Accord sur le traitement des données	Data Processing Agreement
Entre : ci-après : **Client** et **SoSafe GmbH** **Lichtstr. 25a** **50825 Köln** ci-après : **Prestataire**	Between: hereafter: **Client** and **SoSafe GmbH** **Lichtstr. 25a** **50825 Köln** hereafter: **Contractor**
Version 2.5, mise à jour le 02.10.2023	Version 2.5, updated 02.10.2023
1. Introduction, champ d'application, définitions	**1. Introduction, purview, definitions**
(1) Le présent Accord sur le Traitement des Données, relatif au traitement spécifique des données personnelles dans le cadre d'une commande (ci-après dénommé "**Contrat**"), régit les droits et obligations du Client et du Prestataire en ce qui concerne le traitement des informations personnelles dans le cadre d'une commande. (2) Le Contrat s'applique à toutes les activités pour lesquelles le Prestataire ou les sous-traitants désignés par le Prestataire traitent des informations personnelles du Client.	(1) This Data Processing Agreement concerning order-specific processing of personal data (hereafter: "**Contract**") regulates the rights and obligations of the Client and Contractor with regard to the processing of personal information for purposes of an order. (2) This Contract applies to all activities for which the Contractor or subcontractors appointed by the Contractor process personal information of the Client.

(3) Les termes utilisés dans le Contrat sont définis conformément à leur définition dans le Règlement général sur la protection des données de l'UE (ci-après : "**RGPD**"). (4) La prestation de services spécifique (ainsi que l'extraction, le traitement et l'utilisation des données à caractère personnel) repose sur le contrat conclu entre les parties, relatif à la prestation de services de sensibilisation (ci-après dénommé "**Contrat principal**").	(3) Terms used in this Contract are defined in accordance with their definition in the EU General Data Protection Regulation (hereafter: "**GDPR**"). (4) The specific rendering of services (as well as the necessary retrieval, processing, and use of personal data) is based on the contract formed between the parties concerning the rendering of awareness-building services (hereafter: "**Main Contract**").
2. Objet et durée du traitement	**2. Object and duration of processing**
2.1 Objet Dans le cadre de sa prestation de services, le Prestataire exerce notamment les activités pour lesquelles des informations personnelles sont traitées (une liste exhaustive figure dans le contrat principal) : (1) Réalisation de simulations d'hameçonnage anonyme Envoi de courriers d'hameçonnage : • Sur la base des adresses électroniques et des noms des employés (ci-après dénommés "**Utilisateurs**") fournis par le Client, le Prestataire envoie un nombre défini de modèles d'e-mails pendant une période déterminée. • Les modèles d'e-mails sont personnalisés, c'est-à-dire qu'ils contiennent une adresse personnelle avec le nom de l'utilisateur correspondant, afin de simuler une attaque d'hameçonnage réaliste. • Si le Client le souhaite, ce service peut être rendu de manière plus nuancée avec des critères de	2.1 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

catégorisation supplémentaires (par exemple, unité organisationnelle, localisation, statut de membre de la direction). Toutefois, les regroupements de destinataires/utilisateurs résultant de ces critères de catégorisation doivent toujours comprendre au moins cinq (5) personnes. • Chaque email individuel contient également un lien identique vers un fichier image invisible (pixel de suivi) qui est téléchargé lorsque le courriel est ouvert. Retour d'information aux utilisateurs lors de l'utilisation des pages d'apprentissage via le navigateur : • Les modèles d'emails contiennent chacun un lien unique, spécifique au modèle (bien qu'identique pour tous les utilisateurs du Client), qui conduit à une page d'apprentissage hébergée sur un serveur Web du Prestataire. • En cliquant sur le lien, les utilisateurs sont dirigés vers la page d'apprentissage et l'e-mail concerné (sans adresse personnalisée) est présenté avec une explication sur la façon dont il peut être reconnu comme étant un e-mail d'hameçonnage. Utilisation du Bouton d'alerte phishing: • Un module complémentaire pour divers programmes de messagerie (tels que Microsoft Outlook) peut être installé en option, avec lequel les utilisateurs peuvent signaler les courriels suspects. Si l'e-mail en	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

question provient de la simulation, le clic est comptabilisé dans le taux de signalement de l'évaluation, qui est à son tour enregistrée par le Prestataire. Ces données sont anonymes et aucune donnée personnelle n'est enregistrée. Si l'e-mail ne provient pas de la simulation, il est transféré à une adresse e-mail spécifiée par le Client. Dans ce cas, aucun feedback ou flux de données n'est transmis au Prestataire.	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. This is anonymized and no personal information is recorded. 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) Mise à disposition d'une plateforme d'apprentissage en ligne : • Les utilisateurs peuvent s'inscrire sur le portail d'apprentissage en ligne sur la plateforme du Prestataire avec leur adresse électronique professionnelle à l'adresse https://elearning.sosafe.de/registration et avoir accès à tous les modules d'apprentissage en ligne mis à leur disposition ou fournis par le Client. Un court quiz peut être réalisé dans chaque module. Le résultat est déterminé sur la base des réponses (en fonction du nombre de bonnes réponses). Ce quiz peut être répété indéfiniment. • Les modules d'apprentissage en ligne peuvent également être fournis au Client sous forme de fichiers SCORM afin de faciliter leur intégration dans un système de gestion de l'apprentissage existant.	(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) Fourniture d'une évaluation (tableau de bord des rapports) : • Les taux d'ouverture, de réponse, de saisie et de clic (globalement et pour chaque regroupement défini par des critères de catégorisation, voir point 2.1 (1)) peuvent être déterminés sur la base du nombre total d'e-mails envoyés. Ces informations sont fournies au Client via un portail d'évaluation - cependant, un suivi personnalisé n'est pas possible, car chaque unité organisationnelle doit comprendre au moins cinq (5) personnes. • Si la plateforme du Prestataire est utilisée pour l'apprentissage en ligne, les taux d'inscription, la progression des modules et les résultats des quiz d'apprentissage en ligne sont enregistrés pour les utilisateurs individuels et (sauf accord contraire) communiqués au Client. • Lors de l'utilisation du Bouton d'alerte phishing le taux d'identification total et par catégorie (c'est-à-dire le nombre d'e-mails provenant de la simulation qui ont été identifiés par les utilisateurs comme des tentatives d'hameçonnage) est également déterminé et communiqué au Client.	(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 2.1 (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.

