Data Processing Agreement

Version 3.0, updated 13.12.2023

SoSafe GmbH | Lichtstr. 25a | 50825 Cologne | sosafe.de

1. Standard contractual clauses

The parties agree on the text of the Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council.

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with Article 28(3) and (4) of Regulation (EU) 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).

(b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.

(c) These Clauses apply to the processing of personal data as specified in Annex II.

(d) Annexes I to IV are an integral part of the Clauses.

(e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

Clause 2

Invariability of the Clauses

(a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.

(b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

Clause 3

Interpretation

(a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.

(c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

Clause 4

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 5

Docking clause

(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.

(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.

(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.

SECTION II

OBLIGATIONS OF THE PARTIES

Clause 6

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Clause7

Obligations of the Parties

7.1. **Instructions**

(a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.

(b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2. **Purpose limitation**

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3. **Duration of the processing of personal data**

Processing by the processor shall only take place for the duration specified in Annex II.

7.4. **Security of processing**

(a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

(b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5. **Sensitive data**

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6. **Documentation and compliance**

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.

(c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.

(d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7. **Use of sub-processors**

(a) GENERAL WRITTEN AUTHORISATION: The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 14 calendar days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

(b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.

(d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.

(e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8. **International transfers**

(a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under

Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.

(b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Clause 8

Assistance to the controller

(a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.

(b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions

(c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:

(1) the 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') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;

(2) the obligation to consult the competent supervisory authority/ies 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 controller to mitigate the risk;

(3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;

(4) the obligations in Article 32 of Regulation (EU) 2016/679.

(d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Clause 9

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles

34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 **Data breach concerning data processed by the controller**

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

(a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);

(b) in obtaining the following information which, pursuant to Article 33(3) of Regulation (EU) 2016/679, shall be stated in the controller's notification, and must at least include:

(1) 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;

(2) the likely consequences of the personal data breach;

(3) 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.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(c) in complying, pursuant to Article 34 of Regulation (EU) 2016/679, with the obligation to communicate without undue delay 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.

9.2 **Data breach concerning data processed by the processor**

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

(a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);

(b) the details of a contact point where more information concerning the personal data breach can be obtained;

(c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under Articles 33 and 34 of Regulation (EU) 2016/679.

SECTION III

FINAL PROVISIONS

Clause 10

Non-compliance with the Clauses and termination

(a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.

(b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:

(1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;

(2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;

(3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

(c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.

(d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

Annex I – List of Parties

Controller

[Identity and contact details of the controller(s), and, where applicable, of the controller's data protection officer]

Name: Insert the name of the Controller here

Address: Insert the address of the Controller here

Contact person's name, position and contact details:
Insert the contact person's name, position and contact details here

Signature and accession date:

Processor

SoSafe GmbH
Lichtstr. 25a
50825 Köln

Data Protection Officer:

Mr. Sebastian Herting
Herting Oberbeck Datenschutz GmbH
Hallerstraße 76
20146 Hamburg
E-Mail: dpo@sosafe.de

Felix Schürholz, Managing Director

Signature and accession date:

22 April 2024 | 08:37 PDT

DocuSigned by:
Felix Schürholz
6459695B96B249C...

DS
sosaf
SoSafe GmbH

Annex II – Description of the processing

1. Object

For purposes of its rendering of services, the Contractor in particular performs those activities for which personal information is processed (an exhaustive list can be found in the Main Contract):

(1) Conducting anonymous phishing simulations

Sending phishing mails:

- Based on the employee email addresses and employee names (hereafter: "**Users**") provided by the Client, the Contractor sends a defined number of email templates throughout a defined period of time.
- The email templates are personalized, i.e., they contain a personal address with the respective name of the user in order to simulate a realistic phishing attack.
- If desired by the Client, this service can be rendered in a more nuanced manner with additional categorizational criteria (e.g., organizational unit, location, status as a member of management). However, the groupings of recipients/users resulting from these categorizational criteria must always include at least five (5) persons.
- Each individual email also contains an identical link to an invisible image file (tracking pixel) that is downloaded when the email is opened.

