MAKE THE
WORLD SEE

Date: November 4, 2024

XProtect Remote Manager

Data Processing Agreement

milestone

Standard Contractual Clauses

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 XProtect Remote Manager service (also referred to as "Customer" in the Milestone XProtect Remote Manager Terms of Use) and in that relation having accepted the XProtect Remote Manager Terms of Use, cf. https://www.milestonesys.com/terms-of-use-xrm/

(the data controller)

and

Milestone Systems A/S
CVR 20341130
Banemarksvej 50C
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.

1. Table of Contents

2. 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 XProtect Remote Manager Terms of Use (the "Terms") has been accepted by the data controller or from the date the data controller has started to access and use the XProtect Remote Manager (in the Terms it is also referred to as the Service).

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 date 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 XProtect Remote Manager, 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.

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

11. 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.

3. 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[1] 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.

4. 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 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.

5. 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

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

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.

6. 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.

   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.

2. 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.

3. 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.

If subsequently – in the assessment of the data controller – mitigation of the identified risks require 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.

7. 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 written authorisation for the engagement of sub-processors. The data processor shall inform in writing the data 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 the 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.

   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.

4. 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.

5. 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.

8. 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.

9. 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 6.3., 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 9.1. and 9.2.

10. 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 after the data processor has become aware of the personal data breach 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 9(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.

11. 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 unless Union or Member State law requires storage of the personal data.

12. 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 appendices C.7. and C.8.

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.

13. 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.

14. Commencement and termination

1. The Clauses shall become effective on the date of the data controller's acceptance of the XProtect Remote Manager, or on the date the data controller has started to access and use the Service.

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 11.1. 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 provide the data controller with the ability to use the XProtect Remote Manager to remotely manage their XProtect VMS system(s) connected by the data controller to the Service. XProtect Remote Manager will enable the data controller to perform the following functionalities currently available:

a. Auditing of user activities
b. Notification mechanisms
c. Customers adding own notes
d. Live video feed of a single camera at a time

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 of live video feed from the data controller's camara (only one camera at a time), receipt and storing of auditing change log in the data controller's XProtect Remote Manager and receipt and storing of any notes made by the data controller that might include personal data.

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

a. E-mail address and other identification information
b. IP address
c. Live video stream coming from the data controller's surveillance cameras, which may include images and behaviour of individuals, license plates of cars, etc.
d. Own personal notes that may or may not include personal data

The Service also holds personal data of registered users of the Service, like e-mail, 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 Service, including e-mails and other communication regarding the Service, e.g., planned downtimes, feature releases, account management, or other aspects of the Service. Personal data of registered users of the Service is therefore not covered by these Clauses.

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

Data controller's employees or other third party if the data controller includes these in e.g. data controller's private notes made in the Service, individuals and individuals associated with objects appearing in live video feeds which may be the data controller's employees, guest, 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:

For the period of time the data controller uses the XProtect Remote Manager.

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
Amazon Web Services EMEA SARL		38 Avenue John F. Kennedy, L-1855, Luxembourg	Storage of the above-mentioned types of personal data of 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 7.2

Appendix C Instruction pertaining to the use of personal data

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

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

Remote management of deployed XProtect VMS system through XProtect Remote Manager (Service). When making available to the data controller the data processor's Service, the data processor shall:

a. Facilitate the transmission of live video from the data controller's connected cameras to the Service.

b. Store personal data, the data controller has uploaded the Service.

c. Encrypt personal data during transmission to the Service and at rest in the Service.

If the data controller issues instructions to the data processor, and such instructions would prevent or limit the data processor's ability to provide the Service, 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.

The use of the Service 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 data lost, altered, intercepted or stored across those networks.

Technical support
The data controller acknowledges that the data processor is a data controller in its own rights when providing technical support to the data controller. Support provided to the data controller is therefore not covered by these Clauses. 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 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 the data controller and only when requested by the data controller.

b. Only access data through a Customer account generated for the purpose of containing specific material or by receiving a screenshot or live video stream from the data controller.

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

C.2. Security of processing

The data processor shall implement technical and organisational measures to ensure an appropriate level of security to adequately protect personal 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 – 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:
    a. No default logins
    b. Seamless automatic updates
b) In connection with network security the data processor has implemented the following:
    a. Encryption in transit and data is transmitted utilizing TLS 1.2 or greater
    b. Security measures implemented by the cloud provider are accessible here: Cloud Security – Amazon Web Services (AWS)

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 9.1. and 9.2. by implementing the following technical and organisational measures:

a) Internal organization
    a. 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.
    b. 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
    a. 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 the data subjects 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.
    b. The data processor shall not be entitled to respond to requests from a data subject.
    c. The data processor shall, at the request of the data controller, and to the extent the data controller cannot itself comply with the data subject requests by the tools available in the Service, reasonably assist in fulfilling the data controller's obligations.
c) Notification of data breach

a. 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 t the data processor within the time limit referred to in Clause 9.2.

b. 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.

C.4. Storage period/erasure procedures

The following storage periods are defined for the available functionalities:

a) Audit Logs: The personal data of the audit logs is not stored for a period of more than 3 months.
b) Naming and description: The personal data of the descriptions provided by the data controller will be stored for the time of the data controller using the Service.
c) Live video feed: The live video feeds are not stored in the Service and can only be viewed when streamed upon request of the data controller in the Service.

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 XProtect Remote Manager Service is hosted in the AWS data centres located in the EU.

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

The geographical region designated by the data controller is in the EU.

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

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 EUR 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 data, 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, 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 person 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 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.

C.8. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

See Clause C.7

Appendix D The parties' terms of agreement on other subjects

D.1. Liability

The data processor's liability, including any indemnity obligations, towards the data controller is subject to the limitations set out in the Terms of the Service. The data processor shall be liable towards data subjects for damages caused by processing only where the date 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 the 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 participations 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 reasonable caused by the data processors non-compliance with these Clauses or its obligations under the GDPR.

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.