2.2 Durée La durée du traitement par le Prestataire dépend de la durée du Contrat principal. Le traitement et le présent Contrat sur le traitement des données spécifique à la commande prennent donc fin lorsque le Contrat principal prend fin, à condition qu'il n'y ait pas de poursuite des obligations découlant des termes du présent Contrat sur le traitement des données spécifique à la commande ou que le présent Contrat ne prenne pas fin prématurément. A titre exceptionnel, les obligations du présent Contrat subsistent au-delà de la durée du traitement spécifique à la commande et uniquement pour la période au cours de laquelle l'évènement suivant se produit : un "ancien" Contrat principal est remplacé ou modifié par un "nouveau" Contrat principal avec le même client, avec des exigences similaires en matière de traitement des données, associé au présent Contrat de traitement spécifique à la commande, et le traitement des informations personnelles est ainsi poursuivi de manière transitoire en l'absence d'un contrat principal jusqu'à l'entrée en vigueur du « nouveau » Contrat principal. Le traitement par le Prestataire dans le cadre de la commande ne sera pas interrompu, à moins que les Parties n'en décident autrement dans le contrat principal "de remplacement" ou "modifié". La durée du traitement sera alors prévue dans le contrat principal "de remplacement" ou "modifié".	2.2 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. Exceptionally, the obligations from this Contract survive beyond the order-specific processing duration and solely for the respective period in which the following event occurs that an "old" Main Contract is superseded or amended by a "new" Main Contract with the same Client, 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, until the “new” Main Contract enters into force. 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. Type et finalités de l'extraction, du traitement et de l'utilisation des données	**3. Type and purpose of retrieval, processing, and use**
3.1 Finalité du traitement	3.1 Purpose of processing

Le traitement a pour but de permettre au Client de fournir aux utilisateurs les services de sensibilisation achetés auprès du Prestataire.	The processing serves the following purpose: The Client is to be enabled to render the awareness building services purchased from the Contractor for the users.
3.2 Type de données Les données personnelles suivantes sont obtenues et traitées (selon le service spécifié dans le Contrat principal) : (1) Envoi des e-mails d'hameçonnage • Nom et prénom des utilisateurs • Niveau académique (facultatif) • Adresses e-mail professionnelles des utilisateurs • Sexe des utilisateurs (facultatif) • Groupes d'utilisateurs assignés (par exemple, unité organisationnelle, emplacement, rôle) par le Client. • Autres critères de catégorisation si nécessaire (voir section 2.1) • Langue des utilisateurs • Navigateur/version du navigateur et plateforme des utilisateurs • Participation à la sensibilisation (= pas d'opt-out selon la section 3.3) Ces données sont stockées dans une base de données sécurisée (voir Annexe 1) à des fins d'envoi personnalisé. Après l'achèvement des services du Contrat principal, ces données sont irrévocablement supprimées (conformément à l'article 6 et à l'annexe 1). (2) Feedback pour les utilisateurs de pages d'apprentissage sur Internet • La visite de pages d'apprentissage (sans autres données telles que les adresses IP ou les données de géolocalisation - celles-ci ne sont pas récupérées ou sont supprimées des données du journal du serveur par un mécanisme régulier). • Nombre de conseils d'utilisation et message d'aide consultés • Évaluation facultative des réactions ou réactions sur texte libre	3.2 Type of data The following personal information is obtained and processed (according to the service specified in the Main Contract): (1) Sending the phishing e-mails • First and last names of users • Academic level (optional) • Work e-mail 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 2.1) • Language of users • Browser/browser version and platform of users • Participation in awareness building (= no opt-out as per section 3.3) These data are stored in a secured database (see Annex 1) for purposes of personalized sending. After completion of the services of the Main Contract, these data are irrevocably deleted (as per section 6 and Annex 1). (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) Plateforme d'e-learning Lors de l'inscription sur la plateforme d'e-learning et pour l'utilisation continue de celle-ci : • Nom et prénom de l'utilisateur • Adresse électronique professionnelle de l'utilisateur • Langue de l'utilisateur • Sexe de l'utilisateur • Statut d'achèvement des modules e-learning individuels par utilisateur • Résultats des quiz du module par utilisateur Aux fins du retour d'information au Client : • Noms des utilisateurs enregistrés • Etat d'achèvement de tous les modules (agrégé) • Résultat moyen des quiz ou pourcentage de précision des réponses aux quiz (agrégé) • État d'achèvement de tous les modules par utilisateur • Valeur des quiz ou pourcentage de précision des réponses des quiz par utilisateur (facultatif)	(3) E-learning platform When registering on the e-learning platform and for continued use thereof: • First and last name of the user • Work e-mail 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 Si le client a réservé la fonction Escalation Manager, les informations personnelles suivantes sont obtenues et traitées. À des fins d'escalade, elles sont également envoyées au client : - le nom et le prénom, l'adresse électronique professionnelle et les groupes d'utilisateurs assignés aux utilisateurs du client - Statut d'achèvement individuel de tous les modules - Date limite de la campagne - Information indiquant si l'utilisateur a créé un compte ou non (oui/non) - Information si l'utilisateur est nouveau dans la formation (l'utilisateur s'est enregistré dans les 90 derniers jours : oui/non)	(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) Journaux du serveur	(5) Server logs

Les informations techniques suivantes sont conservées dans les journaux du serveur pendant douze (12) semaines à un maximum de six (6) mois: • Adresses IP • Agent de l'utilisateur • URL visité • Heures (6) Journaux de messagerie Les informations techniques suivantes sont conservées dans les journaux du serveur pendant douze (12) semaines : • Adresse électronique • Expéditeur • Serveur de courrier électronique de réception • Heures	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: • E-mail address • Sender • Receiving e-mail server • Time
3.3 Catégories de personnes concernées Les personnes concernées sont, sauf définition contraire dans le Contrat principal, tous les utilisateurs désignés par le Client pour participer. Le Client peut faciliter la non-participation des utilisateurs individuels par le biais d'un processus d'opt-out.	3.3 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.
4. Obligations du Prestataire	**4. Obligations of the Contractor**
(1) Le Prestataire traite les données personnelles uniquement comme convenu contractuellement ou selon les instructions du Client, à moins que le Prestataire ne soit légalement obligé de procéder à certains traitements en vertu de l'art. 28 para. 3 a) du RGPD. Si le Prestataire est lié à de telles obligations, il en informe le Client avant le traitement, à moins que le Prestataire n'ait légalement l'interdiction de divulguer une telle information. Le Prestataire doit immédiatement informer le Client s'il estime qu'une de ses instructions viole les lois applicables. Le Prestataire peut suspendre l'exécution de l'instruction jusqu'à ce qu'elle ait été confirmée ou modifiée par le Client. En outre, le Prestataire n'utilisera pas les données	(1) The Contractor processes personal information solely as contractually agreed or as instructed by the Client, unless the Contractor is legally obligated to conduct certain processing pursuant to Art. 28 para. 3 a) GDPR. If the Contractor is bound to such obligations, the Contractor shall notify the Client of these in advance of the processing, unless the Contractor is legally prohibited from such disclosure. The Contractor shall immediately notify the Client if the Contractor believes that an instruction violates the applicable laws. The Contractor may suspend the implementation of the instruction until it has been confirmed or altered by the Client. Furthermore, the Contractor shall not used the data provided for processing for any other

