DATA PROCESSING AGREEMENT

This agreement, including the Data Specification Annex, the Security Annex and any other documents attached or referred to below (jointly the "**Data Processing Agreement**"), is entered into by and between Axis and You (the "**Data Controller**") to govern the data processing operations performed by Axis in connection with Your use of services (the "**Services**") provided by Axis pursuant to the Axis End User License Agreement (available at End user license agreements | Axis Communications) and applicable product specific terms for the Services (collectively the "**Services Agreement**") and forms an integral part of the Services Agreement.

1. Introduction and Definitions

The purpose of this Data Processing Agreement is to establish necessary terms and conditions to meet the requirements the General Data Protection Regulation (EU) 2016/679 (the "**GDPR**"). Axis will process personal data on behalf of Data Controller, and Axis is hereby appointed as a 'data processor' to Data Controller in the meaning of the GDPR.

In the event of any conflict or inconsistency between this Data Processing Agreement and the Service Agreement regarding the processing of personal data, the provisions of this Data Processing Agreement shall prevail. Terms that are explicitly defined in the GDPR and used in this Data Processing Agreement, such as "controller", "processor", "personal data", "processing" and "data subject", shall be construed and applied in accordance with the meaning set out in the GDPR.

2. Lawful Processing

Axis shall process personal data in accordance with this Data Processing Agreement, the Service Agreement and Data Controller's documented instructions from time to time. Axis shall not process personal data for its own purposes or for any other purpose than what is set out in the Specification Annex. Axis may also process personal data if required to do so by Union or Member State law to which Axis is subject. Axis shall inform Data Controller of such legal requirement before processing personal data, unless the law prohibits such information.

3. Instructions

Data Controller's instructions to Axis related to processing of personal data are exhaustively set out in this Data Processing Agreement. Data Controller may provide additional written instructions to Axis (an "**Additional Instruction**"), and Axis has the corresponding obligation to follow such instructions, subject to this section 3 and provided that Data Controller reimburses Axis pursuant to section 11 below.

Notwithstanding the foregoing, Axis may reject an Additional Instruction if Axis deems that (i) an Additional Instruction infringes the GDPR or other Union or Member State data protection provisions, (ii) an Additional Instruction is unnecessary to fulfil GDPR requirements, or (iii) it is not technically possible or feasible for Axis to adhere to the Additional Instruction. In case of Axis' rejection of an Additional Instruction, Data Controller may terminate the relevant and affected parts of this Data Processing Agreement and the Service Agreement with a notice period of three (3) months.

4. Technical and Organisational Measures

Axis has implemented the technical and organisational measures set out in the Security Annex to ensure a level of security appropriate to the risks for rights and freedoms of natural persons posed by Axis' processing operations. Data Controller hereby confirms and approves that the measures described in the Security Annex are appropriate for Axis' processing of personal data under GDPR.

Axis shall ensure that only persons that need access to personal data in order to fulfil their work tasks as part of the Services have access to personal data, and that such persons are subject to appropriate confidentiality undertakings.

5. Data Transfers

In order to fulfil its obligations under the Service Agreement, Axis or its subcontractors may process personal data using infrastructure, equipment, subcontractors or resources that are located outside the EU/EEA, and/or otherwise transfer personal data outside the EU/EEA, provided that (i) Axis ensures a legal mechanism for the transfer in accordance with chapter V of the GDPR, such as entering into standard contractual clauses adopted by the EU Commission from time to time; and (ii) Axis implements appropriate and effective technical and organizational safeguards to protect the personal data.

6. Obligation to Provide Information and Assist Data Controller

Axis shall assist Data Controller by appropriate technical and organisational measures, for the fulfilment of Data Controller's obligations regarding personal data, such as assistance in responding to data subjects' requests and/or to rectify, erase, restrict and/or block the processing of personal data if so requested by Data Controller.

