DATE

Data Protection Agreement

Between

Customer (Data controller):

and

Supplier (Data processor)
Amesto Solutions A/S

Amesto Solutions A/S | Vandtårnsvej 62 A, 4. sal 2860 Søborg | Tlf.: +45 49 22 46 46
E-mail: sales@amesto.dk | CVR. nr.: 25 38 00 10 | www.amestosolutions.dk

Standard Contractual Clauses

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

Name
CVR
Address
Zip and City
Country
(the data controller)

and

Amesto Solutions A/S
Våndtårnsvej 62 A, 4.sal
2860 Søborg
Danmark

CVR no. 25 38 00 10

(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 Contents

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.

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 contract, 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.

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 State1 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.

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.

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

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.

   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.

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 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 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.

5. 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.

6. 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.

7. The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g. enabling the data controller to instruct the sub-processor to delete or return the personal data.

8. 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 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.

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 72 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.

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 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 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.

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 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

   Date
   Signature

   On behalf of the data processor

   Name
   Position

   Date
   Signature

14 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 processing of personal data by the Data Processor on behalf of the Data Controller:

The purpose of the processing is to assist with support, maintenance and development of standard software on behalf of the Data Controller. As a result, the Data Processor will process personal data through:

- Time-limited access from their own computer
- Access from their own computer
- Temporary and time-limited storage/processing of personal data, for example on a computer or Azure Cloud
- Storage/processing of personal data outside the Data Controller's environment, for example in Azure and Amesto Flow

A.2. The processing of personal data by the Data Processor on behalf of the Data Controller shall primarily relate to (nature of the processing):

The processing relates to the Data Controller's personal data. The purpose of the assignment is not to refine or adapt personal data, apart from in exceptional cases, for example when cleaning personal data or importing personal data.

When working with the Data Controller's system support within ERP, CRM and HRM with associated applications, reporting solutions and integrations, the Data Processor will have access to personal data, either by connection or in the Data Controller's own environment.

A.3. The processing includes the following types of personal data on data subjects, albeit to a varying degree depending on the type of personal data the Data Controller has stored in their systems:

Contact information, such as: First and Last name, Telephone Number, Address, e-mail address, date of birth, employment relationship, etc.

The Data Controller's customers and other stakeholders' personnel: Title, employer, interests, ongoing communication in the form of events and documents/e-mails, etc.

If applicable, via the HRM system: Employee's Name, e-mail, mobile phone number, employee number, role, title, manager, business area, workplace, social security number, etc.

A.4. The processing includes the following categories of data subjects, albeit to a varying degree depending on the type of personal data the Data Controller has stored in their systems:

- The Data Controller's end users
- The Data Controllers' customers, prospects and other stakeholders' personnel
- Employees of the customer

A.5. The processing of personal data by the Data Processor on behalf of the Data Controller may be conducted when the clauses take effect. The duration of the processing is as follows:

Processing/Access	Storage of personal data or access	YES	NO
From own computer, time-limited access regulated by the Data Controller, for example for support, design, technology or development	No personal data is stored. Access ends immediately after the end of the session.		
From own computer, via the Data Processor's own connection information, for example access for support, design, technology or development	No personal data is stored. Connection information is deleted in connection with the termination of the agreement, when the employee leaves or on the instructions of the Data Controller.		
Temporary and time-limited storage/processing of personal data outside the Data Controller's environment, for example on a computer, in e-mail, on an Amesto server.	Deleted 30 days after the assignment is approved or on the instructions of the Data Controller.		
Non-time-limited storage/processing of personal data outside the Data Controller's environment, for example in Azure, Amesto Flow - SaaS	Deleted 30 days after the assignment is completed or on the instructions of the Data Controller.		

Appendix B Approved subcontractors

B.1. Approved subcontractors

When the clauses take effect, the Data Controller approves the use of the following subcontractors:

NAME	CORPORATE IDENTITY NO.	COUNTRY	DESCRIPTION OF THE PROCESSING
Sister Companies affiliated to Amesto Tech House.		Norway, Sweden and Denmark.	Whenever needed Amesto Solutions A/S can use consultants from sister companies as consultants in the project,

The Data Controller shall, when the clauses take effect, approve the use of the above-mentioned subcontractors for the processing described to the Party. The Data Processor shall not have the right - without the written permission of the Data Controller - to hire a subcontractor for processing other than those approved, or to have another subcontractor perform the specified processing.

B.2. Advance information on the approval of subcontractors

Approval of a subcontractor must be approved in writing before the subcontractor may be used for the specified processing.

Appendix C Instructions for the use of personal data

C.1. The scope of/instructions for processing

Obligations as a data processor

The data processor shall only process personal data to the extent necessary to fulfil its tasks and obligations under the Main Agreement or the described assignment.

Confidentiality and Non-disclosure

The data processor shall ensure that authorised persons are obliged to treat personal data confidentially, or are subject to a statutory duty of non-disclosure. This is achieved through a signed non-disclosure agreement entered into upon being employed by Amesto.

The duty of confidentiality also applies after the data processor assignment has been completed.

The data processor shall only authorise persons who require access to the personal data for necessary reasons.

If the Instruction is in violation of the applicable rules, and the Data Controller is informed of this, but the Data Controller considers this as necessary processing to complete the assignment, the responsibility for processing will lie with the Data Controller.

C.2. Security of processing

The data processor takes all necessary measures in accordance with the Personal Data Act, section 32. Security of processing.

The processing only applies to personal data covered by section 9, Processing of sensitive personal data, if the customer has such data in its systems.

