DATA PROCESSING ADDENDUM

This Data Processing Addendum ("DPA") is an agreement between Milestone Systems A/S ("Milestone") and Customer. This DPA supplements the Arcules Terms of Service ("Agreement"). Capitalized terms not otherwise defined herein will have the meanings given to them in the Agreement.

DEFINITIONS

In this DPA, the following definitions apply:

"Customer"	means the user of the Milestone cloud-based video management and access control Solution that has entered into the Agreement.
"Data Protection Legislation"	means, as applicable, the General Data Protection Regulation (EU 2016/679) and any national implementing laws, regulations and secondary legislation, as amended or updated from time to time, and specifically including without limitation national laws and regulations in Switzerland and the United Kingdom analogous to the General Data Protection Regulation (collectively, "European Data Protection Legislation"); current and future United States federal, state, and local laws, ordinances, regulations, and orders relating to privacy, data security, and the processing, storage, protection, and disclosure of Personal Information, including, but not limited to, the California Consumer Privacy Act ("CCPA"), California Privacy Rights Act ("CPRA"), Colorado Privacy Act , Virginia Consumer Data Protection Act , and other United States comprehensive consumer privacy laws and regulations (collectively, "US Data Protection Legislation"); and Japan's Act on the Protection of Personal Information ("APPI").
"Data Subject"	will have the meaning given to it in Data Protection Legislation and includes the term "consumer" as defined in US Data Protection Legislation".
"Personal Data"	means "personal data", as that term and analogous terms are defined in the Data Protection Legislation, that is uploaded to the Milestone Solution under Customer's Milestone account for processing by Milestone including without limitation closed-circuit television recordings.
"Standard Contractual Clauses"	means Appendix 1, attached to and forming part of this DPA if Customer elects to use the Milestone services in connection with the processing of Personal Data of Data Subjects located in the European Economic Area, Switzerland, and/or the United Kingdom as specified herein, pursuant to the European Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation

	(EU) 2016/679 of the European Parliament and of the Council and as supplemented by the UK International Data Transfer Addendum (if applicable).
"Sub-processor"	means any data processor other than Milestone who has been instructed to process Personal Data on behalf of the Customer by Milestone.

DATA PROTECTION REQUIREMENTS

1. Both parties will comply with all applicable requirements of Data Protection Legislation. This DPA is in addition to, and does not relieve, remove or replace, a party's obligations under Data Protection Legislation.

2. This DPA applies when Personal Data is processed by Milestone for Customer. In this context, Milestone will act as "processor" to Customer, who will act as "controller" with respect to Personal Data (as those terms and analogous terms are defined in Data Protection Legislation).

3. Details of Data Processing.

Subject matter. The subject matter of the data processing under this DPA is Personal Data, specifically, (i) closed-circuit television recordings of individuals and/or vehicles on Customer's premises (including video data and/or audio data), (ii) access control logs of individuals and/or vehicles accessing Customer's premises, (iii) access credentials and other Personal Data associated with Customer's Solution end-users, and (iv) other Personal Data provided by Customer in connection with the Solution.

Duration. As between Milestone and Customer, the duration of the data processing under this DPA is determined by Customer. Customer will determine the retention period(s) of Personal Data and inform Milestone of such periods from time to time or take steps to remove Personal Data from the Solution that is beyond its applicable retention period.

Purpose. The purpose of the data processing under this DPA is the provision of the Milestone Solution to Customer. The Milestone Solution will be used by Customer to archive, review, and analyse closed-circuit television recordings and access control logs to prevent or detect unlawful entry to Customer's premises, identify unlawful or non-compliant conduct by individuals on Customer's premises, monitor workplace performance, and calculate and analyse trends in the number of individuals and vehicles entering and existing Customer's premises. The purpose also includes processing as specified in Section 5.1.4.

Nature of the processing: computation, storage, and such other services as described in the Agreement and initiated by Customer from time to time, including without limitation storage, retrieval, and review of Personal Data such as closed-circuit television recordings, and analytics and algorithmic-based processing of closed-circuit television recordings and access control logs using Milestone's proprietary processes.