Axis undertakes to notify Data Controller in writing of any personal data breach without undue delay after the personal data breach is detected by Axis. Where, and in so far as, it is not possible to provide full and comprehensive information at the same time, Axis may provide the information in phases, provided that Axis (i) explains the reasons why full and comprehensive information cannot be provided, and (ii) provides any missing or outstanding information without unnecessary delay. The notification shall be sent to the designated contact in Data Controller's account in the Services, unless otherwise agreed in writing. Axis' notification of or response to a personal data breach will not constitute an acknowledgment of fault or liability with respect to the personal data breach. The obligations in this Section 6 do not apply to personal data breaches that the Data Controller is already aware of, such as personal data breaches caused by Data Controller or Users.

Axis shall also, upon Data Controller's request, assist Data Controller in fulfilling Data Controller's obligations on data protection impact assessments (where related to the Services, and only to the extent that Data Controller does not otherwise have access to the relevant information) and prior consultations.

7. Contact with Data Subjects and Supervisory Authorities

Axis shall notify Data Controller about any and all contacts with data subjects, supervisory authorities, and/or any other third party regarding Axis' processing of Data Controller's personal data. Axis does not have the right to represent Data Controller or in any other way act on behalf of Data Controller in relation to any data subject, supervisory authority or other third party. In the event that a data subject, supervisory authority, or any other third party requests information from Axis regarding processing of personal data on behalf of Data Controller, Axis shall (unless prohibited by law) refer such request to Data Controller and await further instructions.

8. Right to Audit

Axis shall provide Data Controller access to all available and necessary information to demonstrate that Axis has fulfilled its obligations under the GDPR. Axis shall also contribute to audits, including inspections, if and to the extent such audits are required to comply with mandatory law and/or conducted by a supervisory authority having authority over Data Controller' s operations.

Data Controller shall request an audit of Axis in writing at least thirty (30) days in advance; such request to include a comprehensive audit plan indicating what information and resources that Data Controller expects Axis to provide to support the audit. Any audit shall be (i) performed by an independent certified public accountant or the equivalent selected by Data Controller and acceptable to Axis, and (ii) carried out during normal business hours, and Data Controller shall take all necessary measures to minimize disturbances on Axis' business operations. Data Controller must reimburse Axis for its time expended in connection with an audit at Axis' standard hourly rates, which will be made available to Data Controller on request. In addition, Data Controller undertakes to ensure that every person who carries out the audit approves Axis' security policies and upon Axis' request, signs a confidentiality agreement with Axis. Axis shall under no circumstances be obliged to disclose information that is

confidential under law or agreement, nor Axis' trade secrets or other similar information. Data Controller must promptly disclose to Axis any written audit report created, and any findings of noncompliance discovered, as a result of the audit. Data Controller may not perform more than one audit in any 12-month period, except where required by a competent supervisory authority.

To the extent Axis can demonstrate Axis' compliance with the obligations set out in this DPA and the GDPR by providing written documentation, Data Controller undertakes, unless required by a competent supervisory authority, to primarily use and rely on such written documentation to satisfy Data Controller's need for information. If Data Controller can demonstrate that the written documentation provided by Axis is clearly insufficient, Data Controller may request an audit in accordance with the preceding paragraph.

9. Subcontractors

Data Controller hereby grants Axis a general written authorisation to engage subcontractors for processing of personal data. Upon Data Controller's request, Axis shall inform Data Controller of all engaged subcontractors and their geographic location. Furthermore, Axis shall inform Data Controller by way of posting an update on its webpage and/or by providing the relevant information in the relevant Service, of any plans to engage new or replace existing subcontractors, and thereby giving Data Controller the opportunity to object to such changes. Such objections by Data Controller shall be made in writing without undue delay from receipt of the information by Data Controller. Axis shall provide Data Controller with all information that Data Controller may reasonably request to assess whether the appointment of the proposed subcontractor complies with Data Controller's obligations under this DPA and the GDPR. If, in accordance with Data Controller's justifiable opinion, compliance with these obligations is not possible through the proposed subcontractor but the subcontractor is appointed by Axis, Data Controller is entitled to terminate the Service Agreement and this DPA at no extra cost (and notwithstanding anything to the contrary in the Service Agreement). If the objection is not justified, Data Controller is not entitled to terminate the Service Agreement or this DPA.