fournies pour le traitement à d'autres fins que celles convenues contractuellement.	purposes other than those contractually agreed.
(2) Le Prestataire est tenu de respecter strictement la confidentialité pendant le traitement.	(2) The Contractor is obligated to strictly adhere to confidentiality during the processing.
(3) Le Prestataire veille à ce que les employés et les autres personnes chargées du traitement des données ne traitent pas les données autrement que conformément aux instructions. En outre, le Prestataire s'assure que les personnes autorisées à traiter les données sont tenues à la confidentialité ou sont soumises à une obligation de confidentialité raisonnable et légale. L'obligation de confidentialité/secret reste en vigueur après l'exécution de la commande.	(3) The Contractor ensures that the employees and other persons in charge of processing the data are prohibited from processing the data in any manner other than as instructed. Furthermore, the Contractor ensures that the persons authorized to process the data are bound to confidentiality or are subject to a reasonable, legal confidentiality obligation. The confidentiality/secrecy obligation remains in effect after the order has been completed.
(4) Le Prestataire s'assure que l'organisation interne est configurée de manière appropriée aux exigences particulières de la protection des données et que les personnes désignées par le Prestataire pour le traitement ont été formées aux exigences de la protection des données et du présent Contrat avant de commencer le traitement. Les mesures de formation et de sensibilisation correspondantes doivent être régulièrement révisées de manière appropriée. Le Prestataire veille à ce que les personnes chargées du traitement des commandes soient suffisamment formées et supervisées en permanence en ce qui concerne le respect des exigences en matière de protection des données.	(4) The Contractor ensures that the internal organization is configured in a manner appropriate for the special requirements of data protection, and that persons appointed by the Contractor for processing have been instructed in the relevant requirements of data protection and this Contract before commencing processing. Corresponding training and sensitization measures must be regularly reviewed in a suitable manner. The Contractor ensures that the persons appointed to process orders are continuously and suitably instructed and supervised with regard to the fulfillment of the data protection requirements.
(5) En ce qui concerne le traitement commandé, le Prestataire doit assister le Client dans la création et la gestion continue du registre des activités de traitement, ainsi que dans l'évaluation des résultats du traitement des données dans la mesure du nécessaire, et doit en particulier conserver toutes les informations et tous les documents nécessaires et les transmettre au Client dans	(5) In relation to the commissioned processing, the Contractor must assist the Client in the creation and continued management of the record of processing activities as well as in assessing the results of the data processing to the necessary extent, and in particular must retain all necessary information and documentation and forward

les plus brefs délais et sur demande, dans les limites du raisonnable.	these to the Client as quickly as possible, and within reasonable bounds, upon request.
(6) Si le Client fait l'objet d'une surveillance de la part des autorités de contrôle ou d'autres entités, ou si les personnes concernées font valoir leurs droits auprès du Client, le Prestataire est tenu d'assister le Client dans la mesure du nécessaire pour autant que le traitement spécifique à la commande soit concerné.	(6) If the Client is subjected to monitoring by supervisory authorities or other entities, or if data subjects assert their rights to the Client, the Contractor is obligated to assist the Client to the necessary extent provided the order-specific processing is concerned.
(7) Le Prestataire ne peut communiquer des informations à des tiers ou à des personnes concernées qu'avec l'accord préalable du Client. Le Prestataire transmettra immédiatement au Client toute demande qui lui est adressée directement. Le Prestataire doit répondre directement et immédiatement à toute demande des autorités de contrôle. Toutefois, le Prestataire doit également en informer immédiatement le Client, dans la mesure où le traitement des informations personnelles du Client relatif à la commande en est affecté.	(7) The Contractor may only render disclosure to third parties or data subjects with prior consent from the Client. The Contractor will immediately forward to the Client any requests submitted directly to the Contractor. The Contractor must directly and immediately respond to any requests from supervisory authorities. However, the Contractor must also immediately notify the Client of this provided the order-specific processing of personal information of the Client is hereby affected.
(8) Les coordonnées du délégué à la protection des données désigné figurent toujours dans la politique de confidentialité sur le site web du Prestataire à l'adresse https://www.sosafe.de/datenschutz.	(8) The contact information of the appointed data protection officer is always stored in the privacy policy on the website of the Contractor at https://www.sosafe.de/datenschutz.
(9) Le traitement relatif à la commande a lieu uniquement au sein de l'Union européenne. Toute délocalisation vers un pays tiers n'est possible qu'avec le consentement du Client et conformément aux conditions du chapitre V du RGPD ainsi que du présent Contrat.	(9) The order-specific processing occurs solely within the EU. Any relocation to a third country is only possible with consent from the Client and in accordance with the conditions in Chapter V of the GDPR as well as with adherence to the terms of this Contract.
5. Mesures techniques et organisationnelles	**5. Technical and organizational measures**
(1) Les mesures de sécurité des données spécifiées à l'Annexe 1 sont contraignantes. Elles définissent le minimum accepté par le Prestataire. La description des mesures doit être suffisamment détaillée pour qu'une tierce	(1) The data security measures specified in Annex 1 are binding. They define the minimum accepted by the Contractor. The description of the measures must be so detailed that a knowledgeable third party

partie bien informée soit en mesure de déterminer avec certitude quel est le minimum accepté sur la base de la seule description. (2) Les mesures de sécurité des données peuvent être adaptées en fonction d'évolutions techniques et organisationnelles, en ce compris les mises à jour de logiciels par le fabricant, tant que le niveau de sécurité convenu dans le Contrat est respecté. Le Prestataire doit immédiatement mettre en œuvre les changements nécessaires pour assurer la sécurité des informations. Les changements doivent être immédiatement signalés au Client. (3) Si les mesures de sécurité concernées ne répondent pas ou plus aux besoins du Client, le Prestataire en informera immédiatement le Client. (4) Les copies ou les duplicatas ne sont pas créés à l'insu du Client. Cela exclut les copies temporaires, techniquement nécessaires, pour autant que cela ne porte pas atteinte au niveau de protection des données convenu dans le présent Contrat. (5) Le Prestataire vérifie régulièrement le respect de ses obligations, en particulier la mise en œuvre complète des mesures techniques et organisationnelles convenues ainsi que leur efficacité. La vérification doit être présentée au Client sur demande. Cette vérification peut être effectuée par le biais de codes de conduite convenus ou d'un processus de certification convenu.	should be able to determine with certainty what the accepted minimum should be based on the description alone. (2) The data security measures can be adjusted according to the further technical and organizational development, whereby software updates by the manufacturer are also included, as long as the level of security agreed herein is at least fulfilled. The Contractor must immediately implement any changes required to ensure information security. Changes must immediately be reported to the Client. (3) If the security measures concerned do not or no longer meet the needs of the Client, the Contractor shall immediately notify the Client of this. (4) Copies or duplicates are not created without the Client's knowledge. This excludes technically required, temporary duplications, provided this does not impair the level of data protection agreed herein. (5) The Contractor regularly renders verification of its obligations, in particular the full implementation of the agreed technical and organizational measures as well as the efficacy thereof. The verification must be presented to the Client on request. This verification can be rendered via agreed codes of conduct or an agreed certification process.
6. Règles relatives à la correction, la suppression et le blocage des données	**6. Regulation on the correction, deletion, and blocking of data**
(1) Le Prestataire ne corrigera, supprimera ou bloquera les données personnelles traitées à des fins spécifiques à la commande que conformément à l'accord contractuel ou aux instructions du Client, à condition que cela fasse partie des paramètres des instructions.	(1) The Contractor will only correct, delete, or block personal data processed for order-specific purposes in accordance with the contractual agreement or as instructed by the Client, provided such is included in the parameters of the instructions. The admin

