customer, law enforcement, applicable regulators and affected individuals if required under applicable laws and regulations.

10. **Data Retention and Deletion**. Except for anonymized Customer Data, as described above, or as otherwise provided under the Agreement, Motorola deletes all Customer Data ninety (90) days following termination or expiration of the Agreement or the applicable Addendum or Ordering Document unless otherwise required to comply with applicable law. Notwithstanding the foregoing, Motorola 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), Motorola will make Customer Data available to Customer for export or download for a period of thirty (30) days. Motorola has no obligation to retain such Customer Data beyond such thirty (30) day period. Subject to Section 12.3 regarding CJIS Data, Motorola may delete any Service Use Data upon termination or expiration of the Agreement or the applicable Addendum or Ordering Document.

11. **Audit Rights**

11.1. **Periodic Audit.** Motorola will allow Customer to perform an audit of reasonable scope and duration of Motorola 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 **Schedule 3** if (i) Motorola notifies Customer of a Security Incident that results in actual compromise to the Products and/or Services purchased; or (ii) if Customer reasonably believes Motorola is not in compliance with its security commitments under this DPA, or (iii) 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 Motorola'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. Motorola 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, Motorola may satisfy such audit request by providing Customer with a confidential copy of a Motorola'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 Motorola's compliance with industry standards.

11.3. Audit Process. Customer must provide at least sixty days (60) days prior written notice to Motorola 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 Motorola. 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 Motorola'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, Motorola and Customer must mutually agree upon the time, and duration of the audit. Motorola must provide reasonable cooperation with the audit, including providing the appointed auditor a right to review, but not copy, Motorola security information or materials provided such auditor has executed an appropriate non-disclosure agreement. Motorola's policy is to share methodology and executive summary information, not raw data or private information. Customer must, at no charge, provide to Motorola a full copy of all findings of the audit.

12. Regulation Specific Terms

12.1. HIPAA Business Associate. If Customer is a "covered entity" or a "business associate" and includes "protected health information" in Customer Data as those terms are defined in 45 CFR § 160.103, execution of the Agreement includes execution of the Motorola HIPAA Business Associate Agreement Addendum ("BAA"). Customer may opt out of the BAA by sending the following information to Motorola in a written notice under the terms of the Customer's

Agreement: "Customer and Motorola agree that no Business Associate Agreement is required. Motorola is not a Business Associate of Customer's, and Customer agrees that it will not share or provide access to Protected Health Information to Motorola or Motorola's sub-processors."

12.2. FERPA. If Customer is an educational agency or institution to which regulations under the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (FERPA), apply, Motorola acknowledges that for the purposes of the DPA, Motorola is a "school official" with "legitimate educational interests" in the Customer Data, as those terms have been defined under FERPA and its implementing regulations, and Motorola agrees to abide by the limitations and requirements imposed by 34 CFR 99.33(a) on school officials. Customer understands that Motorola may possess limited or no contact information for Customer's students and students' parents. Consequently, Customer must be responsible for obtaining any parental consent for any end user's use of the Online Service that may be required by applicable law and to convey notification on behalf of Motorola to students (or, with respect to a student under 18 years of age and not in attendance at a post-secondary institution, to the student's parent) of any judicial order or lawfully-issued subpoena requiring the disclosure of Customer Data in Motorola's possession as may be required under applicable law.

12.3. CJIS. Motorola agrees to support the Customer's obligation to comply with the Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Security Policy and must comply with the terms of the CJIS Security Addendum for the Term of this Agreement and such CJIS Security Addendum is incorporated herein by reference. Customer hereby consents to allow Motorola "screened" personnel as defined by the CJIS Security Policy to serve as an authorized "escort" within the meaning of CJIS Security Policy for escorting unscreened Motorola personnel that require access to unencrypted Criminal Justice Information for purposes of Tier 3 support (e.g. troubleshooting or development resources). In the event Customer requires access to Service Use Data for its compliance with the CJIS Security Policy, Motorola must make such access available following Customer's request. Notwithstanding the foregoing, in the event the Agreement]or applicable Ordering Document terminates, Motorola must carry out deletion of Customer Data in compliance with **Section 10** herein and may likewise delete Service Use Data within the time frame specified therein. To the extent Customer objects to deletion of its Customer Data or Service Use Data and seeks retention for a longer period, it must provide written notice to Motorola prior to expiration of the 30 day period for data retention to arrange return of the Customer Data and retention of the Service Use Data for a specified longer period of time.

