MAKE THE
WORLD SEE

Date: January 3, 2023

Milestone Kite™ Terms of Service

Data Processing Addendum

milestone

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

between

Customer as identified by the Customer itself in its request for the Milestone Kite cloud based video management and access control solution (also referred to as "You" in the Milestone Kite Terms of Service) and in that relation having accepted the Milestone Kite Terms of Service, cf. www.milestonesys.com/kite-terms-service

(the data controller)

and

Milestone Systems A/S
CVR 20341130
Banemarksvej 50
2605 Brøndby
Denmark

(the data processor)

each a 'party'; together 'the parties'

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

Table of Content

1. Preamble

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller. These Clauses take effect from the date the Milestone Kite Terms of Service (the "Agreement") has been accepted by the data controller or from the date the data controller has started to access and use the Milestone Kite cloud based video management and access control solution (in the Agreement it is also referred to as the Solution).

2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 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 and repealing Directive 95/46/EC (General Data Protection Regulation). If the data controller has no establishment in the European Union or the EEA for the purposes of the processing activity and the processing activity does not fall under the territorial scope of the GDPR as per Article 3(2) GDPR, the data processor's obligations in the Clauses shall be interpreted and limited to take into account that the data controller is not subject to obligations under the GDPR.

3. In the context of the provision of Milestone Kite – a cloud based video management and access control solution– in accordance with the Agreement, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties. For the avoidance of doubt the SCC's referred to in Clause 1.10 and attached as Appendix E shall take priority over the Clauses.

5. Five appendices are attached to the Clauses and form an integral part of the Clauses.

6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

9. Appendix D contains provisions for other activities which are not covered by the Clauses.

10. If the data controller is established in a non-EEA country which has not been deemed by the EU Commission to provide adequate protection of personal data through an adequacy decision, the parties by virtue of accepting this Data Processing Agreement agree to be bound by the Standard Contractual Clauses (SCC's) for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council – module 4 (P2C) (COMMISSION IMPLEMENTING DECISION (EU) 2021/914 of 4 June 2021) as attached as Appendix E.

11. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

12. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

2. The rights and obligations of the data controller

1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State data protection provisions and the Clauses.

2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

3. The data processor acts according to instructions

1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions. The data controller shall then assess without undue delay whether the instructions given by the data controller, contravene the GDPR or the applicable EU or Member State data protection provisions. The parties shall agree in the specific situation whether the data processor shall continue to comply with the instructions given by the data controller on the processing of personal data or whether the processing shall be suspended until the data controller has investigated the matter further. Notwithstanding the foregoing, the data processor will not have liability to the data controller for actions taken by data processor in reliance upon the data controller's instructions.

4. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

5. Security of processing

1. Article 32 GDPR stipulates that, 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, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

2. The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

    a. Pseudonymisation and encryption of personal data;

    b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

    c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

    d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

3. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

4. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

5. If subsequently – in the assessment of the data controller – mitigation of the identified risks requires further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

6. Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

2. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 1 month in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

3. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

4. The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

5. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

6. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

7. Transfer of data to third countries or international organisations

1. Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

2. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

a. transfer personal data to a data controller or a data processor in a third country or in an international organization

b. transfer the processing of personal data to a sub-processor in a third country

c. have the personal data processed in by the data processor in a third country

4. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

8. Assistance to the data controller

1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

   This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

   a. the right to be informed when collecting personal data from the data subject

   b. the right to be informed when personal data have not been obtained from the data subject

   c. the right of access by the data subject

   d. the right to rectification

   e. the right to erasure ('the right to be forgotten')

   f. the right to restriction of processing

   g. notification obligation regarding rectification or erasure of personal data or restriction of processing

   h. the right to data portability

   i. the right to object

   j. the right not to be subject to a decision based solely on automated processing, including profiling

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 5.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

   a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, in the EEA Member state in which the data controller is established,

unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

b. the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

c. the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

d. the data controller's obligation to consult the competent supervisory authority, in the EEA Member state in which the data controller is established, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 8.1. and 8.2.

9. Notification of personal data breach

1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

2. The data processor's notification to the data controller shall, if possible, take place within 48 hours after the data processor has become aware of the personal data breach, through its own observation or from information received from its sub-processor, to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

3. In accordance with Clause 8(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3) GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

a. The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b. the likely consequences of the personal data breach;

c. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

10. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so or if specifically instructed by the data controller on the time of termination to return all the personal data to the data controller and delete existing copies unless Union or Member State law requires storage of the personal data.

11. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in Appendix C.7.

3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

12. The parties' agreement on other terms

1. The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g., liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

13. Commencement and termination

1. The Clauses shall become effective on the date of the data controller's acceptance of the Milestone Kite Terms of Service, or on the date the data controller has started to access and use the Solution.