Feedback to users when using learning pages via browser:

- The email templates each contain a unique, template-specific link (albeit identical for all the Client's users) that leads to a learning page hosted on a web server of the Contractor.
- Upon clicking on the link, the users are directed to the learning page and the respective email (without personalized address) is presented with an explanation of how it can be recognized as a phishing mail.

Use of the Phishing Report Button:

- An add-on for various email programs (such as Microsoft Outlook) can be optionally installed, with which users can report suspicious emails. If the respective email is from the simulation, the click is counted in the reporting rate of the evaluation, which is in turn recorded by the Contractor. Recorded data will be anonymized and only anonymized data will be send to the Client. If the email is not from the simulation, it is forwarded to an email addressed specified by the Client. In this case, no feedback or data flow are forwarded to the Contractor.

(2) Provision of an e-learning platform:

- Users can register for the e-learning portal on the Contractor's platform with their work email address at https://elearning.sosafe.de/registration and gain access to all e-learning modules available to them or provided by the Client. A short quiz can be taken in each module. A result is determined based on the answers (based on number of correct answers). This quiz can be repeated indefinitely.

- Alternatively, the e-learning modules can be provided to the Client as SCORM files to facilitate integration into an existing learning management system.

(3) Provision of an evaluation (Reporting Dashboard):

- The open, reply, input, and click rates (overall and per any defined grouping by categorizational criteria, see item 1.1 (1)) can be determined based on the total number of sent emails. This information is provided to the Client via an evaluation portal – however, personalized tracking is not possible as each organizational unit must include at least five (5) persons.
- If the Contractor's platform is used for e-learning, registration rates, module progress, and results of the e-learning quizzes are recorded for the individual users and (unless otherwise agreed) reported to the Client.
- When using the Phishing Report Button, the total and categorized report rate (i.e., how many emails from the simulation have been identified by users as phishing attempts) is also determined and reported to the Client.

2. Duration

The duration of processing by the Contractor depends on the duration of the Main Contract. The processing and this Contract on order-specific processing thus end when the Main Contract ends, provided there are no continuous obligations stemming from the terms of this Contract on order-specific processing or this Contract is not ended prematurely. The obligations from this contract beyond the order-specific processing apply for the respective period in the event that an "old" Main Contract is superseded or amended by a "new" Main Contract, with similar data protection requirements, associated with this Contract on order-specific processing, and processing of personal information is thus transitionally continued in the absence of a Main Contract. Uninterrupted processing for the order by the Contractor is agreed, unless the Parties regulate otherwise in the "superseding" or "amended" Main Contract. The duration of the processing is then based on the "superseding" or "amended" Main Contract.

3. Purpose of processing

The processing serves the following purpose: The Client is to be enabled to render the awareness building services purchased by the Contractor for the users.

4. Type of data

The following personal information is obtained and processed (according to the service specified in the Main Contract):

(1) Sending the phishing emails

- First and last names of users
- Academic level (optional)
- Work email addresses of users
- Sex of users (optional)
- Assigned user groups (e.g., organizational unit, location, role) of the Client
- Further categorizational criteria if required (see section 1.1)
- Language of users
- Browser/browser version and platform of users

- Participation in awareness building (= no opt-out as per section 5)

These data are stored in a secured database (see Annex III) for purposes of personalized sending. After completion of the services of the Main Contract, these data are irrevocably deleted.

(2) Feedback for users of learning pages on the Internet
- Visiting learning pages (without further data points such as IP addresses or geo-location data – these are either not retrieved or are deleted from the server log data via a regular mechanism)
- Number of tool tips/hint texts viewed
- Optional feedback evaluation or feedback free text

(3) E-learning platform

When registering on the e-learning platform and for continued use thereof:

- First and last name of the user
- Work email address of the user
- Language of the user
- Sex of the user
- Completion status of the individual e-learning modules per user
- Results of the module quizzes per user

For purposes of feedback to the Client:

- Names of registered users
- Completion status of all modules (aggregate)
- Average quiz result or percent accuracy of answers of quizzes (aggregate)
- Completion status of all modules per user
- Quiz value or percent accuracy of answers of quizzes per user (optional)