12.4. CCPA / CPRA. If Motorola is Processing Personal Data within the scope of the California Consumer Protection Act ("CCPA") and/or the California Privacy Rights Act ("CPRA") (collectively referred to as the "California Privacy Acts"), Customer acknowledges that Motorola is a "Service Provider" within the meaning of California Privacy Acts. Motorola must process Customer Data and Personal Data on behalf of Customer and, not retain, use, or disclose that data for any purpose other than for the purposes set out in this DPA and as permitted under the California Privacy Acts, including under any "sale" exemption. In no event will Motorola sell any such data. If a California Privacy Act applies, Personal Data must also include any data identified with the California Privacy Act or Act's definition of personal data. Motorola shall provide Customer with notice should it determine that it can no longer meet its obligations under the California Privacy Acts, and the parties agree that, if appropriate and reasonable, Customer

may take steps necessary to stop and remediate unauthorized use of the impacted Personal Data.

12.5 **CPA, CTDPA, VCDPA.** If Motorola is Processing Personal Data within the scope of the Colorado Privacy Rights Act ("CPA"), the Connecticut Data Privacy Act ("CTDPA"), or the Virginia Consumer Data Protection Act ("VCDPA") Motorola will comply with its obligations under the applicable legislation, and shall make available to Customer all information in its possession necessary to demonstrate compliance with obligations in accordance with such legislation. **Motorola Contact.** If Customer believes that Motorola 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, Chicago, IL USA 90661-3618 or at privacy1@motorolasolutions.com.

12.6 **GDPR**. To the extent Motorola 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.

12.7 **UK-GDPR**. To the extent Motorola is a Processor or Sub-processor of Personal Data subject to the UK-GDPR, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses **Schedule 1** hereto must apply.

13. **Motorola Contact.** If Customer believes that Motorola 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, Chicago, IL USA 90661-3618 or at privacy1@motorolasolutions.com.

Schedule 1

Cross Border Transfer Mechanisms

1.1 ***"Standard Contractual Clauses"*** means the Standard Contractual Clauses approved by the European Commission in decision 2021/914.

1.2 **"*UK IDTA*"** means the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner, Version B1.0, in force 21 March 2022.

2. Cross Border Data Transfer Mechanisms.

2.1 2021 Standard Contractual Clauses. The parties agree that the 2021 Standard Contractual Clauses will apply to personal data that is transferred via the Services from the European Economic Area or Switzerland, either directly or via onward transfer, to any country or recipient outside the European Economic Area or Switzerland that is not recognized by the European Commission (or, in the case of transfers from Switzerland, the competent authority for Switzerland) as providing an adequate level of protection for personal data. For data transfers from the European Economic Area that are subject to the 2021 Standard Contractual Clauses (https://commission.europa.eu/publications/sta), the 2021 Standard Contractual Clauses will be deemed entered into (and incorporated into this Addendum by this reference) and completed as follows:

(a) Module Two (Controller to Processor) of the Standard Contractual Clauses will apply where Customer is the Controller and Motorola is the Processor.
(b) Module Three (Processor to Processor) of the Standard Contractual Clauses will apply where Customer is the Processor and Motorola is the Sub-Processor.
(c) For each Module, where applicable:

	Module 2: Controller to Processor	**Module 3: Processor to Processor**
Clause 7 (Docking Clause)	Intentionally Omitted	Intentionally Omitted
Clause 9 (Use of Sub-processors)	Option 2: General Written Authorisation 30 business days	Option 2: General Written Authorisation 30 business days
Clause 11 (Redress)	Intentionally Omitted	Intentionally Omitted
Clause 13 (Supervision) Option 1: Where the data exporter is established in an EU Member State Option 2: Where the data exporter is not established in an EU Member State and has appointed a representative Option 3: Where the data exporter is not established in an EU Member State without having to appoint a representative	Option 1, Option 2 and/or Option 3 applies in accordance with whether the exporter(s) is/are established in an EU Member State and has/have appointed a representative.	Option 1, Option 2 and/or Option 3 applies in accordance with whether the exporter(s) is/are established in an EU Member State and has/have appointed a representative.
Clause 14 (Local laws and practices affecting compliance with the Clauses)	Applicable	Applicable
Clause 15 (Obligations of the data importer in case of access by public authorities)	Applicable	Applicable
Clause 17 (Governing law)	Denmark	Denmark
Clause 18 (Choice of forum and jurisdiction)	Denmark	Denmark
Appendix: Annex I: A	Data Exporter and Data Importer: Motorola and Supplier, as applicable. Contact Details:	

