Data Processing Agreement

(Standard Contractual Clauses)

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)
(as based on Opinion 14/2019 by the European Data Protection Board).

Between

Company which is included in the Order Form

(the data controller)

And

Coldbyte AS, business reg. no. 938 312 133

(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

1 Table of Contents 1
2 Preamble 2
3 The rights and obligations of the data controller 2
4 The data processor acts according to instructions 3
5 Confidentiality 3
6 Security of processing 3
7 Use of sub-processors 4
8 Transfer of data to third countries or international organisations 5
9 Assistance to the data controller 5
10 Notification of personal data breach 6
11 Erasure and return of data 7
12 Audit and inspection 7
13 The parties' agreement on other terms 7
14 Commencement and termination 8
15 Data controller and data processor contacts/contact points 8
Appendix A Information about the processing 9
Appendix B Authorised sub-processors 10
Appendix C Instruction pertaining to the use of personal data 11
Appendix D The parties' terms of agreement on other subjects 14

sandtro.no

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 Services as described in the Order Form under the Terms of Service which these Clauses form part, 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.

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

sandtro.no

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.

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;

sandtro.no

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.

   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.

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.

sandtro.no

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:

sandtro.no

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 6.4., 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 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 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 shall 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.

sandtro.no

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 D 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.

2. The data processor commits to exclusively process the personal data for the purposes and duration provided for by this law and under the strict applicable conditions.

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

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.

sandtro.no

14 Commencement and termination

1. The Clauses take effect when the Customer accepts the Coldbyte Terms of Service, of which the Clauses form part, and require no separate signature. Where the parties nevertheless sign the Clauses separately, they take effect on the date of the last 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

   These Clauses form part of the Coldbyte Terms of Service and are accepted together with them, as set out in Section 1 of those Terms.

15 Data controller and data processor contacts/contact points

1. The parties may contact each other using the following contacts/contact points as set forth in the Order Form entered into by the parties under the Terms of Service.
2. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

sandtro.no

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 processing is carried out to maintain and improve the security of the Controller's Microsoft 365 environment, including to support the Controller's own obligations under Article 32 GDPR. The Processor does not process the personal data for any other purpose. In particular, the personal data is not used to monitor the performance or behaviour of the Controller's staff beyond the security purpose, for product development, or to train or improve machine-learning models.

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):

Automated and continuous collection and analysis of security metadata from the Controller's tenant, identified by the tenant domain and the Azure subscription identifier stated in the Order Form, through read-only Microsoft Graph permissions; generation of alerts, reports and a dashboard within the Controller's own environment; execution of predefined configuration changes in the tenant, in each case only after approval by a person designated by the Controller; and access by named Processor personnel to the Controller's environment for provisioning, delivery of updates, error correction and agreed support. The Processor does not access content data, meaning mail, files, documents and chat, and does not process personal data in other Microsoft services in the tenant beyond the security metadata described here.

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

Identifiers, including user principal name, display name and user ID. Sign-in metadata, including time, IP address, city, country and geographical coordinates, application and result. Risk and security assessments generated by Microsoft. Audit log events, including group names and role names and the identity of the acting user. Device data, including device name, owner, operating system and compliance state. Multi-factor and authentication status. Derived behavioural indicators, including sign-in country history. Approval and decision logs. Configuration change events with attribution to the acting user. Application identity inventory, including owners, the persons who granted consent and attestation decisions. Where a change is approved, mailbox configuration, never mailbox content, and on account containment the registered authentication methods, which may include a telephone number or an email address.

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

The Controller's employees, contractors and guest users holding an account in the tenant; administrators and designated approvers; and, to a limited extent, third parties appearing in configuration data, such as external forwarding addresses, and IP addresses associated with attempted attacks.

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 carried out for the term of the subscription and, where the parties have entered into the Supplementary Terms for Financial Undertakings (DORA), for any transition period following termination that is agreed under those terms. Collection is continuous. Retention is as set out in Appendix C.4.

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:

The Processor engages no sub-processor that receives the Controller's personal data for the Service. The software runs within the Controller's own tenant and subscription, and the underlying platform is the Controller's own Microsoft subscription under the Controller's own agreement with Microsoft, not appointed by the Processor.

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

Section 7 in the Clauses applies. The Processor holds the Controller's general written authorisation and shall inform the Controller in writing at least thirty days before adding or replacing a sub-processor, so that the Controller may object before the sub-processor is engaged.

sandtro.no

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:

The Processor shall carry out the processing described in Appendix A.2 and no other processing. Configuration changes in the tenant are carried out only where a person on the Controller's list of authorised approvers has approved the change in the Controller's own approval channel, where the approval is signed, time-limited and bound to the exact version of the change presented, and where no authorised approver has rejected it. Measures directed at an individual require the approval of at least two authorised approvers. The Processor's access to the environment is used only for provisioning, updates, error correction and agreed support, and not to read the Controller's business data or personal data beyond what is strictly necessary for those purposes. Personal data seen during support is not taken out of the environment, whether by export, screenshot or local storage.