Categories of Data Subjects: the Data Subjects may include Customer's customers, employees, guests, invitees, suppliers, and end-users.

European Data Subjects: the Data Subjects may include individuals located in the European Economic Area, Switzerland, and/or the United Kingdom.

Special categories of data to be processed: none.

4. *Customer Obligations*.

4.1. Customer represents and warrants that it has, and covenants that it will maintain or obtain, all necessary appropriate consents and has provided all necessary notices, in any form required by Data Protection Legislation, to enable lawful transfer of the Personal Data to Milestone for the duration and purposes of the Agreement. If Customer uses the Milestone Solution in connection with Personal Data of European Data Subjects, Customer acknowledges the Guidelines 3/2019 on processing of personal data through video devices adopted 29 January 2020 by the European Data Protection Board.

4.2. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, Customer will ensure and warrants that Customer utilizes appropriate technical and organizational measures to ensure a level of security appropriate to such risks. The Milestone Solution may provide Customer with a number of controls, including security features and functionalities, that Customer may use to retrieve, correct, delete or restrict Personal Data; however, the provision of such controls, features, and functionalities does not relieve Customer of its obligation to ensure an appropriate security level.

4.3. Customer confirms that it has assessed any security measures in place at the time of this DPA, and that it will continue to do so on an ongoing basis to comply with its obligations under this DPA. Customer is solely responsible (as between the parties and to Data Subjects and supervisory authorities) if such measures fail to conform to the Data Protection Legislation.

4.4. Customer may reasonably monitor and audit Milestone's processing of Personal Data for compliance with this DPA and Data Protection Legislation and Milestone will reasonably cooperate with such monitoring and auditing. If Customer requests to visit an Milestone facility as part of such an audit, Customer may make only one such request per twelve (12) month period and must provide at least thirty (30) days advance written notice to Milestone of Customer's intent to visit. While in the Milestone facility, Customer will abide by all instructions and directions of Milestone's personnel and will use reasonable efforts to minimize the disruption of Customer's visit to Milestone's day-to-day business operations.

4.5. Customer undertakes and confirms that any information required to be provided to a Data Subject has been so provided or an applicable exemption is available and is being relied upon by the Customer.

4.6. Customer will immediately notify Milestone if any necessary appropriate consents and notices required to enable lawful transfer of Personal Data to Milestone for the duration and purposes of this DPA have been breached, terminated, or are otherwise no longer valid.

4.7. Customer is responsible for ensuring the security of transfers of Personal Data to Milestone and Milestone only assumes obligations as a data processor on receipt by Milestone of Personal Data from Customer.

5. *Milestone Obligations*.

5.1. Milestone will retain, process, or disclose Personal Data only on the written instructions of Customer, as necessary for Milestone to provide the Solution or fulfil its obligations under the Agreement, as necessary for Milestone to comply with applicable laws and regulations, or as otherwise permitted under this DPA.

5.2. Milestone understands and agrees that it will not (i) sell Personal Data to any third party, or (ii) retain, use, or disclose Personal Data outside of the direct business relationship between Milestone and Customer. If a governmental body sends Milestone a demand for Personal Data, Milestone will attempt to redirect the governmental body to request that data directly from Customer. As part of this effort, Milestone may provide Customer's basic contact information to the government body. If legally required to disclose Personal Data to a government body, then Milestone will give Customer reasonable notice of the demand to allow Customer to seek a protective order or other appropriate remedy unless Milestone is legally prohibited from doing so.

5.3. To the extent prohibited by Data Protection Legislation, Milestone will not combine Personal Data it processes on behalf of Customer with personal data or personal information it processes on behalf of itself or a third party.

