



Cette traduction est fournie à titre indicatif. Seule la version allemande fait foi. [Voir la version allemande](#)

Accord de sous-traitance selon l'art. 28 du RGPD

Version du 02.10.2026 (version 1.0) · entre le client (titulaire du compte entreprise) et secureIT UG (haftungsbeschränkt)

Remarque : Le présent accord est conclu lors de l'inscription d'un compte entreprise auprès de secureIT. Aucune signature n'est requise. Ce document sert de justificatif pour vos dossiers et pour votre délégué à la protection des données.

Préambule

Le donneur d'ordre (l'organisation qui crée un compte entreprise chez secureIT, ci-après le « client ») utilise la plateforme secureIT de secureIT UG (haftungsbeschränkt), Weinstraße 9, 79282 Ballrechten-Dottingen, représentée par son gérant Patrick Ihle (ci-après le « prestataire »), pour des formations de sensibilisation et des simulations de phishing destinées à ses salariés. Dans ce cadre, le prestataire traite des données à caractère personnel pour le compte du client. Le présent accord régit les droits et obligations des deux parties conformément à l'art. 28 du RGPD. Il est conclu lors de l'enregistrement d'un compte entreprise et s'applique à toutes les formations et simulations lancées via ce compte.

§ 1 Objet et durée

(1) L'objet est la mise à disposition de la formation en ligne, l'envoi d'e-mails de phishing simulés, l'enregistrement des réactions à ceux-ci, l'établissement d'évaluations d'équipe, de certificats de participation et d'attestations de formation ainsi que, en option, des leçons de rappel mensuelles.

(2) L'accord s'applique pendant toute la durée du compte entreprise. Il prend fin avec la suppression de celui-ci par le client ou avec la fin de l'accord d'utilisation.

§ 2 Nature et finalité du traitement, catégories de données, personnes concernées

(1) **Finalité :** formation et sensibilisation des salariés du client au phishing et à la sécurité de l'information, justification de cette formation auprès des assureurs, des donneurs d'ordre et des autorités de contrôle.

(2) **Catégories de données :** prénom, nom, adresse e-mail professionnelle ; lien d'accès personnel ; progression de l'apprentissage (leçons suivies avec horodatage, date d'achèvement, parcours d'apprentissage, résultat du test de connaissances, questions posées sur les leçons) ; pour chaque e-mail simulé, la date et l'heure d'envoi ainsi que le fait qu'il a été ouvert, qu'un lien a été cliqué et qu'une saisie a été effectuée sur la page d'exercice ; les données techniques générées à cette occasion (adresse IP, logiciel de messagerie, horodatage) ; numéro et date du certificat. Les mots de passe saisis ne sont pas enregistrés.

(3) **Personnes concernées :** les salariés et autres personnes inscrites par le client (par exemple apprentis, intérimaires, collaborateurs externes disposant d'une boîte de messagerie professionnelle) ainsi que les administrateurs du client.

§ 3 Soumission aux instructions

(1) Le prestataire traite les données exclusivement dans le cadre du présent accord et selon les instructions documentées du client. Le client donne ses instructions via les fonctions de la plateforme (inscrire des personnes, lancer une formation, arrêter une campagne de test, supprimer des personnes) ou sous forme textuelle à l'adresse indiquée dans les mentions légales.

(2) Si le prestataire estime qu'une instruction est illicite, il en informe le client sans délai et peut en suspendre l'exécution jusqu'à sa confirmation.

(3) Le prestataire n'utilise pas les données à ses propres fins, en particulier pas à des fins publicitaires, et ne les transmet pas à des tiers, sauf disposition contraire du présent accord.

§ 4 Confidentialité et restriction de l'accès

(1) Le prestataire est une entreprise unipersonnelle. Seul le gérant, qui s'est engagé à la confidentialité et est soumis au secret des données, a accès aux données. Si, à l'avenir, des salariés ou des prestataires sont employés, ils seront engagés par écrit à





la confidentialité avant tout accès.

