Data Protection Agreement

Last updated: 19-April-2024

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

between

Seculyze

CVR 42004332

Lathyrusvej 11

3500 Vaerloese

Denmark

(the data processor)

And the undersigned data controller, cf. Clauses 14(5)

(the data controller)

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 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. The Clauses has been drafted based on the recommended Clauses for data processing terms by the Danish Data Protection Agency. Appendix E reflects all changes made to the terms recommended by the Danish Data Protection Agency.

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 Seculyze Software, 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 authorized 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 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.

hello@seculyze.com | +45 21909575

3 The rights and obligations of the data controller

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

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

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

4 The data processor acts according to instructions

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

2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

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.

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 organizational measures to ensure a level of security appropriate to the risk.

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

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.

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).

   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 calendar 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 authorized by the data controller can be found in Appendix B.

2. 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 organizational 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.

3. 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.

hello@seculyze.com | +45 21909575

8 Transfer of data to third countries or international organizations

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. 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.

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 organizational 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.

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 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 to the data controller shall, if possible, take place within 24 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.

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.

hello@seculyze.com | +45 21909575

12 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 Data Processor is managing personal data from the use of tools within the EDR (Endpoint Detection and Response), SIEM (Security Information and Event Management), and the Microsoft Defender portfolio. This management includes monitoring, analyzing, and addressing security alerts, as well as collecting and examining data to improve the efficiency and capabilities of these security monitoring and protection systems.

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):

The Data Processor is acquiring and collecting data relating to security incidents. The mentioned data is analyzed with the help of machine learning (ML), whereby the alarms are grouped in order to identify patterns and unusual behaviour. In addition, data related to all raw security alerts and metadata related to these are collected and analyzed to improve the ML model and to create a better understanding of the underlying threats and activities.

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

General information: This includes in-depth security alerts and log data as processed by Sentinel/Defender systems. It entails very detailed information of security incidents, such as the nature and source of the alert, usernames, emails and the full legal names of individuals, and the type of potential security breach. It also includes IP addresses which can be used to identify the network location of the device. Details about the device, including type, model, operating system, and other pertinent hardware or software specifications, are included. Time of logins refers to the exact dates and times when users access the system. User activities encompass a range of actions performed by the user during their session, including but not limited to file accesses, modifications, and communication activities. System logs refer to the comprehensive records generated by the system

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

- Employees of the data controller who use the IT systems
- External consultants with access to the data controller's network
- Other users, such as students who interact with the controller's IT infrastructure.

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 duration of the data processing agreement follows the terms in the Order.

hello@seculyze.com | +45 21909575

13 Appendix B Authorised sub-processors

B.1. Approved sub-processors

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

NAME	CVR	ADDRESS	DESCRIPTION OF PROCESSING
Auth0, Inc.	464680619	Suite 700, 10800 North East 8th Street, Bellevue, Washington, 98004 USA	Auth0 is used for identity management, user validation and secure API communication
Intercom R&D Unlimited Company	IE538158	2nd Floor, Stephen Court, 18-21 St. Stephen's Green Dublin 2 Republic of Ireland	Support chat and knowledge articles
HubSpot Ireland Ltd.	IE515723	HubSpot House One Sir John Rogerson's Quay, Dublin 2 Republic of Ireland	Generic CRM data
Microsoft Ireland Operations Ltd.	IE256796	South County Business Park, One Microsoft Place, Carmanhall And Leopardstown, Dublin, D18 P521 Irland	Cloud services for data storage and application operation. As well as Clarity which adheres to Microsoft's Privacy Statement.

The data controller shall on the commencement of the Clauses authorize the use of the abovementioned sub-processors for the processing described for that party.

14 Appendix C Instruction pertaining to the use of personal data

C.1. Security of processing

The level of security shall take into account:

1. Pseudonymisation and Encryption of Personal Data:

Data protection extends beyond storage, with AES-256 encryption employed to secure data at rest. This encryption standard offers robust defence against unauthorized access and data breaches. Additionally, all interactions, including APIs and direct data access, are encrypted using FastAPI's TLS, ensuring secure and seamless API communications. Our Azure-based infrastructure further enhances security by facilitating encrypted data transfers through SSL/TLS protocols.

2. Ensuring Ongoing Confidentiality, Integrity, Availability, and Resilience of Processing Systems and Services:

The Data Processor's systems and services are designed to ensure ongoing confidentiality, integrity, availability, and resilience achieved through the use of Azure Kubernetes, FastAPI, and Vue.js in our deployments, supplemented by Dependabot for code health and continuous vulnerability scans. Microsoft Defender safeguards The Data Processor's resources, while Azure's Security Benchmarking informs the Data Processor's remediation strategies. Monitoring is enhanced with Grafana and Loki for Kubernetes, and Azure Sentinel provides comprehensive oversight.