5.4. Milestone may, and Customer directs Milestone to, process Personal Data for the purpose of improving the Solution including, without limitation, processing Personal Data for the purpose of machine learning to train analytic engines to better identify and analyze individuals and objects appearing in data sets. Customer understands and agrees that Personal Data utilized for these purposes will be retained by Milestone as part of a machine learning data set associated with the Solution as provided to Customer and to Milestone's other customers, and it will not be capable of deletion or return to Customer. Upon Customer's provision of the Personal Data processed for these purposes to Milestone, Customer provides a limited, sublicensable (through multiple tiers), assignable, transferrable, irrevocable, royalty-free license to Milestone for Milestone to process, retain, and disclose such Personal Data in connection with improving the Solution including, without limitation, as part of machine learning training data sets. Customer represents and warrants that it has, and covenants that it will maintain or obtain, all necessary and appropriate consents and has provided all necessary notices, in any form required by Data Protection Legislation, to enable lawful transfer of the Personal Data to Milestone for the foregoing purposes. Customer may by written notice to Milestone direct Milestone to process Personal Data for machine learning purposes strictly with regard to improving the Solution as provided to Customer and, in such instance, Personal Data received for processing for such purpose after Customer's notice will be deleted or returned to Customer at termination of the Agreement. For avoidance of doubt and not limitation, Customer's notice will not modify, alter, or restrict Milestone's ability to process Personal Data received by Milestone prior to the date of Customer's notice even if such processing occurs after the date of Customer's notice.

5.5. Milestone will implement commercially reasonable technical, physical, and organisational measures to protect against unauthorised or unlawful processing of Personal Data and against accidental loss or destruction of, or damage to, Personal Data, appropriate to the harm that might result from the unauthorised or unlawful processing or accidental loss, destruction or damage and the nature of the data to be protected, and having regard to the state of technological development and the cost of implementing any measures.

5.6. Milestone will ensure that all Milestone personnel who have access to and/or process Personal Data are obliged to keep the Personal Data confidential.

5.7. Milestone will maintain records of its processing activities carried out on behalf of Customer as required by Data Protection Legislation.

5.8. Milestone will reasonably assist the Customer in responding to any request from a Data Subject and in ensuring compliance with Customer's obligations under Data Protection Legislation with respect to security, breach notifications, data protection impact assessments, cybersecurity audits, and consultations with supervisory authorities or regulators.

5.9. Milestone will notify Customer without undue delay upon having actual knowledge of a Personal Data security incident. For purposes of this DPA, a "security incident" shall mean the unauthorised or unlawful processing of Personal Data or the accidental loss or destruction of, or damage to, Personal Data. Milestone is not obligated to report security incidents that do not result in unauthorized access to Personal Data by a third party or to any of Milestone's equipment or facilities storing Personal Data by a third party, and such unreportable incidents may include, without limitation, pings and other broadcast attacks on firewalls or edge servers, port scans, unsuccessful log-on attempts, denial of service attacks, packet sniffing (or other unauthorized access to traffic data that does not result in access beyond headers), or similar incidents. Milestone's obligation to report or respond to a security incident under this section is not and will not be construed as an acknowledgement by Milestone of any fault or liability of Milestone with respect to the incident.

5.10. Milestone will, at the written direction of Customer, delete or return Personal Data and all copies thereof (excepting copies retained in archive or backup systems) to Customer on termination of the Agreement unless it is required by applicable law to continue to store the Personal Data.

5.11. If Milestone will process the Personal Data of individuals located in the European Economic Area, Switzerland, and/or the United Kingdom, it will ensure that where Personal Data is transferred outside the European Economic Area, Switzerland, and/or the United Kingdom adequate measures are taken to ensure the Personal Data will be protected to an adequate level and the Data Subjects' rights under the Data Protection Legislation will not be prejudiced by such a transfer. Milestone will maintain compliance with the EU-U.S. Data Privacy Framework, including the UK Extension and the Swiss-U.S. Data Privacy Framework (collectively, the "DPF"). If the DPF is invalidated by a competent legal authority, or Milestone's participation in the DPF lapses, the Standard Contractual Clauses attached hereto as Appendix 1 will apply to Personal Data of European Data Subjects that is transferred outside the European Economic Area, Switzerland, and/or the United Kingdom, either directly or via onward transfer, to Milestone in any country not recognized by the European Commission or the UK Secretary of State (as applicable) as providing an adequate level of protection for personal data (as described in the Data Protection Legislation). In the event of a conflict between the Standard Contractual Clauses and the remainder of this DPA, the Standard Contractual Clauses will control.

