Data Processing Agreement

Version 3.2, updated January 2, 2025

SoSafe SE | 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

The contact person designated by the Customer in the SoSafe Manager after signing the Main Contract will be the primary recipient of communications.

Until such person is specified, communications will be directed to the Customer's Administrator as specified in the SoSafe Manager, at the latest by the start of the implementation of the Awareness Building Services.

Processor

SoSafe SE
Lichtstr. 25a
50825 Köln

Data Protection Officer:

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

Note: Please provide a copy of any communication to privacy@sosafe.de

Annex II – Description of the processing

1. Object

Processor's services which form the basis of Processor's processing activities pursuant to this Data Processing Agreement are specified in detail in the Main Contract. Processing of personal data upon Controller's instructions within the scope of this Data Processing Agreement specifically relates to the following:

Delivery of a Software-as-a-Service human risk management, training and user testing platform. As per Controller's selection of discrete SoSafe Awareness Building Services, Users of the Controller or its Affiliates under the Main Contract will gain access to social engineering simulations (e.g. phishing, smishing, vishing), questionnaires, tests, optional AI-powered chatbots and tooling and other user-centric risk profiling mechanisms. Security awareness training, analytics, feedback mechanisms and technical and procedural interventions may be automatically or manually triggered, as configured by the Controller, or otherwise delivered as a result of User interaction with the Platform or data ingested by the Platform via technical integrations with other Controller business systems, as implemented or otherwise specified by the Controller.

The Platform may build a personalised profile of a User and target automated actions to report on or improve the secure behaviours of the User, subject to anonymisation settings selected by the Controller.

2. Duration

The duration of processing by the Processor depends on the duration of the Main Contract. The processing and this Contract on order-specific processing thus end when the Main Contract (plus the applicable retention phase after contract termination in accordance with the deletion concept) 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.

3. Purpose of processing

The processing serves the following purpose: The Processor is to be enabled to render the Awareness Building Services purchased by the Controller for the Users.

4. Types of data

The following types of personal data, all in relation to Users, are processed by Processor on behalf of the Controller within the scope of providing the Awareness Building Services as further specified in the Main Contract.

(1) Registration and Account Management Data

All Awareness Building Services process certain data types required from Users to register for the Awareness Building Services and to manage the Awareness Building Services and account on behalf of the Controller ("**Registration and Account Management Data**"), which in particular include:

- First and last name;
- Business email address;

- Assigned User groups (e.g., organizational unit, location, role), access levels;
- Optional User preferences such as language and salutation

(2) Usage Data

In addition to Registration and Account Management Data, depending on the chosen Awareness Building Services, further data types related to Users may be processed to operate and deliver the Awareness Building Services, as further specified in the Main Contract, which in particular include:

- User scoping and tailoring information such as role, department, level of initial knowledge, responses to introductory questionnaires;
- User activity on the platform such as training initiation and completion, test scores, interaction with tests;
- Escalation information (e.g. line manager relationships);
- Optional AI modules: interaction with AI-powered chatbots and tooling to the extent they contain personal data based on the input received by Processor from the Controller's User of the AI module.
- Optional PhishFeedback module: user region settings (e.g. language, timezone) and reported email, which each may contain personal data.

(3) Technical Data

Data relating to Users required for the operation of the application and infrastructure and meeting the commitments of our Technical and Organizational Measures, which in particular include:

- User system information required by the application such as browser version and platform, user agent information;
- Network data such as IP address, timestamp, URL and API endpoints accessed;
- Mail data such as sender and receiver addresses, routing information and timestamps;
- Data gathered from integrations requested or implemented by the Controller that may include organisation or User data, such as alerts from data loss prevention (DLP) tooling, endpoint detection and response agents.

5. Categories of data subjects

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

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

The technical and organizational measures for ensuring data protection and data security, which the Processor 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. Configurable anonymisation and purpose-based access to data

All Processor services can be configured in a manner that provides Customer Administrators with anonymized aggregated access to user data only by default. Access for specific Controller personnel on an individual level may be configurable when clearly and explicitly requested by the Controller.

2. Encryption

2.1 Data in transfer

All data transfers (both between the Controller and the Processor as well as between all employees of the Processor) are strongly encrypted in accordance with industry good practice, such as ECC with Curve25519, RSA with a key of 2048bits or longer, updated as the state of the art progresses. SoSafe internal network and administrative access is strongly encrypted. Communication with service endpoints require a secure connection.

