Standard Contractual Clauses

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

between

Customer, cf. the Agreement

(the data controller)

and

Mestro AB
Sankt Göransgatan 63,
112 38 Stockholm
Sweden

Reg. no. 556679-4649

(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.

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).

3. In the context of the provision of Mestro, 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.

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

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.

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 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 shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.

3. 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 30 days 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.

4. 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.

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.

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, Datatilsynet, 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, Datatilsynet, 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 hours 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 both parties' signature.

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.

5. Signature

   On behalf of the data controller

   Name
   Position
   Phone number
   E-mail address
   Signature

   On behalf of the data processor

   Name
   Position
   Phone number
   E-mail address
   Signature

15. Data controller and data processor contacts/contact points

1. The parties may contact each other using the following contacts/contact points:

2. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Name
Position
Telephone
E-mail

Name
Position
Telephone
E-mail

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:

The Clauses are entered into as part of or with reference to the parties' agreement concerning the supply of one or more IT services by the data processor to the data controller (the Agreement).

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):

In connection with the data processor's provision of IT services to the data controller, personal data are processed as required in order to deliver the services set out in the Agreement, including storage, collection, registration, structuring, combination, erasure, filing, etc.

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

- ☒ Name
- ☒ Address
- ☒ E-mail
- ☒ Phone number
- ☐ Citizenship
- ☐ Date of birth
- ☐ Gender
- ☐ Marital status
- ☒ Job title
- ☐ Job ID
- ☐ Bank account information
- ☐ Pictures
- ☐ IP and Cookie information
- ☒ Other common personal information

Sensitive personal information (cf. General Data Protection Regulation Art. 9):

- ☐ Race or ethnic origin
- ☐ Political beliefs
- ☐ Religious beliefs
- ☐ Philosophical beliefs
- ☐ Trade Union Membership
- ☐ Genetic data
- ☐ Biometric data
- ☐ Health-related data, including abuse of medicine, narcotics, alcohol etc.
- ☐ The sexual relation or sexual orientation of a physical person

Personal data relating to criminal convictions and offenses (cf. General Data Protection Regulation Art. 10):

- ☐ Criminal convictions
- ☐ Criminal offenses

Information regarding personal identification number (cf. the Danish Data Protection Act, section 11)

☐ Personal identification number

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

☒ Employees

☒ Users, Patients, Citizens, Customers, Clients or similar

☐ Children (0 – 12 years)

☐ Youth (13 – 18 years)

☐ Relatives

☒ Collaborators

☐ Other

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:

The processing is not limited in time and will continue as long as necessary for the data processor's performance of the agreed tasks and compliance with obligations towards the data controller as set out in the Agreement.

Appendix B Authorised sub-processors

B.1. Approved sub-processors

At the time when the Clauses come into force, the data controller has approved the use of the sub-processors set out in the list of sub-processors in the document ”Mestro – Sub-processors”.

The document including the list of sub-processors is available here
https://egsoftware.com/documents/mestro-sub-processors

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

Pursuant to Clause 7.3, the data processor has the data controller’s general approval to use and replace sub-processors. The data processor must notify the data controller by email or in writing in general, e.g. via a digital notification system with the data processor (and/or the data processor’s sub-processors) about any planned changes regarding addition or replacement of sub-processors with at least thirty (30) days’ notice and thereby allow the data controller to object to such changes before using such sub-processor(s).

B.3 Approved sub-processors with special terms

The data processor is responsible for the services provided by sub-processors in the same way as for the data processor’s own services.

If the data processor in the performance of the Agreement uses services from sub-processors, that are subject to other terms than those set out in the Agreement, such other terms will be included in the list of sub-processors ”Mestro – Sub-processors”, cf. Appendix B, Clause B.1.
These terms will apply in the relationship between the data controller and the data processor as regards the processing done by the sub-processor.

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:

Any processing required for the data processor to comply with the obligations set out in the Agreement between the parties. Thus, the following processing activities are comprised by the Clauses: Implementation, operation, support, test and maintenance of the service. In this connection, the data controller accepts transfer of personal data from production to test environment.

Customer specific fields and free text fields

The data controller accepts that no other personal data are specified in connection with customer-specific and free text fields than those set out in Appendix A. If the data controller sets out other personal data than those specified in Appendix A, the data controller shall immediately notify the data processor thereof and update the instruction in the Clauses.

C.2. Security of processing

The level of security shall take into account:

The data processor implements appropriate technical and organizational measures to ensure a level of security appropriate to the risks associated with the processing activities that the data processor performs for the data controller.

The technical and organizational measures are determined taking into account the current technical level, the implementation costs, the nature, scope, coherence and purpose of the processing in question, as well as the risks of varying probability and seriousness for the rights and freedoms of natural persons.

In assessing the appropriate level of security, particular account shall be taken of the risks posed by processing, in particular in the event of accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data transmitted, stored or otherwise processed.

The data processor is then entitled and obliged to make decisions about which technical and organizational security measures must be implemented in order to establish the necessary (and agreed) level of security.

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:

At the specific request of the data controller, the data processor, taking into account the nature of the processing, assists the data controller as far as possible by appropriate technical and organizational measures in compliance with the data controller's obligation to respond to requests for data subjects' rights.