5.12. If Milestone will process the Personal Data of individuals located in the European Economic Area, Switzerland, and/or the United Kingdom, Milestone may provide Customer with the option to select a data center in the European Economic Area as the primary storage location of Personal Data Customer controls; however,

Customer acknowledges and agrees that Milestone may transfer, store, and/or process Personal Data in the United States of America and other third countries in accordance with Section 5.1.11.

5.13. If Milestone determines that it is unable to comply with this DPA or Data Protection Legislation, Milestone will provide prompt written notice of its determination to Customer. Upon receipt of such notice, Customer may take reasonable steps to stop and/or remediate Milestone's noncompliance.

5.14. If Milestone will process Personal Data subject to the APPI, Appendix 2 will apply to such processing. In the event of a conflict between Appendix 2 and this DPA, the terms of Appendix 2 will control with regard to such processing.

6. *Sub-Processors*. Customer agrees that Milestone may use Sub-processors to fulfill its contractual obligations under this DPA or to provide certain services on its behalf, such as providing support services, and consents to the use of Sub-processors as described in this section. A list of Sub-processors that are currently engaged by Milestone to carry out processing activities on Personal Data on behalf of Customer can be found at arcules.com/subprocessors. At least 7 calendar before Milestone engages any new Sub-processor to carry out processing activities on Personal Data on behalf of Customer, Milestone will update the applicable website and provide Customer with a mechanism to obtain notice of that update. If Customer objects to a new Sub-processor, Customer must notify Milestone in writing within 7 calendar days of notice of the updated website (without prejudice to any termination rights Customer has under the Agreement).

7. *Revisions*. Milestone may, at any time on not less than 30 days' notice, propose revisions to this DPA, which will become effective if Customer does not object to such revisions in writing to Milestone prior to the effective date of the revisions. Customer and Milestone will negotiate such objected to revisions in good faith. If Customer and Milestone are not able to reach agreement on such revisions after reasonable negotiations, Customer may terminate the Agreement immediately upon written notice Milestone.

8. *Controlling Document*. In the event of a conflict between this DPA and the Agreement, this DPA will control.

Last revised: February 10, 2025

Appendix 1: Standard Contractual Clauses (controller to processor transfer)

This Appendix applies solely in the event and to the extent that Customer uses the Milestone Solution to process the Personal Data of individuals located in the European Economic Area, Switzerland, and the United Kingdom.

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 8.1(b), 8.9(a), (c), (d) and (e);

(iii) Clause 9(a), (c), (d) and (e);

(iv) Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18(a) and (b).

(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

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 organizational 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 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 organizational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized 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 pseudonymization, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymization, 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 organizational 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 authorized 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:

(i) 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;

(ii) 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;

(iii) 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

(iv) 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) The data importer has the data exporter's general authorization 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 7 calendar days 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. The Parties agree that, by complying with this Clause, the data importer fulfils 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 fulfil 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 authorized 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 organizational 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 authorized to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(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) 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.

(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 authorizing 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 authorizing 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 organizational 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).

(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 fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. 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 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.).

(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 minimization

(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.

(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): The data exporter is the Customer as defined in the Agreement.

Data importer(s): The data importer is Milestone as defined in the Agreement.

B. DESCRIPTION OF TRANSFER

The Personal Data transferred, categories of Data Subjects subject to the transfer, nature of the processing, and duration of processing, including retention of the Personal Data is as described in the body of the DPA.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority will be the supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer.

ANNEX II

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

Milestone has implemented numerous technical and organizational measures designed to support security of the Personal Data processed by Milestone. These measures are documented in Milestone's SOC2 report which Milestone will make available to Customer upon request.

Addendum to Appendix 1

This Addendum to Appendix 1 applies solely in the event and to the extent that Customer uses the Milestone Solution to process the Personal Data of individuals located in the United Kingdom.

Part 1: Tables

Table 1: Parties

Start Date: The date on which Customer enters into the Agreement.

Exporter: The Customer.

Importer: Milestone Systems A/S, Banemarksvej 50, DK-2605 Brøndby, Denmark

Table 2: Selected SCCs, Modules and Selected Clauses

This Addendum is appended to the version of the Approved EU SCCs appearing above as promulgated in Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council.