L'interface d'administration permet au Client de modifier ou de supprimer les données des utilisateurs finaux. Le Prestataire n'est que subsidiairement tenu de fournir une assistance en ce qui concerne la correction, la suppression ou le blocage via l'interface d'administration.	interface makes it possible for the customer to modify or delete the end users' data. The Contractor is only secondarily obligated to provide assistance with regard to the correction, deletion, or blocking via the admin interface.
(2) Le Prestataire se conformera aux instructions émises par le Client même après la fin du présent Contrat.	(2) The Contractor will always abide by the instructions issued by the Client, even after this Contract has ended.
(3) À la fin de la relation contractuelle, ou à tout moment à la demande du Client, le Prestataire doit détruire les données faisant l'objet d'un traitement spécifique à la commande d'une manière conforme à la protection des données, ou les restituer au Client. Le Client choisit l'option à retenir. Toutes les copies des données doivent également être détruites. Cette destruction doit être effectuée de manière à ce qu'il ne soit pas possible de reproduire les informations, même résiduelles, au prix d'efforts raisonnables.	(3) Upon the end of this Contract relationship, or at any time at the Client's request, the Contractor must either destroy the data subjected to order-specific processing in a manner compliant with data protection, or return these to the Client. The Client selects which option is to be chosen. All copies of the data must also be destroyed. This destruction must be conducted such that it is not possible to reproduce even residual information with reasonable effort.
(4) Le Prestataire est également tenu de faire en sorte que les sous-traitants restituent ou suppriment immédiatement les données.	(4) The Contractor is obligated to induce immediate return or deletion by subcontractors as well.
(5) Le Prestataire doit vérifier que la destruction est bien effectuée. Quand toutes les données du Client sont supprimées (suppression du Client du logiciel de gestion SoSafe), un rapport de suppression est généré qui documente le moment et la portée de la suppression. Ce rapport de suppression doit être immédiatement présenté au Client sur demande.	(5) The Contractor must render verification of proper destruction. When all the Client's data are deleted (Client deletion from the SoSafe Management Software), a deletion report is generated that documents the time and scope of the deletion. This deletion report shall immediately be presented to the Client upon request.
(6) Le Prestataire n'a aucun droit de rétention sur les matériaux et les résultats des travaux.	(6) The Contractor has no right of retention to materials and work results.
(7) La documentation servant à vérifier le traitement correct des données doit également être conservée par le Prestataire	(7) Documentation that serves to verify proper data processing must also be retained by the Contractor in accordance with the respective retention periods, including beyond the end of the Contract period. The Contractor

dans le respect des délais de conservation applicables, y compris au-delà de la fin de la période contractuelle. Le Prestataire peut fournir cette documentation au Client à la fin de la période contractuelle.	may provide this documentation to the Client upon the end of the Contract period.
7. Sous-traitance	**7. Subcontracting**
(1) L'emploi de sous-traitants par le Prestataire n'est autorisé qu'avec le consentement du Client. Ce consentement est considéré comme accordé pour les sous-traitants spécifiés à l'Annexe 2. La désignation ou le changement d'un sous-traitant par le Prestataire doit être signalé au Client par un écrit, sous forme manuscrite ou numérique, avant la désignation. Le Client dispose alors de 14 jours calendaires, à compter de la remise des documents à examiner, pour s'opposer à cette nomination en cas de motif impérieux. Il y a notamment motif impérieux lorsqu'il existe des indications objectives selon lesquelles le sous-traitant n'est pas en mesure de satisfaire aux exigences de la protection des données et du Contrat. En cas d'opposition justifiée, le Prestataire peut décider de ne pas engager le sous-traitant. Si le Prestataire décide d'employer le sous-traitant malgré l'opposition justifiée du Client, ce dernier dispose de sept (7) jours calendaires après avoir pris connaissance de sa décision (d'employer le sous-traitant malgré son opposition) pour exercer un droit spécial de résiliation du présent Contrat sans préavis. Après l'écoulement de 14 jours sans opposition, le consentement est considéré comme accordé. (2) L'emploi de sous-traitants en tant que prestataires supplémentaires pour remplir les services du Prestataire n'est possible que si le sous-traitant est lié à des obligations de protection des données comparables à celles spécifiées dans le présent Contrat, et que le respect de la protection des données est au moins garanti. Sur demande, le Client reçoit un aperçu des éléments pertinents du Contrat entre le Prestataire et le sous-traitant.	(1) The employment of subcontractors by the Contractor is only permitted with consent from the Client. This consent is considered granted for the subcontractors specified in Annex 2. The appointment or change of another subcontractor by the Contractor must be reported to the Client in writing or text form before the appointment. The Client then receives 14 calendar days, beginning with the submission of the documents to be examined, to appeal against this appointment in the event of compelling cause. Compelling cause in particular is present when there are objective indications that the subcontractor is not capable of fulfilling the data protection and contractual requirements. In the event of a justified appeal, the Contractor may decide not to employ the subcontractor. If the Contractor decides to employ the subcontractor despite the justified appeal by the Client, the Client has seven (7) calendar days after becoming aware of the circumstances (employment of the subcontractor in spite of appeal) to exercise a special right of cancellation of this agreement without notice. After 14 days have passed without appeal, the consent is considered granted. (2) The employment of subcontractors as additional (sub-)contractors to fulfil the Contractor's services is only possible if the subcontractor has at least been bound to data protection obligations that are comparable to those specified in this Contract, and that the level of data protection is at least met. Upon request the Client receives insight into the relevant Contract components between the Contractor and subcontractor.