(4) Escalation Manager

If the Client has booked the Escalation Manager feature, the following personal information is obtained and processed. For escalation purposes it is also sent to the Client:

- First and last names, work email addresses, and assigned user groups of Client's users
- Individual completion status of all modules
- Deadline of the campaign
- Information whether the user has created an account or not (yes/no)
- Information if the user is new in training (user has registered in the last 90 days: yes/no)

(5) Server logs

The following technical information is stored in server logs for twelve (12) weeks to maximum six (6) months:

- IP addresses
- User agent
- URL visited
- Time

(6) Mail logs

The following technical information is stored in server logs for twelve (12) weeks:

- Email address
- Sender
- Receiving email server
- Time

5. Categories of data subjects

Data subjects are, unless otherwise defined in the Main Contract, all users specified for participation by the Client. The Client is free to facilitate non-participation for individual users via an opt-out process.

Annex III – Technical and organizational measures including technical and organisational measures to ensure the security of the data

The technical and organizational measures for ensuring data protection and data security, which the Contractor must at least establish and continuously uphold, are defined below. The goal in particular is the guarantee of confidentiality, integrity, and availability of the information subject to order-specific processing.

1. Anonymization

Personal information is not retrieved for purposes of the execution and processing of the Phishing Simulation. None of the behavioral data (e.g., clicks on links in the simulated phishing emails) are associated with personal information, but rather assigned randomly generated codes and stored in conjunction with these codes. This anonymization is automatically performed by the system (privacy-by-design approach).

2. Encryption

2.1 Data in transfer

All data transfers (both between the Client and the Contractor as well as between all employees of the Contractor) are encrypted in accordance with the recommendations for encryption from BSI. With the integration of AWS, we apply the recommended ELBSecurityPolicy-2016-08 from AWS predefined SSL security policies. This includes TLS 1.2 with SHA 256, ECDHE key exchange and ECDSA for authentication with AES 128 for encryption as a minimum requirement. Network access requires a VPN connection. Communication with service endpoints require a secure connection.

2.2 Data at rest

All personally identifiable Client and user data (e.g., user email addresses) are encrypted when stored in protected databases (authorization system, password policy with the aforementioned attributes, SSH certificate, access only possible via the internal IP area). Block storage encryption is used for data at rest using AWS SYMMETRIC_DEFAULT_Policy. This represents AES-256-GCM symmetric algorithm which is an industry standard for secure encryption. Data encrypted under AES-256-GCM is protected now and in the future as it is considered quantum resistant.

2.3 Data in use

The Contractor's solution concerns a pure cloud application with which the front end on the end user's computer is operated. This offers no possibility for encryption.

3. Confidentiality

3.1 Access control

The Contractor's office spaces are only accessible with the respective keys or transponders with matching security locks. The issuance of keys and transponders is documented and countersigned by the Contractor's management. Furthermore, there is in these spaces a reception or permanently present employees who ensure further access control. Video monitoring of all access points is also present.

3.2 Digital access control

There are specific requirements for the issuance of passwords (randomly generated, at least twelve (12) (usually longer where we use password managers) characters long, upper and lower case, numbers, and special characters) for all systems in which personal information is processed. These requirements are directly implemented in the systems via technical measures if possible. It is ensured that all authorized persons are informed that passwords must be stored securely and must not be disclosed to other parties. The appointed persons are instructed to only use unique passwords, i.e., passwords that the user does not use in any other (especially personal) systems. All clients are timed out after no more than five (5) minutes of inactivity. All clients possess an individual antivirus and firewall software with an automatic update function.

Two-factor authentication is used to ensure authorized access to server systems that process personal information. A hardware and software firewall is also used to secure the Contractor's company network, and the Contractor possesses a network and network zone concept. Mobile device management software is used, and VPN technology is employed for external access to the Contractor's company network.

3.3 Internal access control

Access to both the database systems and the application management system is granted on a need-to-know basis, i.e., the IT administrator issues the user rights as necessary only to those employees entrusted with the administration of campaigns. Every instance of internal access to the database systems is documented and regularly inspected by the IT administrator. This documentation is saved in a non-editable format. This comprises documentation of the granted authorizations. The authorizations for productive, testing, development, and administrative systems are granted separately.