Table 3: Appendix Information

"**Appendix Information**" means the information which must be provided for the selected modules as set out in the Appendix of the Approved EU SCCs (other than the Parties), and which for this Addendum is set out in:

Annex 1A: List of Parties: See Annex 1A.
Annex 1B: Description of Transfer: See Annex 1B
Annex II: Technical and organisational measures including technical and organisational measures to ensure the security of the data: See Annex II
Annex III: List of Sub processors (Modules 2 and 3 only): The data importer has the data exporter's general authorisation for the engagement of sub-processors from an agreed list

and to provide notice of changes prior to the engagement of new or replaced sub-processors.

Table 4: Ending this Addendum when the Approved Addendum Changes

Ending this Addendum when the Approved Addendum changes	Which Parties may end this Addendum as set out in Section 0: ☒ Importer ☒ Exporter ☐ neither Party

Part 2: Mandatory Clauses

Entering into this Addendum

Each Party agrees to be bound by the terms and conditions set out in this Addendum, in exchange for the other Party also agreeing to be bound by this Addendum.

Although Annex 1A and Clause 7 of the Approved EU SCCs require signature by the Parties, for the purpose of making Restricted Transfers, the Parties may enter into this Addendum in any way that makes them legally binding on the Parties and allows data subjects to enforce their rights as set out in this Addendum. Entering into this Addendum will have the same effect as signing the Approved EU SCCs and any part of the Approved EU SCCs.

Interpretation of this Addendum

Where this Addendum uses terms that are defined in the Approved EU SCCs those terms shall have the same meaning as in the Approved EU SCCs. In addition, the following terms have the following meanings:

Addendum	This International Data Transfer Addendum which is made up of this Addendum incorporating the Addendum EU SCCs.
Addendum EU SCCs	The version(s) of the Approved EU SCCs which this Addendum is appended to, as set out in Table 2, including the Appendix Information.
Appendix Information	As set out in Table 3.

Appropriate Safeguards	The standard of protection over the personal data and of data subjects' rights, which is required by UK Data Protection Laws when you are making a Restricted Transfer relying on standard data protection clauses under Article 46(2)(d) UK GDPR.
Approved Addendum	The template Addendum issued by the ICO and laid before Parliament in accordance with s119A of the Data Protection Act 2018 on 2 February 2022, as it is revised under Section 0.
Approved EU SCCs	The Standard Contractual Clauses set out in the Annex of Commission Implementing Decision (EU) 2021/914 of 4 June 2021.
ICO	The Information Commissioner.
Restricted Transfer	A transfer which is covered by Chapter V of the UK GDPR.
UK	The United Kingdom of Great Britain and Northern Ireland.
UK Data Protection Laws	All laws relating to data protection, the processing of personal data, privacy and/or electronic communications in force from time to time in the UK, including the UK GDPR and the Data Protection Act 2018.
UK GDPR	As defined in section 3 of the Data Protection Act 2018.

This Addendum must always be interpreted in a manner that is consistent with UK Data Protection Laws and so that it fulfils the Parties' obligation to provide the Appropriate Safeguards.

If the provisions included in the Addendum EU SCCs amend the Approved SCCs in any way which is not permitted under the Approved EU SCCs or the Approved Addendum, such amendment(s) will not be incorporated in this Addendum and the equivalent provision of the Approved EU SCCs will take their place.

If there is any inconsistency or conflict between UK Data Protection Laws and this Addendum, UK Data Protection Laws applies.

If the meaning of this Addendum is unclear or there is more than one meaning, the meaning which most closely aligns with UK Data Protection Laws applies.

Any references to legislation (or specific provisions of legislation) means that legislation (or specific provision) as it may change over time. This includes where that legislation (or

specific provision) has been consolidated, re-enacted and/or replaced after this Addendum has been entered into.

Hierarchy

Although Clause 5 of the Approved EU SCCs sets out that the Approved EU SCCs prevail over all related agreements between the parties, the parties agree that, for Restricted Transfers, the hierarchy in Section 0 will prevail.