2.2 Data at rest

All personally identifiable Controller and User data are appropriately encrypted by the Platform at the storage level using strong industry good practice algorithms and implementations, such as AES-256-GCM or stronger.

2.3 Data in use

The Processor'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 Physical access control

The Processor'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 Processor's management. Appropriate intruder alarms, CCTV coverage and response procedures are in place. SoSafe offices provide no special network access rights beyond access to the internet.

The SoSafe Platform is hosted by industry leading hyperscale Cloud Service Providers. These providers operate from data centers implementing appropriate physical and environmental security controls, such as but not limited to:

- Tracking and monitoring of all visitor access and staff movement

- CCTV monitoring with 90 days retention period
- Strong access control to all data hosting, networking and mechanical and environmental spaces
- At least N+1 redundancy of power, networking and environmental services

Cloud Service Providers must have ISO 27001 and/or SOC2 accreditation, or similar. SoSafe assesses their physical security through review of audit and accreditation materials.

3.2 Logical access control

All logical access requires multi-factor authenticated VPN connection. The office networks confer no special network privileges beyond access to the internet. Authentication to SoSafe business systems is via SSO requiring multi-factor authentication and strong, policy-defined passwords according to industry good practice. All systems access, including access to Customer data, is provided on an auditable, scoped, need-to-know basis only. Internal user access rights are regularly reviewed.

3.3 Endpoint security

All end user devices are securely configured by Mobile Device Management enforcing all controls and use Endpoint Detection and Response agents. Full disk encryption is in place. End user devices are timed out after no more than five (5) minutes of inactivity. All end user devices possess an individual antivirus and firewall software with an automatic update function. End user device operating system and key software package version updates are appropriately managed.

3.4 Forwarding control

Data traffic with personal information is minimized and limited to the extent required to render the service. On the Processor side, only the relevant and necessary personnel have scoped access to personal information (on a need-to-know basis).

A remote work policy and appropriate controls are in place. Personal data is not permitted to be stored on end user devices. All employees are contractually bound to maintain confidentiality and protect business secrets.

A Bring Your Own Device (BYOD) risk assessment has been performed under ISO 27001 and a relevant policy is in place to limit the use of and risks posed by BYOD. Appropriate centrally managed controls are in place.

3.5 Deletion of data

Logical data destruction is provided by the underlying Cloud Service Providers that are deployed by the Processor, according to industry good practice.

System logs and security data may be retained for up to 12 months from point of creation to enable appropriate security incident response and forensics. System backups are appropriately protected and any User data within will be deleted within 12 months of creation, as per backup policies of the Processor.

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, enforced by database logic.

4. Integrity

Access to the databases of the productive systems is logged and saved for twelve (12) months. Appropriate backup and recovery procedures are in place to protect data integrity. Access to the database is restricted on a role-basis.

5. Availability

5.1 Business Continuity

The productive systems and servers are continuously monitored by the Processor to ensure constant availability. Processor operates an appropriate architecture and business continuity system under ISO 27001 audit and accreditation sufficient to meet the SLAs defined in the Main Contract. 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 Processor. Access is solely granted to the Processor's administrators.

5.2 Security awareness & training

All employees of the Processor 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. Incident management

Processor operates appropriate security monitoring, incident detection and response measures, including technical logging and automated auditing controls, a Security Operations team and capability and organisation-wide incident response processes. All significant security incidents including near-misses require a formal retrospective and root cause analysis.

7. Information Security Management System

Processor operates a formal Information Security Management System (ISMS) according to ISO 27001 requirements and externally audited and accredited to the same. The Processor also obtains further industry accreditations such as TISAX as required. Formal risk assessment and management policies and procedures are operated by the Security organisation, with regular scheduled input and reporting to the Security Committee comprising relevant Security and Executive Team members. The ISMS is formally sponsored and supported by the Executive Team and the CEO.

The ISMS and all Security functions are operated by an appropriately resourced Security organisation led by a Chief Information Security Officer.

8. Regular assessment of technical and organizational measures

All relevant Security, privacy and operational processes are internally audited by expert, qualified auditors on an annual basis, with input into the ISMS and Security Committee. Processor's ISMS is formally externally audited by a credible professional firm at least once a year.

Annex IV – List of sub-processors

Please visit https://sosafe-awareness.com/legal/sub-processors/ for an up-to-date list of our sub-processors, processing activities and protections in place.