	Motorola: privacy1@motorolasolutions.com; Supplier: Supplier's publicly available email address for receiving privacy related notices. The Data Exporter's role is as set forth in the Agreement. The Data Importer's role is as set forth in the Agreement. Signature and Date: By entering into the Agreement, Data Exporter and Data Importer are deemed to have signed these Standard Contractual Clauses incorporated herein, including their Annexes, as of the Effective Date of the Agreement.	
Appendix: Annex I: B	The Categories of data subjects are described in Schedule 2 (Details of Processing) of this Addendum. Sensitive Data transferred is described in Section 2 of Schedule 2 (Details of Processing) of this Addendum The frequency of the transfer is a continuous basis for the duration of the Agreement or as may otherwise be specified in the Agreement, a Work Order or a Purchase Order. The nature of the processing is described in Section 2 of this Addendum The period for which the	

	personal data will be retained is described in Section 2 (Details of Processing) of this Addendum	
Appendix: Annex I: C (Competent Supervisory Authority)	Datatilsynet (Danish Data Protection Agency)	Datatilsynet (Danish Data Protection Agency)
Link to Sub-processor list (Optional)	This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1). However, MSI requires it to be filled out in either case, with a link to an online subprocessor list being sufficient. Controller shall inform, in writing, of any intended changes to the agreed list of sub-processors. In addition to the sub-processors linked in Annex III, Controller has authorized the use of the following sub-processors: 1. Name: … Address: … Contact person's name, position and contact details: … Description of processing (including a clear delimitation of responsibilities in case several sub-processors are authorized): …	
Annex II	Schedule 3 (Technical and Organizational Security Measures) of this Addendum serves as Annex II of the Standard Contractual Clauses.	

2.2 Data Transfers From Switzerland. For data transfers from Switzerland that are subject to the Standard Contractual Clauses, the Standard Contractual Clauses will be deemed entered into (and incorporated into this Addendum by this reference) and completed as set out in Section 2.1 of this Schedule 1, subject to the following modifications:

(i) references to “EU Member State” and “Member State” will be interpreted to include Switzerland, and

(ii) insofar as the transfer or onward transfers are subject to the Swiss Federal Act on Data Protection, as revised (FADP):

(1) references to "Regulation (EU) 2016/679" are to be interpreted as references to the FADP;

(2) the "competent supervisory authority" in Annex I, Part C will be the Swiss Federal Data Protection and Information Commissioner;

(3) in Clause 17 (Option 1), the EU Standard Contractual Clauses will be governed by the laws of Switzerland; and

(4) in Clause 18(b) of the EU Standard Contractual Clauses, disputes will be resolved before the courts of Switzerland.

2.3 UK International Data Transfer Agreement. The parties agree that the UK IDTA will apply to personal data that is transferred via the Services from the United Kingdom, either directly or via onward transfer, to any country or recipient outside of the United Kingdom that is not recognized by the competent United Kingdom regulatory authority or governmental body as providing an adequate level of protection for personal data. For data transfers from the United Kingdom that are subject to the UK IDTA, the UK IDTA will be deemed entered into (and incorporated into this Addendum by this reference) and completed as follows:

(a) In Table 1 of the UK IDTA, the parties’ details and key contact information is located in Section 2.1(d)(vi) of Schedule 2 of this Addendum.

(b) In Table 2 of the UK IDTA, information about the version of the Approved EU SCCs, modules and selected clauses which this UK International Data Transfer Agreement is appended to is located in Section 2.1 of this Addendum.

(c) In Table 3 of the UK IDTA:

1. The list of Parties is located in Annex 1 A of the EU SCCs as set forth in this Schedule 1 of the Addendum.

2. The description of the transfer is set forth in Section 1 (Nature and Purpose of the Processing) of Schedule 2 (Details of the Processing) of this Addendum.