Where there is any inconsistency or conflict between the Approved Addendum and the Addendum EU SCCs (as applicable), the Approved Addendum overrides the Addendum EU SCCs, except where (and in so far as) the inconsistent or conflicting terms of the Addendum EU SCCs provides greater protection for data subjects, in which case those terms will override the Approved Addendum.

Where this Addendum incorporates Addendum EU SCCs which have been entered into to protect transfers subject to the General Data Protection Regulation (EU) 2016/679 then the Parties acknowledge that nothing in this Addendum impacts those Addendum EU SCCs.

Incorporation of and changes to the EU SCCs

This Addendum incorporates the Addendum EU SCCs which are amended to the extent necessary so that:

a. together they operate for data transfers made by the data exporter to the data importer, to the extent that UK Data Protection Laws apply to the data exporter's processing when making that data transfer, and they provide Appropriate Safeguards for those data transfers;

b. Sections 0 to 0 override Clause 5 (Hierarchy) of the Addendum EU SCCs; and

c. this Addendum (including the Addendum EU SCCs incorporated into it) is (1) governed by the laws of England and Wales and (2) any dispute arising from it is resolved by the courts of England and Wales, in each case unless the laws and/or courts of Scotland or Northern Ireland have been expressly selected by the Parties.

Unless the Parties have agreed alternative amendments which meet the requirements of Section 0, the provisions of Section 0 will apply.

No amendments to the Approved EU SCCs other than to meet the requirements of Section 0 may be made.

The following amendments to the Addendum EU SCCs (for the purpose of Section 0) are made:

a. References to the "Clauses" means this Addendum, incorporating the Addendum EU SCCs;

b. In Clause 2, delete the words:

"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";

c. Clause 6 (Description of the transfer(s)) is replaced with:

"The details of the transfers(s) and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred) are those specified in Annex I.B where UK Data Protection Laws apply to the data exporter's processing when making that transfer.";

d. Clause 8.7(i) of Module 1 is replaced with:

"it is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer";

e. Clause 8.8(i) of Modules 2 and 3 is replaced with:

"the onward transfer is to a country benefitting from adequacy regulations pursuant to Section 17A of the UK GDPR that covers the onward transfer;"

f. References to "Regulation (EU) 2016/679", "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)" and "that Regulation" are all replaced by "UK Data Protection Laws". References to specific Article(s) of "Regulation (EU) 2016/679" are replaced with the equivalent Article or Section of UK Data Protection Laws;

g. References to Regulation (EU) 2018/1725 are removed;

h. References to the "European Union", "Union", "EU", "EU Member State", "Member State" and "EU or Member State" are all replaced with the "UK";

i. The reference to "Clause 12(c)(i)" at Clause 10(b)(i) of Module one, is replaced with "Clause 11(c)(i)";

j. Clause 13(a) and Part C of Annex I are not used;

k. The "competent supervisory authority" and "supervisory authority" are both replaced with the "Information Commissioner";

l. In Clause 16(e), subsection (i) is replaced with:

"the Secretary of State makes regulations pursuant to Section 17A of the Data Protection Act 2018 that cover the transfer of personal data to which these clauses apply;";

m. Clause 17 is replaced with:

"These Clauses are governed by the laws of England and Wales.";

n. Clause 18 is replaced with:

"Any dispute arising from these Clauses shall be resolved by the courts of England and Wales. A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of any country in the UK. The Parties agree to submit themselves to the jurisdiction of such courts."; and

o. The footnotes to the Approved EU SCCs do not form part of the Addendum, except for footnotes 8, 9, 10 and 11.

Amendments to this Addendum

The Parties may agree to change Clauses 17 and/or 18 of the Addendum EU SCCs to refer to the laws and/or courts of Scotland or Northern Ireland.

If the Parties wish to change the format of the information included in Part 1: Tables of the Approved Addendum, they may do so by agreeing to the change in writing, provided that the change does not reduce the Appropriate Safeguards.