If a data subject submits a request for the exercise of his rights to the data processor, the data processor shall notify the data controller without undue delay.

Taking into account the nature of the processing and the information available to the data processor, the data processor, upon specific request, assists the data controller in ensuring compliance with the data controller's obligations in relation to:

- Implementation of appropriate technical and organizational measures
- Security breach
- Notification of breach of personal data security to the data subject
- Conducting impact assessments
- Prior consultations with the supervisory

C.4. Storage period/erasure procedures

Upon termination of the service regarding processing of personal data, the data processor shall either delete or return the personal data in accordance with Clause 11.1, unless otherwise specifically agreed between the parties.

C.5. Processing location

Details on the data processor's and its sub-processors' processing facilities can be obtained by contacting the data processor. This information can be disclosed to the extent disclosure can take place without any safety risk in the opinion of the data processor. In such situation, only information about country and town for the processing facility will be disclosed.

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

The data processor is entitled to use sub-processors in third countries to fulfil the data processor's obligations towards the data controller.

Use of sub-processors in third countries is only allowed if (i) the transfer is based on an adequacy decision of the European Commission, including e.g. that the said third country has an adequate level of protection, (ii) the transfer is comprised by sufficient guarantees like e.g. the European Commission's standard provisions or (iii) the transfer is comprised by relevant binding corporate rules. If required pursuant to the transfer basis applied that the data controller is a direct party in the transfer basis, the data processor shall be considered authorised to accept such an agreement on behalf of the data controller. The data processor is entitled to transfer this authorisation to sub-processors whereby sub-processors can set up and agree to a valid transfer basis on behalf of the data controller.

Appendix B, Clause B.1, includes a specification of the sub-processors in third countries approved by the data controller, and which sub-processors the data processor is thus entitled to transfer personal data to when the Clauses come into force.

The data processor is authorised by the data controller to enter into an agreement on amendment of the EU standard provisions attached to the Agreement. This can result from changes in the data protection legislation, including new standard provisions from the EU. Any amendments will only be made in accordance with the EU rules for using EU standard provisions in force from time to time. The current version of the agreed EU standard provisions

can be obtained from the data processor at the request of the data controller or the data subject.

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.

The parties agree to comply with the process set out in Appendix B, Clause B.2 and B.3, regarding addition or replacement of sub-processors in third countries. Thus, the data controller's instruction also comprises transfer of personal data to new sub-processors in third countries, which during the term of the Clauses are engaged by the data processor in accordance with the process set out in Appendix B, Clause B.2 and B.3 and this Clause C.6.

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

If the data processor is required to obtain an audit report of types ISAE 3402 or ISAE 3000 or equivalent from an independent third party regarding the data processor's compliance with the General Data Protection Regulation, data protection provisions deriving from other EU law or the national law of the Member States and these provisions (Clauses), this will be at the data controller's expense.

The data processor shall make available to the data controller all information necessary to demonstrate compliance with the requirements of the Clauses. The data processor hereby provides the opportunity for and contributes to audits, including inspections carried out by the data controller or another auditor authorized by the data controller.

If an audit is performed by someone other than the data controller himself, this other auditor must be independent and non-competitive with the data processor and otherwise be subject to a duty of confidentiality and secrecy either as a result of law or as a result of a confidentiality agreement on which the data processor can support the direct auditor in question directly.

The data processor shall immediately notify the data controller if an instruction to make information available or allow for audits and inspections in the data processor's opinion is in breach of the GDPR or data protection provisions of other EU or national law.

The data controller shall compensate the data processor's time and cost related to monitoring (e.g. physical inspections, collection of written information and reply to questionnaires). Unless otherwise agreed between the parties, the data processor's contribution to such monitoring will be invoiced on a time and materials basis, cf. Appendix D.

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

The data processor or another auditor authorized by the data processor audits the sub-processor based on the specific processing activity performed by the sub- processor in order to determine the sub- processor's compliance with the General Data Protection Regulation, data protection provisions deriving from other EU law or the national law of the Member States and these provisions (Clauses).

The documentation of the conducted audit with the relevant sub-processor can be obtained from the data processor at the request of the data controller.

Appendix D The parties' terms of agreement on other subjects

D.0. Modifications of the Clauses

Clause 14.5
As the Clauses represent an appendix to the parties' Agreement, this document is not to be signed separately between the parties.

Clause 15
The parties' contact persons, cf. Clause 15, are further specified in the Agreement.

D.2. Payable service

The data processor is entitled to separate payment for services in accordance with Clauses 9 (Assistance to the data controller) and 10 (Notification of personal data breach) and for participation in audits in accordance with Clause 12 (Audit and inspection) and Clause C.7. of Appendix C (Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor) and Clause C.3. of Appendix C, unless otherwise explicitly agreed.

If the data processor's work on the handling of security breaches in relation to Clause 9.2.a and 9.2.b is due to breach of contract on the part of the data processor, the data processor will not be entitled to payment for this work.

Before initiating a task, the data processor's estimated fee shall be approved by the data controller. This, however, does not apply if the nature of the task requires the data processor to take immediate action. In such situations, the data processor shall obtain the data controller's written approval of the estimated fee for the task as soon as possible. If the work related to the tasks exceeds the approved estimate, the data processor shall immediately notify the data controller thereof, including the reason for exceeding the estimated fee.