(2) Le prestataire ne met pas à la disposition du client les résultats personnels de la simulation de phishing (quelle personne a ouvert, cliqué ou répondu à quel e-mail). Le client reçoit exclusivement des évaluations d'équipe anonymisées, qui supposent un effectif minimal de trois personnes. Le prestataire lui-même a accès aux données individuelles à des fins de maintenance et d'assistance ; cet accès est journalisé.

§ 5 Mesures techniques et organisationnelles

Le prestataire met en œuvre les mesures techniques et organisationnelles décrites en annexe conformément à l'art. 32 du RGPD et les fait évoluer en permanence. Les mesures peuvent être remplacées par des mesures équivalentes, sans que le niveau de protection ne puisse diminuer.

§ 6 Sous-traitants ultérieurs

(1) Le client consent au recours aux sous-traitants ultérieurs suivants :

- **IONOS SE**, Elgendorfer Str. 57, 56410 Montabaur, Allemagne : hébergement de la plateforme et de la base de données, envoi et réception d'e-mails. Traitement exclusivement dans des centres de données situés en Allemagne.
- **ElevenLabs Inc.**, New York, États-Unis : synthèse vocale pour certains modèles de simulation comportant un message vocal. Seul le texte à lire est transmis, lequel contient au plus le prénom de la personne concernée. Le transfert vers un pays tiers repose sur l'EU-US Data Privacy Framework, dans la mesure où le fournisseur y est certifié, et à défaut sur les clauses contractuelles types de l'UE. Il n'y est recouru que si le client sélectionne un tel modèle.

(2) Le prestataire informe le client de tout changement ou de l'ajout d'autres sous-traitants ultérieurs au moins quatre semaines à l'avance par e-mail adressé à l'adresse de l'administrateur. Le client peut s'y opposer pour un motif grave dans ce délai ; à défaut d'accord, le client peut mettre fin au compte entreprise.

§ 7 Assistance au client

(1) Le prestataire assiste le client dans le traitement des demandes des personnes concernées (accès, rectification, effacement, limitation, portabilité des données). Le client peut procéder directement dans la plateforme aux effacements et rectifications concernant des personnes individuelles.

(2) Le prestataire assiste le client lors d'une analyse d'impact relative à la protection des données et pour les demandes des autorités de contrôle, dans la mesure où le traitement relevant du présent accord est concerné.

§ 8 Notification des violations de données à caractère personnel

Le prestataire notifie au client toute violation de données à caractère personnel concernant des données du client sans délai, au plus tard dans les 24 heures après en avoir pris connaissance, à l'adresse de l'administrateur. La notification contient, dans la mesure où ils sont connus, la nature et l'étendue de la violation, les personnes et données concernées, les conséquences probables et les mesures prises. Le délai imparti au client en vertu de l'art. 33 du RGPD (72 heures) n'est pas affecté ; le prestataire assiste le client pour la notification.

§ 9 Effacement et restitution

(1) À la fin de l'accord, le prestataire efface toutes les données du client dans un délai de 30 jours, sauf obligation légale de conservation contraire (par exemple pour les données de facturation en vertu du § 147 AO (code fiscal allemand) et du § 257 HGB (code de commerce allemand)). Auparavant, le client peut télécharger les évaluations d'équipe et les attestations de formation au format PDF.

(2) Pendant la durée de l'accord, le client peut supprimer à tout moment des personnes individuelles ; la suppression porte sur les données d'accès, la progression de l'apprentissage et les résultats de simulation de la personne concernée. Les certificats déjà délivrés conservent leur numéro de vérification, afin que les attestations présentées restent vérifiables ; le client peut également exiger leur effacement.

(3) Les sauvegardes de données sont écrasées selon un cycle fixe ; les données effacées disparaissent ainsi également des sauvegardes au plus tard 30 jours après leur effacement.





§ 10 Justificatifs et contrôles

(1) Le prestataire justifie du respect de ses obligations au moyen de l'annexe au présent accord, du registre des activités de traitement et, sur demande, d'une auto-déclaration écrite.