3. Annex II is located in Schedule 3 (Technical and Organizational Security Measures) of this Addendum.

(d) In Table 4 of the UK IDTA, both the Importer and the Exporter may end the UK IDTA in accordance with the terms of the UK IDTA.

SCHEDULE 2

(Annex I of the EU SCC)

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. Motorola 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), Agreemental 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 antisocial 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 offenses); 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.*

To the extent that a solution sold under an Agreement requires the processing of sensitive personal information, it will be restricted to the minimum processing necessary for the solution functionality and be subject to technical security measures appropriate to the nature of the information.

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 to which this DPA applies.

Nature of the processing

The nature, scope and purpose of processing personal data is to carry out performance of Motorola's obligations with respect to provision of the Products and Services purchased under the Agreement and applicable Ordering Documents. 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 Motorola's obligations with respect to provision of the Products and Services purchased under the Agreement and applicable Ordering Documents. 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 Addendum

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 Motorola's obligations with respect to provision of the Products and Services purchased under the Agreement and applicable Ordering Documents. 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.

SCHEDULE 3

(Annex II of the EU SCC)

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

EXPLANATORY NOTE:

The technical and organizational 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.

Measures of pseudonymisation and encryption of personal data

Where technically feasible and when not impacting services provided:

- Motorola Solutions 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.
- Motorola Solutions encrypts data in transit and at rest.
- Motorola Solutions pseudonymised 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, Motorola Solutions Information Protection policy mandates the institutionalization of information protection throughout solution development and operational lifecycles. Motorola Solutions 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 Motorola Solutions employees and contractors The Motorola Chief Information Security Officer maintains responsibility and executive oversight for such policies, including formal governance, revision management, personnel education and compliance. Motorola Solutions 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. Motorola Solutions maintains a global incident response plan to address any physical or technical incident in an expeditious manner. Motorola 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. Motorola maintains business continuity and disaster preparedness plans for critical functions and systems within Motorola'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 organizational measures in order to ensure the security of the processing

Motorola 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. Motorola documents the results of these evaluations and any remediation activities taken in response to such evaluations. Motorola 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**.** Motorola uses industry standard practices to identify and authenticate users who attempt to access Motorola information systems. Where authentication mechanisms are based on passwords, Motorola requires that the passwords are at least eight characters long and are changed regularly. Motorola 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**.** Motorola maintains a record of security privileges of individuals having access to Customer Data, including personal information. Motorola 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. Motorola deactivates authentication credentials on a periodic basis.

Measures for the protection of data during transmission

Data is generally encrypted during transmission within the Motorola 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 **Schedule 3**.

Measures for the protection of data during storage

Data is generally encrypted during storage within the Motorola 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 **Schedule 3**.

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

Motorola maintains appropriate physical and environment security controls to prevent unauthorized access to Customer Data, including personal information. This includes appropriate physical entry controls to Motorola 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 Motorola policy. Motorola revokes personnel access to Motorola facilities and controlled areas upon separation of employment in accordance with Motorola policies. Motorola 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. Motorola maintains processes for authorizing and supervising its employees, and contractors with respect to monitoring access to Customer Data. Motorola 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 Motorola.

Security and Privacy Awareness. Motorola 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. Motorola requires periodic Information security training, privacy training, and business ethics training for all employees and contract resources

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

Background Checks. Motorola follows its standard mandatory employment verification requirements for all new hires. In accordance with Motorola 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 Motorola.

Measures for ensuring events logging

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

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. Motorola assesses organization's effectiveness annually via external assessors who report and share the assessment findings with Motorola Audit Services who tracks any identified remediations. For more information, please see the Motorola Trust Center at MSI Trust Center

Measures for certification/assurance of processes and products

Motorola 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 Motorola'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, Motorola 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

Motorola Solutions policies require processing of all personal information in accordance with applicable law, including when that law requires data minimisation. Further, Motorola Solutions 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

Motorola Solutions 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, Motorola Solutions 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

Motorola Solutions 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, Motorola Solutions 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, Motorola Solutions will provide personal data in a structured, commonly used and machine readable format. Where possible and if an individual requests it, Motorola Solutions can directly transmit the personal information to another organization.

SCHEDULE 4

(Annex III of the EU SCC)

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 authorized the use of the following sub-processors:

Motorola Sub-Processors unless otherwise identified below.