From time to time, the ICO may issue a revised Approved Addendum which:

a. makes reasonable and proportionate changes to the Approved Addendum, including correcting errors in the Approved Addendum; and/or
b. reflects changes to UK Data Protection Laws;

The revised Approved Addendum will specify the start date from which the changes to the Approved Addendum are effective and whether the Parties need to review this Addendum including the Appendix Information. This Addendum is automatically amended as set out in the revised Approved Addendum from the start date specified.

If the ICO issues a revised Approved Addendum under Section 0, if any Party selected in Table 4 "Ending the Addendum when the Approved Addendum changes", will as a direct result of the changes in the Approved Addendum have a substantial, disproportionate and demonstrable increase in:

a its direct costs of performing its obligations under the Addendum; and/or

b its risk under the Addendum,

and in either case it has first taken reasonable steps to reduce those costs or risks so that it is not substantial and disproportionate, then that Party may end this Addendum at the end of a reasonable notice period, by providing written notice for that period to the other Party before the start date of the revised Approved Addendum.

The Parties do not need the consent of any third party to make changes to this Addendum, but any changes must be made in accordance with its terms.

Appendix 2

個人情報保護に関する措置の確認書
Written confirmation

_____社が取得し、Milestone Systems A/S.へ提供するユーザーの個人情報の取扱いについて、以下の措置を講じていることに相違ありません。
Regarding the handling of personal information of users obtained by Customer and provided to Milestone Systems A/S, There is no difference in that the following measures have been taken.

利用目的の特定と制限 Identification and Restriction of Purpose of Use	個人情報は下記利用目的のみに利用し、その他の目的には利用しない。 利用目的:契約および契約製品に関わるサービス、サポートの提供 Personal information shall be used only for the following purposes and shall not be used for other purposes. Purpose of Use: Provision of services and support related to contracts and contractual products
不適正な利用の禁止 Prohibition of improper use	個人情報は、適切に取り扱い、違法または不当な行為につながる利用をしない。 Personal information shall not be handled inappropriately or used in a manner that leads to illegal or improper conduct.
データ内容の正確性の確保 Security related to the accuracy of data contents	個人情報の利用目的の達成に必要な範囲内において、個人情報を正確かつ最新の内容に保つとともに、利用する必要がなくなったときは、当該個人データを遅滞なく消去する。 Personal Information shall be kept accurate and up-to-date to the extent necessary for the achievement of the Purpose of Use of Personal Information, and if it is no longer necessary to use such Personal Information, such Personal Information shall be deleted without delay.
安全管理措置 Security Control Measures	取り扱う個人情報の安全管理のために必要かつ適切な措置を講じる Take necessary and appropriate measures to safely manage personal information handled
従業者の監督 Supervision of Employees	個人情報を取り扱う従業員に対して、個人情報の安全管理が図られるよう、必要かつ適切な監督を行う。 Provide necessary and appropriate supervision to employees handling personal information in order to ensure the safe management of personal information.
委託先の監督 Supervision of Trustees	※先に委託先有無を確認し、該当する場合のみを記載 委託先無の場合:委託先は無し。 委託先有の場合:委託先に対して必要かつ適切な監督を行う。 ※Confirm the presence or absence of outsourcer first, and state only if applicable. No outsourcee: No outsourcee. In the case of an entrusted company: Provide necessary and appropriate supervision to the entrusted company.
第三者提供の制限 Restriction of Provision to A Third Party	第三者への提供は行わない。 Do not provide to a third party.
漏えい等の報告等 Report of Leakage, etc.	・日本の個人情報保護法において、個人情報保護委員会への報告が義務付けられている漏洩等が発生した場合は、個人情報保護委員会への即時報告と本人通知の対応をおこなう。 ・本人の数が 1000 人を超える個人情報の漏洩または発生したおそれ ・不正の目的をもって行われたおそれのある個人情報の漏えい(サイバー攻撃など) ・In the event of a leak, etc., which is required to be reported to the Personal Information Protection Committee under the Privacy Protection Law of Japan, the Company shall immediately report to the Personal Information Protection Committee and respond to such information by notifying the Personal Information Protection Committee. ・Leakage or possible occurrence of personal information of more than 1000 persons ・Leakage of personal information (cyber attacks, etc.) that may have been committed with unauthorized purposes