2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 10.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

Appendix A Information about the processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

To make available to the data controller the data processor's cloud based video management and access control solution (Milestone Kite or Solution as referred to in the Agreement) to enable the data controller to remotely access surveillance cameras connected by the data controller to the Solution at one or more sites designated by the data controller and to enable the data controller to monitor live video, and manage, store, retrieve, play-back, review and analyse video recordings from the data controller's cameras.

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

Transmission, receipt and storage of live feeds and recordings from the data controller's cameras and providing access to such recordings to the data controller and allowing the data controller to administer and analyse recordings by tools available in the Solution. Ultimately returning or deleting recordings.

A.3. The processing includes the following types of personal data about data subjects:

Image and behaviour of individuals captured and recorded by the data controller's surveillance cameras. Images of objects that may include personal data, e.g., license plates of cars. The Solution allows the data controller to include authorisations, event and identification data related to the surveillance, and the Solution includes certain free text fields to be used at the data controller's discretion.

The Solution also holds personal data of registered users of the Solution, like email, name, phone number, etc. The data controller acknowledges that the data processor is a data controller in its own right when collecting and using such data for the purpose of the Solution, including emails and other communication regarding the Solution, e.g., planned downtimes, features releases, account management, or other aspects of the Solution, cf. Section 1.6 of the Agreement. Personal data of registered users of the Solution is therefore not covered by these Clauses.

A.4. Processing includes the following categories of data subject:

Individuals and individuals associated with objects appearing in live feed and recordings, which may be the data controller's employees, guests, invitee's, customers, and suppliers etc.

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

Until termination of the Agreement.

Appendix B Authorised sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

NAME	CVR	ADDRESS	DESCRIPTION OF PROCESSING
Arcus Holding A/S	CVR 38330365	C/O Milestone Systems A/S Banemarksvej 50 2605 Brøndby	Supplier of the Solution and related tools used in processing.
Arcules, Inc.		17875 Von Karman Ave. Suite 450, Irvine California 92614 USA	Supplier of the Solution and related tools used in processing. Storage of video recordings via sub-processor.
Sub-processor to Arcules, Inc: Google, LLC	EIN: 770493581 Delaware Corp #: 3582691 VAT: EU372000041	1600 Amphitheatre Parkway, Mountain View, CA 94043	Storage of video recordings in cloud in the geographical region designated by the data controller.

The data controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

B.2. Prior notice for the authorisation of sub-processors

As established in Clause 6.2.

Appendix C Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

Cloud based video management and access control solution

When making available to the data controller the data processor's Solution, the data processor shall:

a. Make the Solution available to the data controller including processing tools designated by the data controller at set-up.

b. Facilitate transmission and recording of live video from the data controllers' connected cameras to the Solution using appropriate security measures to protect against loss, unauthorised disclosure of, or access to data transmitted and stored.

c. Store data and enable the data controller to make use of the Solution and the processing tools designated by the data controller at set-up, including to retrieve, search in, review, analyse and delete content by use of tools available to the data controller in the Solution.

d. Host data in a cloud based platform located within the geographical region instructed by the data controller at the time of entering into the Agreement.

e. Ensure that the transmitted content data are encrypted during transmission to the Solution and at rest in the Solution.

If the data controller issues instructions to the data processor (including without limitation, changing the location of the cloud based platform or changing any aspect of the Solution to adjust data flows), and such instructions would prevent or limit the data processor's ability to provide the Solution, or require material or costly changes to it, the data processor may limit or adjust or terminate the subscription accordingly without obligation to the data controller and without any right for the data controller to claim damages, refunds, or any compensation.

For the purpose of clarity, the data controller is responsible for its lower layer internet connectivity, while the data processor is responsible for the communication between the Gateway and the Solution on application level. The use of the Solution requires transmission of data over the Internet and through networks that are not owned, operated or controlled by the data processor, and, respectively, the data processor is not responsible for any of data lost, altered, intercepted or stored across those networks.
Technical, analytical and forensic support.

The data controller acknowledges that the data processor is a data controller in its own right when providing technical, analytical and forensic support to the data controller. Support provided to the data controller is therefore not covered by these Clauses.

Technical, analytical and forensic support may be provided by the sub-processor Arcules, cf. Appendix B.1. on behalf of the data processor. The data controller is encouraged to only give the data processor access to personal data to the extent required for the provision of support and to ensure it has a lawful basis to do so. When providing support to the data controller, the data processor shall:

a. Only access content data as required to provide support to the data controller and only when requested by the data controller.

b. Only access data through a customer account generated for the purpose containing specific material/recordings or by receiving a screenshot or closed-circuit television recording from the data controller.

c. Delete all content data once the support request is completed.

