



This is a translation for your convenience. Only the German version is legally binding. [Go to the German version](#)

Data processing agreement under Art. 28 GDPR

Version as of 02.10.2026 (version 1.0) · between the customer (holder of the company account) and secureIT UG (haftungsbeschränkt)

Note: This agreement is concluded upon registration of a company account with secureIT. No signature is required. This document serves as proof for your records and for your data protection officer.

Preamble

The client (the organisation that creates a company account with secureIT, hereinafter the “Customer”) uses the secureIT platform of secureIT UG (haftungsbeschränkt), Weinstraße 9, 79282 Ballrechten-Dottingen, represented by its managing director Patrick Ihle (hereinafter the “Contractor”), for awareness training and phishing simulations for its employees. In doing so, the Contractor processes personal data on behalf of the Customer. This agreement governs the rights and obligations of both parties pursuant to Art. 28 GDPR. It is concluded upon registration of a company account and applies to all training courses and simulations started via this account.

§ 1 Subject matter and duration

(1) The subject matter is the provision of the online training, the sending of simulated phishing e-mails, the recording of the reactions to them, the preparation of team evaluations, certificates of participation and proofs of training, and, optionally, monthly refresher lessons.

(2) The agreement applies for the duration of the company account. It ends upon deletion of the account by the Customer or upon termination of the terms of use.

§ 2 Nature and purpose of the processing, types of data, data subjects

(1) **Purpose:** Training and awareness-raising of the Customer’s employees with regard to phishing and information security; proof of this training vis-à-vis insurers, clients and supervisory authorities.

(2) **Types of data:** first name, surname, business e-mail address; personal access link; learning progress (lessons completed with time, completion date, learning path, result of the knowledge test, questions asked about lessons); for each simulated e-mail, the time of sending and whether it was opened, whether a link was clicked and whether an entry was made on the practice page; technical data arising in this context (IP address, e-mail client, time); certificate number and date. Passwords entered are not stored.

(3) **Data subjects:** employees and other persons entered by the Customer (such as apprentices, temporary staff, external staff with a business mailbox) as well as the Customer’s administrators.

§ 3 Obligation to follow instructions

(1) The Contractor processes the data exclusively within the scope of this agreement and in accordance with the documented instructions of the Customer. The Customer issues instructions via the functions of the platform (entering persons, starting training, stopping a test run, deleting persons) or in text form to the address stated in the Legal notice.

(2) If the Contractor considers an instruction to be unlawful, it shall inform the Customer without undue delay and may suspend its execution until it is confirmed.

(3) The Contractor does not use the data for its own purposes, in particular not for advertising, and does not pass it on to third parties unless this agreement provides otherwise.

§ 4 Confidentiality and restriction of access

(1) The Contractor is a one-person business. Only the managing director, who has undertaken to maintain confidentiality and is subject to data secrecy, has access to the data. If employees or contractors are engaged in future, they will be obliged in writing





to maintain confidentiality before being given access.

(2) The Contractor does not make individual results of the phishing simulation (which person opened, clicked on or replied to which e-mail) available to the Customer. The Customer receives exclusively anonymised team evaluations, which require a minimum size of three persons. The Contractor itself has access to individual data for maintenance and support purposes; this access is logged.

§ 5 Technical and organisational measures

The Contractor implements the technical and organisational measures described in the Annex pursuant to Art. 32 GDPR and continuously develops them further. Measures may be replaced by equivalent measures; the level of protection must not be reduced in the process.

§ 6 Sub-processors

(1) The Customer consents to the use of the following sub-processors:

- **IONOS SE**, Elgendorfer Str. 57, 56410 Montabaur, Germany: hosting of the platform and the database, sending and receiving of e-mails. Processing exclusively in data centres in Germany.
- **ElevenLabs Inc.**, New York, USA: speech synthesis for individual simulation templates with a voice message. Only the text to be read out is transmitted, which contains at most the first name of the data subject. The basis for the transfer to a third country is the EU-US Data Privacy Framework, insofar as the provider is certified under it, and otherwise the EU Standard Contractual Clauses. It is used only if the Customer selects such a template.

(2) The Contractor informs the Customer of any change or addition of further sub-processors at least four weeks in advance by e-mail to the administrator address. The Customer may object within this period for good cause; if no agreement is reached, the Customer may terminate the company account.