(3) Les droits du Client doivent pouvoir être effectivement exercés à l'égard du sous-traitant. Le Client doit notamment être autorisé à effectuer un contrôle des sous-traitants à tout moment, ou à permettre un tel contrôle par des tiers, dans le cadre prévu par les présentes.	(3) It must be possible for the rights of the Client to be effectively exercised relative to the subcontractor. In particular, the Client must be authorized at any time to conduct monitoring of subcontractors, or allow such monitoring by third parties, in the scope specified herein.
(4) Les responsabilités du Prestataire et du sous-traitant doivent être clairement différenciées les uns des autres.	(4) The Contractor's and subcontractor's responsibilities must be clearly demarcated from each other.
(5) Le Prestataire choisit soigneusement le sous-traitant en tenant compte de l'adéquation des mesures techniques et organisationnelles prises par le sous-traitant.	(5) The Contractor carefully selects the subcontractor with special consideration of the suitability of the technical and organizational measures taken by the subcontractor.
(6) L'emploi de sous-traitants qui n'effectuent pas le traitement des données spécifique à la commande exclusivement au sein de l'UE ou de l'EEE n'est possible que dans le respect des conditions énumérées à la section 4 (9) du présent Contrat. En particulier, il n'est autorisé que dans la mesure où le sous-traitant présente des garanties appropriées en matière de protection des données. Le Prestataire informe le Client des garanties spécifiques de protection des données offertes par le sous-traitant, et de la manière d'en obtenir la vérification.	(6) The employment of subcontractors who do not exclusively conduct order-specific data processing within the EU or the EEA is only possible in accordance with the conditions listed in section 4 (9) of this Contract. In particular, it is only permissible if and as long as the subcontractor makes appropriate data protection guarantees. The Contractor shall notify the Client of the specific data protection guarantees offered by the subcontractor, and how to obtain verification of this.
(7) Le Prestataire doit évaluer régulièrement et raisonnablement le respect des obligations du sous-traitant. L'évaluation et ses résultats doivent être soigneusement documentés de manière à être compréhensibles pour un tiers bien informé. La documentation doit être soumise au Client sur demande.	(7) The Contractor must regularly and reasonably assess adherence to the subcontractor's obligations. The assessment and results thereof must be thoroughly documented such that they are comprehensible to a knowledgeable third party. The documentation must be submitted to the Client on request.
(8) Si le sous-traitant ne respecte pas ses obligations en matière de protection des données, le Prestataire en est responsable vis-à-vis du Client.	(8) If the subcontractor fails to meet their data protection obligations, the Contractor is liable for this to the Client.
	(9) Upon finalization of this Contract, the subcontractors specified in Annex 2 with their

(9) Dès la finalisation du présent Contrat, les sous-traitants spécifiés à l'Annexe 2 avec leur nom, leur adresse et les services qu'ils proposent sont employés pour traiter les informations personnelles dans le cadre respectif qui y est mentionné, et sont acceptés par le Client. Les autres obligations du Prestataire envers les sous-traitants spécifiés dans le présent Contrat ne sont pas affectées. (10) Les services de sous-traitance conformément au présent Contrat ne comprennent que les services se rapportant directement à la prestation du service principal. Les services accessoires, tels que les services de télécommunication ou le service aux utilisateurs (sauf s'ils sont dus conformément au Contrat principal) ne sont pas inclus. L'obligation du Prestataire d'assurer le respect de la protection et de la sécurité des données dans ces cas n'est pas affectée.	name, address, and services are employed to process personal information in the respective scope mentioned therein, and are accepted by the Client. The other obligations of the Contractor to the subcontractors specified herein remain unaffected. (10) Subcontracting services in accordance with this Contract only include those services directly pertaining to the rendering of the main service. Auxiliary services, such as telecommunication services or user service (unless owed as per the Main Contract) are not included. The Contractor's obligation to ensure adherence to data protection and data security in these instances remains unaffected.
8. Droits et obligations du Client	**8. Rights and obligations of the Client**
(1) Le Client est seul responsable du respect des dispositions légales en matière de protection des données, notamment de la légalité de la communication des données au Prestataire et du traitement des données, et de la préservation des droits des personnes concernées, pour autant que cela concerne le responsable du traitement. (2) Le Client émet toutes les commandes, sous-commandes ou instructions, ainsi que leurs modifications, compléments ou remplacements, par écrit, sous forme manuscrite ou numérique. En cas d'urgence particulière, des instructions verbales peuvent être données. Les instructions verbales doivent être immédiatement confirmées par écrit par le Client. (3) Le Client doit immédiatement informer le Prestataire s'il découvre des erreurs ou des anomalies lors de l'évaluation des résultats du traitement ou en ce qui concerne les	(1) The Client is solely responsible for adhering to the legal provisions of the data protection laws, in particular the legality of data disclosure to the Contractor and of data processing and preserving data subject rights, provided these concern the responsible party. (2) The Client issues all orders, sub-orders, or instructions, as well as changes, supplements, or replacements thereof in written or an electronic format (text form). In cases of particular urgency, verbal instructions can be issued. Verbal instructions must immediately be confirmed in writing or text form by the Client. (3) The Client shall immediately notify the Contractor if it discovers errors or discrepancies during the assessment of the processing results or with regard to the data protection requirements.

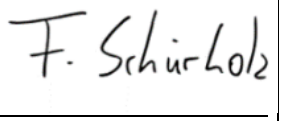
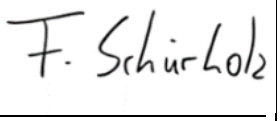
exigences en matière de protection des données. (4) Le Client est autorisé à contrôler raisonnablement (ou à faire contrôler raisonnablement) le respect des règles de protection des données et des exigences des accords contractuels conclus avec le Prestataire, notamment en obtenant des informations et en consultant les données stockées et les programmes de traitement des données, ainsi que par d'autres inspections sur place. Le Prestataire doit accorder l'accès et la consultation aux personnes chargées du contrôle, si nécessaire. Le Prestataire est tenu de fournir les informations nécessaires, de démontrer les processus et de procéder aux vérifications requises pour le contrôle. Si une tierce partie effectue l'inspection, cette tierce partie doit être soumise à la protection des données et au secret tels que décrits dans la section A article 8 des conditions générales de SoSafe. (5) Les inspections dans les locaux du Prestataire ne doivent pas entraîner d'entraves évitables à ses activités commerciales. À moins qu'il n'y ait des raisons urgentes que le Client doit étayer, les inspections ne doivent être effectuées qu'après un délai de préavis raisonnable et pendant les heures d'ouverture du Prestataire, et au maximum tous les douze (12) mois. Si le Prestataire effectue une vérification de la bonne exécution des obligations convenues en matière de protection des données, l'inspection doit se limiter à un échantillonnage aléatoire. Si l'inspecteur désigné par le Client est en concurrence avec le Prestataire, le Prestataire peut s'y opposer.	(4) The Client is authorized to reasonably monitor (or commission the reasonable monitoring of) adherence to the data protection regulations and requirements of the contractual agreements with the Contractor, in particular by obtaining information and viewing the stored data and data processing programs, as well as other on-site inspections. The Contractor must grant access and insight to the monitoring persons as necessary. The Contractor is obligated to issue the necessary information, demonstrate processes, and render verification required for monitoring. If a third party is conducting the inspection, this third party must be bound to data and secret protection as described in section A article 8 of the SoSafe Terms and Conditions. (5) Inspections on the Contractor's premises must not result in any avoidable impairments of its business operations. Unless otherwise induced by urgent reasons that the Client must document, inspections must only be conducted following a reasonable notice period and during the Contractor's hours of operation, and not more often than every twelve (12) months. If the Contractor renders verification of the proper implementation of the agreed data protection obligations, inspection shall be limited to random sampling. If the inspector appointed by the Client is in competition with the Contractor, the Contractor has the right to appeal this.
9. Obligations de notification	**9. Notification obligations**
(1) Le Prestataire doit informer immédiatement le Client de toutes atteintes à la sécurité des informations personnelles. Les cas de suspicion justifiés doivent également	(1) The Contractor shall immediately notify the Client of violations of the security of personal information. Justified instances of suspicion must also be reported. This reporting