The Solution allows the data controller to improve the analytic tools applied to the data controller's data. The data controller acknowledges that this requires the data controller to transfer permanently and irrevocably data (e.g., video frames etc.) to the data processor and its sub-processor Arcules, cf. Appendix B.1. to add such data to the training set used for the Solution. The data processor and the sub-processor will act as data controllers in their own right for this processing. The data controller is encouraged to only transfer personal data to the extent required for the purpose and to ensure it has a lawful basis to do so.

C.2. Security of processing

The data processor shall implement technical and organisational measures to ensure an appropriate level of security to adequately protect data during transmission, storage and processing.

The data processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security.

The data processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the data controller:

a. In connection with platform security the data processor has implemented the following measures:

   - No default logins
   - Single sign-on (SSO/SAML)
   - Granular user permission
   - Seamless automatic updates
   - Multi-factor authentication (MFA) via SAML

b. In connection with network security the data processor has implemented the following measures:

   - Encryption in transit and data is transmitted utilizing TLS 1.2 or greater
   - Outbound traffic only
   - Secure by default as the gateway will refuse to connect to external devices using their factory default credentials
   - Package signing where each package of code deployed to the host is signed secret signature

Security measures implemented by the cloud provider are accessible here: https://cloud.google.com/terms/data-processing-addendum.

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 8.1. and 8.2. by implementing the following technical and organisational measures:

a. Internal organisation

- In the context of its assistance to the data controller, the data processor shall establish an internal organisation responsible for ensuring that the data processor complies with its obligations to the data controller.
- The data processor has named a contact person or facility to respond to requests from the data controller.
- The data processor shall keep a record of processing activities in accordance with Article 30 GDPR describing the processing activities carried out by the data processor on behalf of the data controller.

b. Data subject requests

- The data processor shall, without undue delay, after having been made aware of it, inform the data controller in writing (email acceptable) of any request addressed to the data processor by a data subject to exercise his or her rights under the GDPR and the applicable EU or Member State data protection provisions related to the data processor's processing activities on behalf of the data controller.
- The data processor shall not be entitled to respond to requests from a data subject.
- The data processor shall, at the request of the data controller, and to the extent the data controller cannot itself comply with data subject requests by the tools available in the Solution, reasonably assist in fulfilling the data controller's obligations.

c. Notification of data breach

- The assistance of the data processor in relation to the obligations of the data controller under Articles 33 and 34 GDPR shall be provided by the data processor providing the information referred to in Clause 9.3 to the data processor within the time limit referred to in Clause 9.2.
- The data processor shall subsequently assist the data controller by providing to the data controller, at the data controller's request, the information necessary for the data controller to notify the competent supervisory authority of a personal data breach or necessary for the data controller to notify the data subject.

C.4. Storage period/erasure procedures

Storage periods are defined by the data controller in the set-up of the Solution. Data may be deleted by the data controller whenever the data controller chooses to do so.

Upon termination of the provision of personal data processing services, the data processor shall either delete or return the personal data in accordance with Clause 10.1. hereof and Section 5.3 of the Agreement.

If the subscription has not been renewed before the end of the data controller's current subscription term, the data controller is solely responsible for the data (including "Your Content" as referred to in the

Agreement) and for all related expenses. The data controller is solely responsible for retrieval of the data prior to termination of the subscription, and the data processor will be under no obligation to store, maintain, or provide any of the data after termination; the data processor may block the data controller's access to the Solution and delete the data. If the data controller chooses to export the data from the cloud environment, the data controller is obligated to reimburse Milestone for the fees charged by the cloud service provider hosting the data. Before the end of subscription, the data controller may provide instructions regarding the data via email kitesupport@milestonesys.com.

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller's prior written authorisation:

The geographical region designated by the data controller at set-up of the Solution. If the data controller is established in the EEA, the data controller is encouraged to designate an EEA geographical region for the hosting of data.

Google Cloud Platform and, respectively the Solution, is located in the United States (Iowa), European Union (Belgium), and Japan.

C.6. Instruction on the transfer of personal data to third countries

The geographical region designated by the data controller at set-up shall be considered the data controllers instruction to transfer personal data to the designated region.

If the data controller chooses to transfer personal data to the sub-processor Arcules, cf. Appendix B.1. for the purposes of technical, analytical and forensic support or improvement of analytic tools as set out in Appendix C.1 – such transfer shall be considered as a controller to controller transfer initiated by the data controller.

If the data controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the data processor shall not be entitled within the framework of the Clauses to perform such transfer.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor and sub processors

The data controller or the data controller's representative shall have access to perform a physical inspection of the places, where the processing of personal data is carried out by the data processor, including physical facilities as well as systems used for and related to the processing to ascertain the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data processor and the data controller will discuss and agree in advance on the reasonable start date, scope and duration of, and security and confidentiality controls applicable to, any audit or inspection. Any audit or inspection requested by the data controller will be for the data controller's costs.