3.4 Forwarding control

Data traffic with personal information is minimized and limited to the extent required to render the service. On the Contractor side, only the responsible project managers and IT administrators have access to the personal information.

A remote work regulation is in place. Personal information is processed in the front end of the SoSafe Management Software. All data transfers (both between the Client and the Contractor as well as between employees of the Contractor) to the SoSafe Management Software are https-encrypted via AES 256bit following our data in transit encryption definitions. Access to the databases is documented and regularly inspected by the IT administrator. Direct database access is only possible in the local company network of the Contractor, or via VPN when working remotely. All WiFi networks are encrypted with WPA2. No physical, external data storage media are used for business operations.

The Contractor's employees are bound to the prohibition on the betrayal of trade and business secrets as per the applicable law.

A bring-your-own-device (BYOD) regulation is in place. However, the Client's personal information that this Contract concerns is not stored on the Contractor's employees' private devices. The private devices (smartphones) solely serve the purpose of internal and external communication via email and collaboration tool (Microsoft Teams). The processing of the personal information concerned here is solely conducted via company devices (laptops and servers) to which the technical and organizational measures for data protection described herein apply.

3.5 Deletion of data

There is a standard process for deleting personal information, adherence to which is assessed by both the IT administrator as well as the responsible key account manager. Protective Class P4 as per DIN 66399 applies to the destruction of physical data.

3.6 Separation control

There is a separation of productive, testing/development, and administration systems. Database rights have been defined and there is a logical separation of clients in the software. . In addition, all accounts are separated by their workload. Storage, Compute, Network is independently handled for every account.

4. Integrity

Access to the databases of the productive systems is logged and saved for twelve (12) months.

5. Availability

5.1 Ensuring availability

A disaster recovery plan is available. We have a business continuity management plan in place. This is described in a business continuity management policy which is based on ISO 22301:2019 Business Continuity Management to maintain continuity of business process to operational status based on Minimum Business Continuity Output (MBCO). In addition, we use multiple availability zones within our cloud architecture. which ensures uptime also during an outage of a complete datacenter. Data is backed up on a daily basis. All applications are containerized and can be rebuild and deployed on demand.

5.2 Purpose limitation

There are order-specific data processing contracts with all service providers. All employees of the Contractor are continuously and comprehensively trained (seminars, e-learning, and interactive formats like quizzes) on the data protection requirements as well as fundamental information security topics.

6. Durability of systems

The productive systems and servers are continuously monitored by the service provider in order to ensure constant availability.

7. Reproduction following incident

The servers and productive systems are continuously ensured every day via full back-up. The back-ups are encrypted and stored on separate server systems of the service provider. Access is granted to the Contractor’s administrators. Each back-up is stored for 30 days.

8. Regular assessment of technical and organizational measures

An employee of the Contractor is appointed to be responsible for incident response management. For purposes of continuous improvement of the Contractor's information security, the technical and organizational measures for ensuring data protection and data security are continuously monitored, examined, and improved by the Contractor's management.

Annex IV – List of sub-processors

- Amazon Web Services EMEA SARL (Amazon Web Services, Inc. as the contractual party of the EU standard contractual clauses)

38 avenue John F. Kennedy, L-1855, Luxemburg

Hosting of all current and future components required for service provision, including API interface, database system as well as mail server for phishing simulation. We have taken the following measures to protect the data:

- Storage and processing of all data in certified data centers in Germany (Frankfurt a.M.).
- Encryption of all customer data using a master key generated by Processor, so that neither AWS nor any other third party can access customer data, either inside or outside the EU / EEA.
- Conclusion of a data processing agreement as well as the conclusion of the EU standard contractual clauses ((EU) 2021/915, 4.6.2021, module 2 and 3), incl. numerous obligations of AWS on handling and transparency in case of potential authority requests.
- Transfer Impact Assessment (TIA) conducted by an external data protection expert.
- Data protection expert opinion on Processor's use of AWS, which can be provided upon request.