être signalés. Cette notification doit être faite au plus tard 24 heures après que le Prestataire a pris connaissance de l'incident en question, et adressée à une partie spécifiée par le Client. Il doit contenir au moins les informations suivantes : a. une description du type de violation de la sécurité des informations personnelles, si possible avec spécification des catégories et du nombre approximatif de données personnelles concernées ; b. le nom et les coordonnées du délégué à la protection des données ou d'une autre personne à contacter pour obtenir des informations supplémentaires ; c. une description des conséquences probables de la violation de la sécurité des informations personnelles ; d. une description des mesures prises ou suggérées par le Prestataire pour remédier à la violation de la sécurité des informations personnelles et, le cas échéant, des mesures visant à atténuer les conséquences potentiellement négatives de cette violation. (2) Les perturbations significatives de la prestation de services, ainsi que les violations par le Prestataire ou ses employés des règles de protection des données ou des décisions prises dans le cadre du présent Contrat, doivent également être immédiatement signalées. (3) Le Prestataire informe immédiatement le Client des contrôles ou des mesures prises par les autorités de surveillance ou d'autres tiers, pour autant qu'ils concernent le traitement de données spécifiques à la commande. (4) Le Prestataire assure qu'il soutiendra le Client, dans la mesure du nécessaire, dans le respect de ses obligations en vertu des articles 32-36 du RGPD.	must be rendered no later than 24 hours after the Contractor has become aware of the relevant incident, and directed to a party specified by the Client. It must contain at least the following information: a. a description of the type of violation of the security of personal information, if possible with specification of the categories and approximate number of affected personal data sets; b. the name and contact information of the data protection officer or other contact for further information; c. a description of the likely consequences of the violation of the security of personal information; d. a description of the measures taken or suggested by the Contractor to remedy the violation of the security of personal information and, if applicable, measures for alleviating any potentially negative consequences thereof. (2) Significant disruptions to the rendering of services, and violations by the Contractor or its employees against data protection regulations or the determinations made in this Contract, must also immediately be reported. (3) The Contractor shall immediately notify the Client of inspections or measures by supervisory authorities or other third parties, provided these pertain to the order-specific processing. (4) The Contractor ensures that it shall support the Client to the necessary extent with its obligations pursuant to Art. 32-36 GDPR.
10. Instructions	**10. Instructions**

(1) Le Client dispose du droit de donner des instructions aux fins du traitement spécifique aux commandes. (2) Le Client et le Prestataire désignent les seules personnes autorisées à donner et à recevoir des instructions dans l'Annexe 3. (3) En cas de changement ou d'incapacité durable de ces personnes désignées, l'autre partie doit être immédiatement informée des successeurs ou représentants. (4) Le Prestataire est tenu d'informer le Client s'il estime qu'une instruction émise par le Client viole les dispositions légales. Le Prestataire est en droit de suspendre l'exécution de l'instruction en question jusqu'à ce qu'elle ait été confirmée ou modifiée par le responsable représentant le Client. (5) Le Prestataire doit documenter les instructions qui lui ont été données et la façon dont elles ont été réalisées.	(1) The Client reserves a comprehensive right of instruction for purposes of order-based processing. (2) The Client and Contractor appoint the sole persons authorized to issue and receive instructions in Annex 3. (3) In the event of a change in or long-term inability of these appointed persons, the other party must immediately be notified of successors or representatives. (4) The Contractor must notify the Client if it believes that an instruction issued by the Client violates legal regulations. The Contractor is authorized to suspend the rendering of the respective instruction until it has been confirmed or altered by the responsible party representing the Client. (5) The Contractor must document instructions issued to it and the rendering thereof.
11. Demandes des personnes concernées	**11. Data subject requests**
Lorsqu'une personne concernée contacte le Prestataire pour une réclamation concernant ses droits en vertu de l'art. 12 du RPGD, le Prestataire orientera la personne concernée vers le Client lorsque la transmission de sa réclamation au Client est possible en fonction des déclarations de la personne concernée. Le Prestataire transmet immédiatement la demande de la personne concernée au Client. Le Prestataire assiste le Client conformément aux instructions et conformément au Contrat.	If a data subject contacts the Contractor with a claim concerning data subject rights as per Art. 12 GDPR, the Contractor will refer the data subject to the Client if assignment to the Client is possible according to the statements made by the data subject. The Contractor immediately forwards the data subject's request to the Client. The Contractor assists the Client as instructed and as agreed.
12. Compensation	**12. Compensation**
La rémunération du Prestataire est régie exclusivement par le Contrat principal. Il n'y a pas de rémunération distincte ou de	The Contractor's compensation is definitively regulated in the Main Contract. There is no separate compensation or reimbursement of costs for purposes of this Contract.