3. The Ability to Restore the Availability and Access to Personal Data in a Timely Manner in the Event of a Physical or Technical Incident:

In the event of a physical or technical incident, the Data Processor's systems are designed for quick restoration of data availability and access. This is facilitated by the Data Processor's resilient infrastructure with data housed in isolated Kubernetes and Azure environments. The Data Processor's setup ensures that application and database environments are separate, prioritizing data integrity and rapid recovery.

4. Processes for Regularly Testing, Assessing, and Evaluating the Effectiveness of Technical and Organizational Measures for Ensuring the Security of the Processing:

The Data Processor's approach to ensuring the security of processing involves regular testing, assessment, and evaluation. Tests are automated within pipelines allowing for consistent and thorough evaluation of the technical and organizational measures. This automation ensures ongoing effectiveness and compliance with security standards.

5. Access to Data Online:

Access to data online is tightly controlled and secured. The Data Processor's uses Auth0 to provide tailored access based on organizational needs, with three distinct role levels. This control integrates with our APIs, and Azure AD's Multi-Factor Authentication (MFA) further secures identity verification for the Data Processor's employees. The Data Processor's Azure IAM model adheres to the principle of least privilege, ensuring that only authorized entities have access to relevant data.

6. Protection of Data During Transmission:

Data protection during transmission is ensured through our robust encryption protocols. All data transmissions are secured using SSL/TLS encryption, as part of the Azure-based infrastructure. This encryption safeguards data against interception and unauthorized access during its transit.

7. Protection of Data During Storage:

For data protection during storage, the Data Processor's employs AES-256 encryption, providing a high level of security against breaches and unauthorized access. This encryption is a key part of our strategy to ensure the safety and confidentiality of stored data.

8. Describe Requirements for Physical Security of Locations at Which Personal Data are Processed:

We refer to Microsoft Azure facilities, premises, and physical security[2].

9. Logging:

[2] https://learn.microsoft.com/en-us/azure/security/fundamentals/physical-security

The logging requirements include comprehensive capture and storage of activity logs. These logs are monitored and analyzed for any unusual activities or potential security threats. The use of Azure Sentinel enhances the logging capabilities, providing detailed insights into system activities. In addition, the Data Processor also use Grafana and log analytics to monitor the application, Kubernetes and container logs.

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 organizational measures:

- The data processor has formal procedures for how assistance to the data controller is handled in the company.
- The data processor ensures sufficient internal procedures so that the data processor can comply with its obligation to assist with security incidents, requests from the data subject and handling of the data subject's rights.
- The data processor does not answer or solve a query from a data subject about their rights, including access, but forwards the query to the data controller as soon as the data processor is aware that it is the data controller who must process the query.
- The data processor will journalize and document all correspondence with the data controller that relates to assistance to the data controller.

C.4. Storage period/erasure procedures

See section 11.

Application data is retained for the duration of our engagement with the customer. This retention policy ensures that we can provide continuous and efficient service to our customers for as long as they use our products or services. Once the customer relationship concludes, personal data associated with the customer's account will be automatically erased from our systems. The erasure process is initiated following a predefined time period, which is set to 30 days after the end of the customer relationship. This period allows for any necessary final account processing or customer inquiries.

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:

hello@seculyze.com | +45 21909575

- Microsoft Azure
    - Data hosting location: Western Europe
    - Sub-data processor: Microsoft Azure
    - Relevant Information: For Azure cloud services, a customer is usually the controller and Microsoft acts as the data processor. More information can be found in the Microsoft Azure GDPR documentation

- Auth0
    - Data hosting location: Europe
    - Sub-data processor: Auth0
    - Relevant Information: Auth0 applies the GDPR principles broadly, including consent, individuals' rights and both data protection by design and as a default setting. The Company's services are designed to store and manage user data in accordance with the GDPR, especially for EU citizens. For a detailed review, please refer to Auth0's GDPR guide

- Intercom
    - Data hosting location: European Union
    - Sub-data processor: Intercom
    - Relevant Information: Although GDPR does not require Intercom to store personal data exclusively in the EU, the company ensures legal data transmissions from the EU. Intercom is certified pursuant to Data Privacy Framework agreed between the US and EU, thus ensuring an adequate level of data protection for data transfers from the EU to the US. More about Intercom's data protection measures can be found on their GDPR guide

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

Intercom is certified pursuant to the Data Privacy Framework agreed between the US and EU, thus ensuring an adequate level of data protection. This method aligns with the GDPR's requirements for international data transfers, providing a solid legal foundation for such actions.

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

See standard contract terms

15 Appendix D The parties' terms of agreement on other subjects

These Clauses are agreed as part of the terms of in the Agreement. Accordingly, any matters or subjects not explicitly governed by the Clauses is governed by the remaining terms of the Agreement.

hello@seculyze.com | +45 21909575