- Hetzner Online GmbH

Industriestr. 25, 91710 Gunzenhausen

Use of mail services for the Phishing Simulation from SoSafe GmbH. If explicitly agreed with the Controller individually: Provision of the API interface.

ISO27001 certificate for datacenters: https://www.hetzner.de/pdf/FOX_Zertifikat.pdf

- salesforce.com Germany GmbH

Mail: Salesforce.com Sarl, Route de la Longeraie 9, Morges, 1110, Switzerland, attn: Director, EMEA Sales Operations, Legal Department: Erika-Mann-Strasse 31-37, 80636, Munich, Germany

Provision of support software (Customer Service Cloud) for customer service (support form or email to support@sosafe.de). This provider is only relevant for the Controller if the Controller uses SoSafe's customer support.

More information: https://trust.salesforce.com/

ISO27001 certificate can be accessed here: https://compliance.salesforce.com/en/iso-27017. In addition, the following measures have been taken:

- Storage and processing of all data in certified data centers in Germany (Frankfurt a.M.).
- Encryption of all data with industry-standard encryption products during transfers as well as at rest.
- Conclusion of a data processing agreement incorporating the approved Binding Corporate Rules (BCR) concluded by Salesforce for its group companies and subcontractors as well as the 2021 EU standard contractual clauses with numerous obligations vis-à-vis the competent supervisory authority as well as further voluntary commitments.

- Transfer Impact Assessment (TIA) conducted by an external data protection expert.

- Microsoft Ireland Operations Ltd

One Microsoft Place, South County Business Park Leopardstown Dublin 18, D18 P521

Provision of an email server infrastructure for customer communication in support cases via the support software (support form or email to support@sosafe.de). This provider is only relevant to the Controller if the Controller uses SoSafe's customer support. The following measures have been taken:

- All data are processed and stored exclusively within the European Union as part of the Azure EU Cloud.
- All datacenters are ISO27001- and ISO27018-certified: https://docs.microsoft.com/de-de/azure/security/fundamentals/infrastructure.
- Encryption of all data using industry-standard encryption products during transfers as well as at rest.
- Implementation of the Customer Lockbox, which ensures that Microsoft cannot access content without the Processor's explicit consent.
- Conclusion of a data processing agreement as well as conclusion of the EU standard contractual clauses ((EU) 2021/915, 4.6.2021, module 2 and 3).
- Transfer Impact Assessment (TIA) conducted by an external data protection expert.

- Kombo Technologies GmbH (Optional)

Lohmühlenstraße 65, 12435 Berlin, Germany

Integration of Client Active Directory. This provider is only required to the extent that the Client requests Active Directory integration for automated uploading and regular updating of end-user data on the Contractor platform. The following measures have been taken:

- All data are processed and stored exclusively within the European Union. Server hosting provider: Google Cloud EMEA Limited.
- Kombo Technologies GmbH is ISO27001 certified. Access can be requested here: https://security.kombo.dev/?itemUid=1fed9faa-4a87-427c-9a95-96b4d6bf66b7&source=click/. More information about Technical and Organizational Security Measures of Kombo Technologies GmbH can be found at security.kombo.dev.
  - Encryption
    - All customer data is encrypted using symmetric AES-256 encryption at rest, including backup copies.
    - Data in transit: All outgoing traffic (to integration APIs) uses the highest TLS version available by the respective integration's API (e.g., Google Workspace). All incoming traffic via the Kombo API is enforced to use TLS 1.3. Connections from Kombo's application workloads to Kombo's database also use TLS 1.3 with an AES-256 cipher.
- Conclusion of a data processing agreement.

SoSafe GmbH | Lichtstr. 25a | 50825 Cologne | Managing Directors: Dr. Niklas Hellemann,
Lukas Schaefer, Felix Schürholz, Felix Fichtl | HRB96220 | Amtsgericht Köln | VAT ID: DE322382415 |
Visitor address and parking: Lichtstr. 25a | 50825 Cologne | Tel: +49 (0) 221 6508 3800 |
Email: info@sosafe.de | Web: sosafe.de