Axis shall enter into a data processing agreement with each subcontractor. Such agreement shall impose obligations on the subcontractor that are essentially the same and corresponding to Axis' obligations under this Data Processing Agreement.

10. Confidentiality

In addition to the confidentiality undertakings in the Service Agreement, Axis undertakes to not disclose personal data or otherwise reveal information about the processing of personal data to any third party without Data Controller's approval.

Axis shall ensure that each person who has access to personal data is subject to a written confidentiality undertaking.

The confidentiality undertaking above shall not prevent Axis from sharing personal data or information with subcontractors, provided that Axis has entered into a data processing agreement in accordance with section 9 above. Such data processing agreement shall however include a corresponding confidentiality obligation for the subcontractor.

If a competent authority requests information from Axis regarding the processing of personal data, Axis shall inform Data Controller thereof without undue delay. Axis may not act in any way on behalf of Data Controller or as its agent and may not transfer or otherwise disclose personal data or other information relating to the processing of personal data to third parties without the prior consent of Data Controller, unless it is required by GDPR or other Union or Member State data protection provisions or pursuant to a non-appealable decision by a competent court or authority.

11. Compensation

The Services are generally designed to enable Data Controller to comply with the GDPR without any additional work efforts from Axis, e.g. by means of built-in functionality to retrieve and delete user

data in the Services. If and to the extent Data Controller still requests Axis to perform work which is out-of-scope of the Services, Axis is entitled to charge and receive fair additional compensation in accordance with Axis' standard hourly rates (unless otherwise agreed). Without prejudice or limitation of the generality of the foregoing, this means that Axis may charge for the following efforts:

- To assess and, if applicable, adhere to and comply with Additional Instructions;
- To assist Data Controller in responding to requests from data subjects exercising their rights under the GDPR.
- To assist Data Controller with data protection impact assessments and prior consultation in accordance with section 6.
- To allow for and contribute to audits carried out by Data Controller in accordance with section 8.
- To assist Data Controller with transfers of personal data in connection with termination of the processing in accordance with section 12.

12. Termination of Processing of Personal Data

Unless another procedure for download/recovery of data in connection with termination of the Services Agreement is described in the Services Agreement, Axis shall upon termination of the Services Agreement (regardless of cause) at Axis' discretion either (i) transfer all personal data to Data Controller in a suitable manner and in format that Data Controller instructs; or (ii) permanently delete and erase all personal data and any existing copies thereof. Following such transfer or deletion, Axis shall ensure that personal data cannot be recovered by Axis.

13. Term

This Data Processing Agreement enters into force upon Data Controller's acceptance of the Services Agreement and shall remain in force for the duration of the Service Agreement and as long as Axis processes personal data (whichever is longer).

14. Governing Law and Dispute Resolution

This Data Processing Agreement is governed by the laws set out in the Services Agreement. Any dispute regarding the interpretation or application of this Data Processing Agreement shall be settled in accordance with the dispute resolution clause in the Service Agreement.

* * *

DATA SPECIFICATION ANNEX

Purposes and the subject-matter of the processing	Personal data shall be processed for Axis' provision of services according to the Service Agreement. Axis will solely process personal data for the purposes of providing the services to the Data Controller according to this Data Processing Agreement and the Service Agreement and as initiated by the Data Controller by use of the Services. Data Controller herby instructs Axis to process the personal data described below on behalf of Data Controller (as part of the Services).
Categories of Personal Data	The following categories of personal data will be collected and processed as part of the Services: IP addresses, contact information, etc. IP addresses Name Email License plate verifier data Images (when enabled) Video (when enabled) Audio (when enabled)
Categories of Data Subjects	The personal data will concern the following categories of data subjects: - Users of the Axis Technology - Customers employers and/or Customers customer
Duration of the Processing	Personal data will be retained and processed by Axis for the duration of the Services Agreement and as long as Data Controller has an active account in the Services. Thereafter, the personal data will be returned or deleted pursuant to section 12 in the Data Processing Agreement).
Technical and Organisational Security Measures	The Parties have agreed that the security measures stated in the Security Annex constitute appropriate technical and organisational security measures to protect personal data from accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access when transmitted, stored or otherwise processed.
Sub-processors	Axis may and will engage the sub-processors listed on End user license agreements | Axis Communications from time to time. Axis shall notify Data Controller of any changes to subcontractors in accordance with section 9 in the Data Processing Agreement.