C.2. Security of processing

The level of security shall take into account:

The level of security shall take into account that the processing concerns metadata about the Controller's staff and their use of the environment, and that special categories of personal data within the meaning of Article 9 GDPR may appear indirectly through metadata such as group names, distribution lists and audit log entries, even though the Service is not designed to process such data. The Processor shall in any event implement the following measures: per-customer isolation with all storage in the Controller's own subscription; a continuously running component holding read-only permissions only, with any write identity isolated to a separate component activated only for an approved change and without inbound network access; explicit field selection on all data sources, so that the most personal-data-intensive fields are not collected, and no collection of content data; encryption in transit using TLS 1.2 or higher and encryption at rest; federated identities without client secrets, and key material held in the Controller's key vault with purge protection; an append-only event log of changes, approvals and Processor operations, available to the Controller; and access for named personnel only, subject to a duty of confidentiality and to phishing-resistant authentication, reviewed at least annually and withdrawn immediately on a change of personnel.

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:

The Service supports the rights of data subjects as functionality. Export under Articles 15 and 20 compiles the records the deployment holds about a data subject, and erasure under Article 17 removes those records and reports any time-limited residual data and its expiry. Each action is carried out on the Controller's instruction and logged. The Processor maintains and makes available the technical factual basis the Controller needs for a data protection impact assessment, namely a data map, an access matrix and a retention overview, and notifies the Controller of changes that require the assessment to be updated. Assistance beyond this is provided at the Processor's applicable hourly rates, subject to the Controller's prior approval.

C.4. Storage period/erasure procedures

Raw data is retained for thirty days, behavioural baselines for one hundred and eighty days, raw posture and remediation artefacts for ninety days, the configuration drift timeline for ninety days or up to four hundred events, and the approval and attestation log for four hundred days as the record required under Article 5(2) GDPR. Erasure is automated. The personal data processed under the Clauses resides in the Controller's own subscription and no copy is held by the Processor. On termination, erasure under Clause 11.1 is carried out in accordance with the Coldbyte Terms of Service, under which the Controller deletes the Service instance and the registered application within thirty days, or allows the Processor to do so, and confirms to the Processor that this has been done. Where the Controller elects to retain the data, the Processor's obligation under Clause 11.1 is discharged by confirming in writing that its access has been withdrawn and that it holds no copies.

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:

Processing takes place solely within the Controller's own Microsoft Azure subscription and Microsoft 365 tenant, identified by the tenant domain and the subscription identifiers stated in the Order Form, and in the region stated there. Access by the Processor's personnel takes place from Norway. Processing at any other location requires the Controller's prior written authorisation.

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

The Controller gives no instruction to transfer personal data to a third country or to an international organisation, and the Processor shall not carry out any such transfer under the Clauses.

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 Controller may verify the Processor's compliance by reviewing documentation, and the Processor shall on request make available its access lists, event logs, the results of its automated tests, its self-assessment and any penetration test summaries that exist. The Processor is not certified against ISO/IEC 27001, SOC 2 or comparable standards and does not undertake to obtain such certification or to commission penetration testing on request. Where documentation is not sufficient to establish compliance, the Controller may carry out an inspection on four weeks' written notice, at the Controller's own cost and at times that limit disruption to the Service. The Processor operates no data centre or other premises of its own from which the Service is provided, and Clause 12.3 is performed by giving access to the documentation and systems referred to above. Because the environment resides in the Controller's own subscription, the Controller has continuous access to the resources, logs and costs of the deployment, and the Service shall not be arranged in a way that reduces that access.

sandtro.no

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

Not applicable while no sub-processor is engaged. Where a sub-processor is engaged under Appendix B.2, the procedure in C.7 applies correspondingly, and the Processor obtains and makes available the documentation needed to establish the sub-processor's compliance.

sandtro.no

Appendix D The parties' terms of agreement on other subjects

D.1. When assisting the Controller in notifying a personal data breach to the supervisory authority, the Processor shall provide the nature of the breach and, where possible, the categories and approximate number of data subjects and of records concerned; the likely consequences; and the measures taken or proposed, including measures to mitigate adverse effects. Notification is given in phases where the information is not available at once, in accordance with Article 33(4) GDPR.

D.2. Security incidents affecting the Processor's own supply chain, including its code repository, its deployment infrastructure and its access credentials, are treated as notifiable even where it cannot be established that the Controller's personal data is affected.

D.3. Liability, limitation of liability, governing law and venue are governed by the Coldbyte Terms of Service and are not regulated here.

sandtro.no