§ 7 Assistance to the Customer

(1) The Contractor assists the Customer in responding to requests from data subjects (access, rectification, erasure, restriction, data portability). The Customer can carry out erasures and rectifications for individual persons directly in the platform.

(2) The Contractor assists the Customer with a data protection impact assessment and with enquiries from supervisory authorities, insofar as the processing under this agreement is concerned.

§ 8 Notification of personal data breaches

The Contractor notifies the Customer of any personal data breach affecting the Customer's data without undue delay, at the latest within 24 hours of becoming aware of it, to the administrator address. The notification contains, as far as known, the nature and extent of the breach, the persons and data concerned, the likely consequences and the measures taken. The Customer's deadline under Art. 33 GDPR (72 hours) remains unaffected; the Contractor assists with the notification.

§ 9 Deletion and return

(1) After the end of the agreement, the Contractor deletes all of the Customer's data within 30 days, unless a statutory retention obligation precludes this (such as invoice data under § 147 AO (German Fiscal Code) and § 257 HGB (German Commercial Code)). Before that, the Customer can download team evaluations and proofs of training as PDF files.

(2) During the term of the agreement, the Customer can delete individual persons at any time; the deletion covers the access data, learning progress and simulation results of that person. Certificates already issued retain their verification number so that proofs that have been presented remain verifiable; the Customer can also request their deletion.

(3) Data backups are overwritten according to a fixed cycle; deleted data thus also disappears from the backups no later than 30 days after deletion.

§ 10 Evidence and inspections

(1) The Contractor demonstrates compliance with its obligations by means of the Annex to this agreement, the record of





processing activities and, on request, a written self-disclosure.

(2) After reasonable notice (at least 14 days), the Customer may carry out inspections during normal business hours or have them carried out by an auditor bound to secrecy, at most once per calendar year unless there is a specific reason. The Contractor's effort for inspections going beyond the self-disclosure is remunerated on a time-and-effort basis.

§ 11 Responsibility of the Customer

As the controller, the Customer is responsible for ensuring that the processing is lawful, in particular for the legal basis vis-à-vis its employees (as a rule § 26(1) BDSG (German Federal Data Protection Act), Art. 6(1)(f) GDPR), for informing the employees pursuant to Art. 13 GDPR and, where a works council exists, for its participation pursuant to § 87(1) no. 6 BetrVG (German Works Constitution Act). For this purpose, the Contractor provides an information sheet and a model works agreement and includes the information for employees in the invitation e-mail.

§ 12 Liability and final provisions

(1) Liability is governed by Art. 82 GDPR and the terms of use.

(2) The Contractor notifies the Customer of amendments to this agreement by e-mail; the currently valid version is available at secureit.icu/auftragsverarbeitung. German law applies. Should any provision be invalid, the remainder of the agreement remains valid.

Annex: Technical and organisational measures (Art. 32 GDPR)

Physical access and system access control: Operation in an ISO 27001-certified IONOS data centre in Germany. Server access only via SSH with a key over a non-standard port, automatic blocking after repeated failed attempts. Administrative access to the platform only with a verified e-mail address and password; sessions expire.

Data access control: Role model (superadmin, company administrator, supporting partner, teacher, participants). Company administrators see only their own organisation; individual simulation results cannot be retrieved by them. Access by supporting partners is logged with name and time.

Transfer and transport control: All connections exclusively via TLS (HTTPS). E-mails sent via our own mail server with SPF, DKIM and DMARC. No transfer of participant data to third parties other than the sub-processors named.

Input control: Security-relevant actions (start of training, control of test runs, deletions, invoices, partner access) are recorded in an audit log with user, time and IP address.

Data minimisation: Only name and business e-mail address are collected. Passwords entered on the practice pages are discarded; only the fact that an entry was made is stored. The website statistics work without cookies and without user profiles.

Availability control: Daily backups of the database, retention according to a fixed cycle, tested recoverability; security updates for the server are installed promptly.

Separation control: Data of different customers is logically separated by organisation identifiers; every query is restricted to the customer's own organisation. Test and production systems are separate; test data is not mixed with real data.

Organisation: Record of processing activities pursuant to Art. 30 GDPR; documented procedure for security incidents; regular review of the measures and of the platform for vulnerabilities; deletion concept in accordance with § 9 of this agreement.