remboursement des coûts aux fins du présent Contrat.	
13. Responsabilité civile	**13. Liability**
Les dispositions du RGPD, en particulier l'article 82 du RGPD, et la deuxième phrase du paragraphe 4 de l'article 28 du RGPD en cas de recours à un sous-traitant, sont applicables.	The terms of the GDPR, in particular Art. 82 GDPR, and Art. 28 para. 4 sentence 2 GDPR in the event of use of a subcontractor, apply.
14. Droit spécial de résiliation	**14. Special right of cancelation**
(1) Le Client peut résilier le présent Contrat à tout moment sans délai de préavis ("résiliation sans préavis") en cas de violation grave de la règlementation relative à la protection des données par le Prestataire, ou si le Prestataire refuse les droits de contrôle du Client en violation du Contrat. (2) En particulier, il y a violation grave si le Prestataire ne remplit pas ou pas suffisamment les obligations définies dans le présent Contrat, notamment les mesures techniques et organisationnelles convenues. (3) En cas de violations graves, le Client accorde au Prestataire un délai suffisant pour y remédier. S'il n'y est pas remédié dans le temps imparti, le Client est autorisé à résilier le présent Contrat sans préavis, comme décrit dans la présente section.	(1) The Client can cancel this Contract at any time without adherence to a term ("cancelation without notice") in the event of a grave violation against data protection regulations by the Contractor, or if the Contractor denies the Client's monitoring rights in violation of the Contract. (2) In particular, a grave violation has occurred if the Contractor does not fulfil or has not sufficiently fulfilled the obligations defined in this Contract, in particular the agreed technical and organizational measures. (3) In the event of grave violations, the Client grants the Contractor a sufficient remedy period. If remedy is not rendered in a timely fashion, the Client is authorized to cancel this Contract without notice as described in this section.
15. Divers	**15. Miscellaneous**
(1) Chaque Parties doit considérer comme confidentielles tous les secrets commerciaux et les mesures de protection des données de l'autre Partie obtenues dans le cadre de la relation contractuelle, y compris après la fin de la période contractuelle. En cas de doute sur le fait qu'une information est soumise à l'obligation de confidentialité, elle doit être traitée comme confidentielle jusqu'à ce que l'autre Partie ait donné son accord par écrit.	(1) Both parties are obligated to treat with confidentiality all knowledge of trade secrets and data protection measures of the respective other party obtained due to the contract relationship, including beyond the end of the Contract period. If there is any doubt as to whether a piece of information is subject to the confidentiality obligation, it must be treated as confidential until written approval by the other party has been rendered.

(2) Si les biens du Client détenus par le Prestataire sont mis en danger en raison de mesures prises par des tiers (par exemple, par le biais d'un nantissement ou d'une confiscation), d'une procédure d'insolvabilité ou de conciliation, ou d'autres événements, le Prestataire doit immédiatement en informer le Client. Le Prestataire informera immédiatement tous les responsables de traitement concernées que la souveraineté et la propriété des données reviennent uniquement au Client en tant que "responsable de traitement" conformément au RGPD.	(2) Should the any of the Client's property in the Contractor's possession be endangered due to third-party measures (e.g., via pledge or confiscation), insolvency or conciliation proceedings, or other events, the Contractor must immediately notify the Client. The Contractor will immediately notify all concerned responsible parties that the sovereignty and ownership of the data lie solely with the Client as the "responsible party" in accordance with the GDPR.
(3) Les modifications du présent Contrat, les conventions annexes et les déclarations faites dans le cadre du présent Contrat requièrent la forme écrite conformément à l'article 126 du Code civil allemand (BGB), les e-mails remplissant également cette exigence de forme écrite.	(3) Written form pursuant to § 126 BGB is required for changes to this Contract, collateral agreements, and declarations made in this Contract, to which end e-mails also fulfill this written form requirement.
(4) Le recours au droit de conservation conformément à l'article 273 du Code civil allemand (BGB) est exclu en ce qui concerne les données faisant l'objet d'un traitement relatif à la commande et les supports de données correspondants.	(4) Appeal of the right of retention pursuant to § 273 BGB is ruled out with regard to the data subjected to order-specific processing and respective data storage media.
(5) Si certains éléments du présent Contrat sont invalides, la validité du reste du Contrat n'est pas affectée.	(5) Should individual components of this agreement be invalid, the validity of the reminder of the agreement is not affected.
(6) Les lois de la République fédérale d'Allemagne sont applicables.	(6) The laws of the Federal Republic of Germany apply.
(7) Le présent Contrat est établi en français et en anglais. En cas de contradiction(s) entre ces deux versions du présent Contrat, la version anglaise prévaudra.	(7) This Contract is hereby drawn up in a French version and in an English version. In case of contradiction(s) between these two versions of this Contract, the English version shall prevail.
Signatures Lieu, date : Cologne, le ## ##### #####	**Signatures** Place, date: Cologne, on ## #### #####

			
Client	**Prestataire**	**Client**	**Contractor**

Annexe 1 - Mesures techniques et organisationnelles	**Annex 1 – Technical and organizational measures**
Les mesures techniques et organisationnelles visant à assurer la protection et la sécurité des données que le Prestataire doit au minimum mettre en place et respecter en permanence, sont définies ci-après. L'objectif est notamment de garantir la confidentialité, l'intégrité et la disponibilité des informations faisant l'objet d'un traitement relatif à la commande.	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. Anonymisation	**1. Anonymization**
Les informations personnelles ne sont pas récupérées aux fins de l'exécution et du traitement de la simulation d'hameçonnage. Les données comportementales (par exemple, les clics sur les liens dans les e-mails de phishing simulés) ne sont pas associées à des informations personnelles, mais se voient attribuer des codes générés de manière aléatoire et sont stockées en même temps que ces codes. Cette anonymisation est effectuée automatiquement par le système (approche privacy-by-design).	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 e-mails) are not 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. Cryptage	**2. Encryption**
2.1 Données en cours de transfert Tous les transferts de données (aussi bien entre le Client et le Prestataire qu'entre tous les employés du Prestataire) sont cryptés conformément aux recommandations de BSI en matière de cryptage. Avec l'intégration d'AWS, nous appliquons la politique ELBSecurityPolicy-2016-08 recommandée à partir des politiques de sécurité SSL	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

prédéfinies d'AWS, qui comprend TLS 1.2 avec SHA 256, échange de clés ECDHE et ECDSA pour l'authentification avec AES 128 pour le cryptage comme exigence minimale. L'accès au réseau nécessite une connexion VPN. La communication avec les points de terminaison du service nécessite une connexion sécurisée.	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 Données inactives Toutes les données personnelles identifiables du Client et de l'utilisateur (par exemple, les adresses e-mail des utilisateurs) sont cryptées lorsqu'elles sont stockées dans des bases de données protégées (système d'autorisation, politique de mot de passe avec les attributs susmentionnés, certificat SSH, accès uniquement possible via la zone IP interne). Le chiffrement par bloc est utilisé pour les données au repos à l'aide de la politique AWS SYMMETRIC_DEFAULT_Policy. Il s'agit de l'algorithme symétrique AES-256-GCM, qui est une norme industrielle de cryptage sécurisé. Les données cryptées sous AES-256-GCM sont protégées aujourd'hui et à l'avenir, car elles sont considérées comme résistantes aux attaques quantiques.	2.2 Data at rest All personally identifiable Client and user data (e.g., user e-mail 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 Données en cours d'utilisation La solution du Prestataire concerne une simple application Cloud avec laquelle la partie frontale de l'ordinateur de l'utilisateur final est exploité. Cela n'offre aucune possibilité de cryptage	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. Confidentialité	**3. Confidentiality**
3.1 Contrôle d'accès Les bureaux du Prestataire ne sont accessibles qu'avec les clés ou les transpondeurs correspondants et les serrures de sécurité correspondantes. La délivrance des clés et des transpondeurs est documentée et contresignée par la direction du Prestataire. En outre, ces espaces disposent d'une réception ou d'employés présents en permanence qui	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