SECURITY ANNEX

1. **Informational security – Organizational measures**

Axis will restrict the access to personal data to only a limited and needed target set of employees and contractors. The access is continuously reviewed and managed. If an employee or contractor is no longer actively working with the functionality dependant on the personal data, the access is immediately revoked.

To secure the information security, there are continuous security audits conducted on a per team basis. Each team will create and update a threat model of their respective software vertical. Potential vulnerabilities are classified and addressed, based on the risk they pose, using the Axis Security Development Model. This is a standardised practise within Axis that relies on one common process. The process is overlooked by a central group of persons (Software Security Group, SSG) that help spread knowledge and best practises to the rest of the teams, constantly educating and raising awareness on the topic of information security.

In addition to the threat modelling, there is the organizational backbone to address the vulnerabilities reported internally as well as externally. Axis is an approved Common Vulnerability and Exposures (CVE) Numbering Authority and identifies, discloses and patches vulnerabilities according to the international framework laid out by the global CVE-Program through the Axis Vulnerability Management Policy. Axis is also continuously reviewing what potential external certifications that could be of interest to further explain its information security story, based on an open certification standard. Axis has its own Security Operations Center that is carefully monitoring its IT systems for abnormalities.

2. **Informational security – Technical measures**

The Axis Security Development Model governs Axis initiated 3rd party vendor risk assessments on hardware and software components, outlines best practices for periodic vulnerability scanning on software components based on industry standard tools and orchestrate 3rd party security audits through yearly penetration testing and by facilitating a bug bounty program (vulnerability reward program). Constant monitoring of publicly available vulnerabilities and audit logging is in place to ensure best practices are followed.

3. **Information Security Policies and Procedures**

Axis will maintain information security policies and procedures designated to (i) help secure Personal Data against accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access when transmitted, stored or otherwise processed, (ii) identify reasonably foreseeable and internal risks to security and unauthorized access to the Services, and (iii) minimize security risks, including through risk assessment and regular testing.

4. **Network Security**

Axis maintains corrective action and incident response plans to respond to potential security threats. The Services handling the transport of personal data is end-to-end encrypted, based on industry standards (HTTPS/TLS RFC 2818/8446) and Axis prevents unauthorized access and eavesdropping to these resources or devices. It is at customers discretion to allow Axis employees explicit time-limited access to personal data, and devices for debugging purposes.

5. **Physical Security**

Axis takes responsibility for the physical security measures to protect personal data.

a. Physical access control

Physical components of the Sub-processor's data centre facilities, servers, networking equipment and host software systems (e.g., virtual firewalls) are housed in nondescript facilities (the "Facilities"). Physical barrier controls are used to prevent unauthorized entrance to the Facilities both at the perimeter and at building access points. Passage through the physical barriers at the Facilities requires either electronic access control validation or validation by human security personnel. Everyone entering a restricted zone needs to be authenticated using multi-factor identification to access a specific zone. Visitors are required to be always escorted by designated personnel. The Sub-processor only provides access to the Facilities to those employees and contractors who have a legitimate business need to access the Facilities.

b. Physical Security Protections

All access points (other than main entry doors) are maintained in a secured, locked state. The Facilities are monitored by video surveillance cameras, this includes the front and- back of each server rack. The Sub-processor also maintains electronic intrusion detection systems designed to detect unauthorized access to the facilities, including monitoring points of vulnerability with door contacts, grass breakage devices, interior motion detection, or other devices designed to detect individuals attempting to gain access to the Facilities. All physical access to the Facilities by employees and contractors is logged and routinely audited.