(2) Le client peut, moyennant un préavis raisonnable (d'au moins 14 jours), effectuer des contrôles pendant les heures d'ouverture habituelles ou les faire effectuer par un auditeur tenu au secret, au maximum une fois par année civile, sauf motif concret. Les frais engagés par le prestataire pour des contrôles allant au-delà de l'auto-déclaration sont rémunérés en fonction du temps passé.

§ 11 Responsabilité du client

En sa qualité de responsable du traitement, le client est tenu de veiller à la licéité du traitement, en particulier quant à la base juridique à l'égard de ses salariés (en règle générale le § 26, al. 1 BDSG (loi fédérale allemande sur la protection des données), art. 6, par. 1, point f) du RGPD), à l'information des salariés conformément à l'art. 13 du RGPD et, s'il existe un comité social et économique (CSE, Betriebsrat), à sa participation conformément au § 87, al. 1, n° 6 BetrVG (loi allemande sur l'organisation des entreprises). Le prestataire met à cet effet à disposition une fiche d'information et un modèle d'accord d'entreprise et intègre l'information des salariés dans l'e-mail d'invitation.

§ 12 Responsabilité et dispositions finales

(1) La responsabilité est régie par l'art. 82 du RGPD et par les conditions d'utilisation.

(2) Le prestataire communique au client par e-mail toute modification du présent accord ; la version en vigueur peut être consultée à l'adresse secureit.icu/auftragsverarbeitung. Le droit allemand est applicable. Si une disposition devait être invalide, le reste de l'accord demeure valable.

Annexe : Mesures techniques et organisationnelles (art. 32 du RGPD)

Contrôle de l'accès physique et de l'accès aux systèmes : exploitation dans un centre de données IONOS certifié ISO 27001 en Allemagne. Accès au serveur uniquement par SSH avec clé via un port non standard, blocage automatique en cas de tentatives infructueuses répétées. Accès d'administration à la plateforme uniquement avec une adresse e-mail vérifiée et un mot de passe ; les sessions expirent.

Contrôle de l'accès aux données : modèle de rôles (super-administrateur, administrateur d'entreprise, partenaire accompagnateur, enseignant, participants). Les administrateurs d'entreprise ne voient que leur propre organisation ; les résultats de simulation personnels ne leur sont pas accessibles. Les accès des partenaires accompagnateurs sont journalisés avec le nom et l'horodatage.

Contrôle de la transmission et du transport : toutes les connexions exclusivement via TLS (HTTPS). Envoi des e-mails via notre propre serveur de messagerie avec SPF, DKIM et DMARC. Aucune transmission de données des participants à des tiers, à l'exception des sous-traitants ultérieurs mentionnés.

Contrôle de la saisie : les actions pertinentes pour la sécurité (lancement d'une formation, pilotage des campagnes de test, suppressions, factures, accès des partenaires) sont consignées dans un journal d'audit avec l'utilisateur, l'horodatage et l'adresse IP.

Minimisation des données : seuls le nom et l'adresse e-mail professionnelle sont collectés. Les mots de passe saisis sur les pages d'exercice sont rejetés ; seul le fait qu'une saisie a eu lieu est enregistré. Les statistiques du site web fonctionnent sans cookies et sans profils d'utilisateurs.

Contrôle de la disponibilité : sauvegardes quotidiennes de la base de données, conservation selon un cycle fixe, capacité de restauration vérifiée ; les mises à jour de sécurité du serveur sont installées rapidement.

Contrôle de la séparation : les données des différents clients sont séparées logiquement par des identifiants d'organisation ; chaque requête est limitée à l'organisation concernée. Les systèmes de test et de production sont séparés, les données de test ne sont pas mélangées avec des données réelles.

Organisation : registre des activités de traitement conformément à l'art. 30 du RGPD ; procédure documentée en cas d'incident de sécurité ; vérification régulière des mesures et de la plateforme quant aux vulnérabilités ; concept d'effacement





secureIT

Daten und User schützen. Mit Sicherheit.

conformément au § 9 du présent accord.



secureIT

Daten und User schützen. Mit Sicherheit.