PROCESSING/ACCESS	YES	NO
Processing takes place in the Data Controller's development, administration/system development and operating environment via an approved Amesto PC for a time-limited period for the handling of, for example, support, design, technical assistance or development	X	
Temporary and time-limited storage/processing of personal data outside the Data Controller's environment.		X
Storage/processing of personal data outside the data controller's environment.		X

Pursuant to Amesto Security Policy, Approved Amesto PC means, among other things, that the workstation locks out others; only a valid account can be logged on to the device. Uses Remote Wipe on a lost PC to secure content.

Refer to Amesto Privacy Policy section 3. https://www.amestosolutions.dk/om-amesto/gdpr/persondatapolitik/

The transfer of data containing personal data from the Data Controller to the Data Processor shall take place using secure transfer systems, by agreement with the Data Controller.

C.3. Assistance to 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 sections 9.1. and 9.2. by implementing the following technical and organisational measures:

Physical protection

For cloud solutions, Amesto Solutions uses the supplier's data centres to store information. These run around the clock and secure operations by protecting against power outages, physical intrusion and network outages. These data centres comply with recognised industry standards for physical security and reliability.

Monitoring and protection

When Amesto Solutions makes services available to its customers, they are closely monitored. This includes continuous scanning for vulnerabilities, monitoring of attempted intrusion and detection of abuse. For more information: Amesto Trust Center: https://www.amesto.com/amesto-trust-center/

C.4. Procedure for storage time/deletion

PROCESSING/ACCESS	STORAGE OF PERSONAL DATA OR ACCESS
From own PC, time-limited access provided by the Data Controller for assistance related to, for example, support, design, technical assistance or development	No personal data is stored. Access ends immediately after the assignment is completed
From own PC for access provided by the Data Controller for assistance related to, for example, support, design, technical assistance or development	No personal data is stored. Access information is deleted in connection with termination of the agreement, when an employee of Amesto Solutions resigns from his/her position or at the request of the Data Controller
Temporary and time-limited storage/processing of personal data outside the Data Controller's own environment, for example on a PC, email, Amesto server	Deleted 30 days after the assignment is approved or at the request of the Data Controller
Non time-limited storage/processing of personal data outside the Data Controller's own environment. For example in Azure, Amesto Flow - SaaS	Deleted 30 days after the assignment is approved or at the request of the Data Controller

C.5. Processing location

Processing takes place in the Data Processor's development, management/system development and operating environment in Norway, Sweden and Denmark.

If the location is outside the EU/EEA (Third Country) or the location is changed from that stated here, this shall be handled pursuant to section 8 of the Data Processing Agreement.

C.6 Instructions regarding transfers of personal data to a third country

The Data Processor must process the personal data only on documented instructions from the Data Controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by European Union or Member State law to which the Data Processor is subject; in such a case, the Data Processor shall inform the Data Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest, cf. Article 28, subsection 3, letter a.

If the Data Controller does not provide documented instruction regarding the transfer of personal data to a third country in these Provisions or subsequently, the Data Processor is not entitled to make such transfers within the framework of these Provisions.

C.7 Procedures for the Data Controller's audits, including inspections, of the processing of personal data handed over to the Data Processor

The Data Processor shall, upon written request, provide the Data Controller with documentation of the technical and organizational measures taken to ensure an appropriate level of security, as well as other information necessary to document the Data Processor's compliance with the General Data Protection Regulation, the data protection provisions of other European Union law or Member State law and these Provisions.

The Data Controller has the right to obtain an audit statement once a year from an independent third party. The Data Controller shall cover all expenses in connection with the audit, and the Data Processor is entitled to compensation for all costs that arise as a result of the audit, including reasonable compensation to the Data Processor for time spent by the Data Processor and its employees for assistance during the audit. However, the Data Processor shall cover such costs if an audit reveals significant deficiencies in the fulfilment of the obligations set out in these Provisions or in Data Protection legislation.

On the basis of the audit statement, the Data Controller is entitled to request the implementation of additional measures to ensure compliance with the General Data Protection Regulation, the data protection provisions of other European Union law or Member State law and these Provisions.

Appendix D The parties' terms of agreement on other subjects

D.1. Notification of personal data breach

The Data Processor shall provide reasonable assistance so that the Data Controller can fulfil its obligations to provide supplementary information to the relevant supervisory authority and the data subjects.

D.2. Notification of personal data breach

The Data Processor shall implement necessary and recommended corrective measures. The Data Processor shall also cooperate with the Data Controller to prevent, minimise the consequences of or correct Security Breaches.

D.3. Liability

No party shall be liable to the other party for indirect losses or consequential damages of any kind (including, but not limited to losses due to business interruptions, loss of data, lost profits or the like) regardless of the basis of liability, whether in contract, culpability, product liability or otherwise, even if the party has been notified of the possibility of such damages (collectively referred to as "Indirect Losses").

No party shall be liable to the other party for;

1. errors or delays beyond the reasonable control of the party, including general internet or line delays, power outages or mechanical faults; or

2. errors caused by the other party's systems or actions, negligence or omissions, which shall be the sole responsibility of that party.

The total and maximum liability for each twelve (12) month period, for one party to the other party under or pursuant to this Data Processing Agreement, shall under no circumstances exceed an amount equal to the total amount paid for the Service under the Agreement during the twelve (12) months prior to the tortious act.

The above limitations shall not apply to damages resulting from fraud, gross negligence or wilful misconduct.

amesto
Solutions

Simplifying business.

Amesto Solutions
Rosenlundsgatan 54
118 63 Stockholm