The data processor may object to any third-party auditor appointed by the data controller to conduct any audit if the auditor is, in the data processor's reasonable opinion, not suitably qualified or independent, a competitor of the data processor or otherwise manifestly unsuitable. Any such objection by the data processor will require the data controller to appoint another auditor or conduct the audit itself. The auditor in question must be subject to confidentiality, either contractually or by law.

Where a sub-processor makes available security audit reports, certifications or declarations etc. the data controller may request access to such reports. The data controller accepts that the data processors audit of processing performed by sub-processors are carried out by review of such available security audit reports, certifications or declarations.

The data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses. Any such further measures shall be for the data controller's costs. The data processor will provide the data controller with further details of any applicable fee and costs for itself and any sub processor, and the basis of its calculation, in advance of any such audit. The data controller acknowledges and accept that audits and inspections of sub-processors may be subject to standard terms provided by such sub-processors.

Appendix D The parties' terms of agreement on other subjects

D.1. Liability

The data processors liability, including any indemnity obligation, towards the data controller is subject to the limitations set out in the Agreement.

The data processor shall be liable towards data subjects for damages caused by processing only where the data processor has not complied with its obligations under the GDPR or where the data processor has acted outside or contrary to the lawful instructions of the data controller. To the extent data subjects claim compensation from the data processor in accordance with the GDPR or other provisions on joint liability for data controllers and data processors then the data controller will indemnify and reimburse the data processor for any claim which is not due to the data processors violation of the Clauses or the GDPR.

D.2. Assistance to the data controller

The data processor's assistance to the data controller for the fulfilment of the data controller's obligations under the GDPR, cf. Clause 8, and for participation in audits, cf. Clause 11, and Appendix C.7, is subject to payment of compensation to the data processor based on a market conform applicable hourly rate for external IT consultants and/or other relevant consultants, to the extent that the request for such assistance is not reasonably caused by the data processors non-compliance with the these Clauses or its obligations under the GDPR.

Appendix E Standard Contractual Clauses (Module 4 – Processor to Controller transfer)

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.

(a) 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").

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

(c) 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) and Clause 8.3(b);

(iii) [*Intentionally left blank*];

(iv) [*Intentionally left blank*];

(v) Clause 13;

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

(vii) Clause 16(e); and

(viii) Clause 18.

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7

Docking clause

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

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

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

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

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

8.1 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9

Use of sub-processors

[*Intentionally left blank*].

Clause 10

Data subject rights

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11

Redress

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

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) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party 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 under Regulation (EU) 2016/679.

(c) 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.

(d) The Parties agree that if one Party is held liable under paragraph (c), 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.

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

Clause 13

Supervision

[*Intentionally left blank*].

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

Clause 14

Local laws and practices affecting compliance with the Clauses

[*Clause omitted as it has been indicated that the EU processor will not combine the personal data received from the third country-controller with personal data collected by the processor in the EU*]

Clause 15

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

[*Clause omitted as it has been indicated that the EU processor will not combine the personal data received from the third country-controller with personal data collected by the processor in the EU*]

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 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 collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof. 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 a country allowing for third-party beneficiary rights. The Parties agree that this shall be the law of Denmark.

Clause 18

Choice of forum and jurisdiction

Any dispute arising from these Clauses shall be resolved by the courts of Denmark.

APPENDIX

ANNEX I

A. LIST OF PARTIES

Data exporter(s):

Name: Milestone Systems A/S

Address: Banemarksvej 50, 2605 Brøndby, Denmark

Contact person's name, position and contact details: Kristine C. Sorken, Head of Group Compliance, +4531547737, KSO@milestone.dk

Activities relevant to the data transferred under these Clauses: The Milestone Kite cloud based video management and access control solution is delivered by the data exporter as set out in Appendix A in the data processing agreement concluded between the data exporter and the data importer, of which these Clauses form part.

Role: Processor

Data importer(s):

Name: Customer as identified by the Customer itself in its request for the Milestone Kite cloud based video management and access control solution and, in that relation, having accepted the Milestone Kite Terms of Service.

Role: Controller

Signature and date: The Clauses shall become effective on the date of the data importer's acceptance of the Milestone Kite Terms of Service, or on the date the data importer has started to access and use the Milestone Kite cloud based video management and access control solution.

B. DESCRIPTION OF TRANSFER

Reference is made to *"Appendix A Information about the processing"* and "*Appendix C Instruction pertaining to the use of personal data"* in the data processing agreement concluded between the data exporter and the data importer, of which these Clauses form part.

Milestone Systems is a leading provider of data-driven video technology software in and beyond security that helps the world see how to ensure safety, protect assets, and increase business efficiency. Milestone enables an open platform community that drives collaboration and innovation in the development and use of network video technology, with reliable and scalable solutions that are proven in more than 500,000 customer sites worldwide. Founded in 1998, Milestone is a stand-alone company in the Canon Group.