assurent un contrôle d'accès supplémentaire. Une surveillance vidéo de tous les points d'accès est également présente.	control. Video monitoring of all access points is also present.
3.2 Contrôle d'accès numérique Il existe des exigences spécifiques pour l'attribution de mots de passe (générés de manière aléatoire, d'au moins douze (12) caractères (généralement plus long lorsque nous utilisons des gestionnaires de mots de passe). Ces mots de passe sont composés de majuscules et minuscules, chiffres et caractères spéciaux. pour tous les systèmes dans lesquels des informations personnelles sont traitées. Ces exigences sont directement mises en œuvre dans les systèmes par des mesures techniques , si cela est possible. Il est veillé à ce que toutes les personnes autorisées soient informées que les mots de passe doivent être stockés en toute sécurité et ne doivent pas être divulgués à d'autres parties. Les personnes désignées ont pour instruction de n'utiliser que des mots de passe uniques, c'est-à-dire des mots de passe que l'utilisateur n'utilise pas dans d'autres systèmes (notamment personnels). Tous les Clients sont déconnectés après un maximum de cinq (5) minutes d'inactivité. Tous les Clients possèdent un logiciel antivirus et pare-feu individuel avec une fonction de mise à jour automatique. Une authentification à deux facteurs est utilisée pour garantir l'accès autorisé aux systèmes de serveurs qui traitent les informations personnelles. Un pare-feu matériel et logiciel est également utilisé pour sécuriser le réseau de l'entreprise du Prestataire, et ce dernier possède un concept de réseau et de zone de réseau. Un logiciel de gestion des appareils mobiles est utilisé, et la technologie VPN est employée pour l'accès externe au réseau de l'entreprise du Prestataire.	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 Contrôle d'accès interne	3.3 Internal access control

L'accès aux systèmes de base de données et au système de gestion des applications est accordé uniquement si nécessaire, c'est-à-dire que l'administrateur informatique n'accorde les droits d'utilisateur nécessaires qu'aux employés chargés de l'administration des campagnes. Chaque accès interne aux systèmes de base de données est documenté et régulièrement contrôlé par l'administrateur informatique. Cette documentation est enregistrée dans un format non modifiable. Elle comprend la documentation des autorisations accordées. Les autorisations pour les systèmes de production, de test, de développement et d'administration sont accordées séparément.	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 Contrôle de la transmission Le transfert de données contenant des informations personnelles est réduit au minimum et limité à ce qui est nécessaire pour la fourniture du service. Du côté du Prestataire, seuls les chefs de projet et les administrateurs informatiques responsables ont accès aux informations personnelles. Un règlement sur le travail à distance est en place. Les informations personnelles sont traitées dans la partie frontale du logiciel de gestion SoSafe. Tous les transferts de données (tant entre le Client et le Prestataire qu'entre les employés du Prestataire) vers le logiciel de gestion SoSafe sont cryptés par https via AES 256bit selon nos définitions du cryptage des données en transit. L'accès aux bases de données est documenté et régulièrement inspecté par l'administrateur informatique. L'accès direct aux bases de données n'est possible que dans le réseau local de l'entreprise du Prestataire, ou via VPN en cas de travail à distance. Tous les réseaux WiFi sont cryptés avec WPA2. Aucun support de stockage de données physique et externe n'est utilisé pour les opérations commerciales.	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.

Les employés du Prestataire sont tenus de respecter l'interdiction de divulguer les secrets commerciaux et d'affaires conformément à la loi sur les secrets commerciaux (Geschäftsgeheimnisgesetz) ainsi que la limitation de l'objectif et l'obligation de confidentialité conformément à l'article 78, paragraphe 1, du SGB X. Un règlement sur le "bring-your-own-device" (BYOD) a été instauré. Cependant, les informations personnelles du Client que ce Contrat concerne ne sont pas stockées sur les appareils privés des employés du Prestataire. Les appareils privés (smartphones) servent uniquement à la communication interne et externe via le courrier électronique et l'outil de collaboration (Microsoft Teams). Le traitement des informations personnelles concernées ici s'effectue uniquement via les appareils de l'entreprise (ordinateurs portables et serveurs) auxquels s'appliquent les mesures techniques et organisationnelles de protection des données décrites dans le présent document.	The Contractor's employees are bound to the prohibition on the betrayal of trade and business secrets as per the Trade Secret Act (Geschäftsgeheimnisgesetz) as well as the purpose limitation and confidentiality obligation as per § 78 para. 1 SGB X. 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 e-mail 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 Suppression des données Il existe un processus standard de suppression des informations personnelles, dont le respect est évalué à la fois par l'administrateur informatique et par le responsable des comptes clés. La classe de protection P4 selon la norme DIN 66399 s'applique à la destruction des données physiques.	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 Contrôle de la séparation Les systèmes de production, de test/développement et d'administration sont séparés. Les droits sur les bases de données ont été définis et il existe une séparation des Clients dans le logiciel. En outre, tous les comptes sont séparés en fonction de leur charge de travail. Le Stockage, l'Informatique et le Réseau sont gérés indépendamment pour chaque compte.	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. Intégrité	**4. Integrity**
L'accès aux bases de données des systèmes de production est enregistré et conservé pendant douze (12) mois.	Access to the databases of the productive systems is logged and saved for twelve (12) months.
5. Disponibilité	**5. Availability**
5.1 Assurer la disponibilité Un plan de reprise après sinistre est disponible. Nous avons mis en place un plan de gestion de la continuité des activités. Celui-ci est décrit dans une politique de gestion de la continuité des services qui est basée sur la norme ISO 22301:2019 Gestion de la continuité des services pour maintenir la continuité des activités à un statut opérationnel basé sur le Minimum Business Continuity Output (MBCO). En outre, nous utilisons plusieurs zones de disponibilité au sein de notre architecture cloud, ce qui garantie la disponibilité même en cas de panne d'un centre de donnée complet. Les données sont sauvegardées quotidiennement. Toutes les applications sont conteneurisées et peuvent être reconstruites et déployées à la demande.	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 Limitation de l'objet Il existe des contrats de traitement des données relatives à la commande avec tous les prestataires de services. Tous les employés du Prestataire reçoivent une formation continue et complète (séminaires, apprentissage en ligne et formats interactifs tels que des quiz) sur les exigences en matière de protection des données ainsi que sur les thèmes fondamentaux de la sécurité des informations.	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. Durabilité des systèmes	**6. Durability of systems**
Les systèmes de production et les serveurs sont surveillés en permanence par le	The productive systems and servers are continuously monitored by the service provider

prestataire de services (voir annexe 2) afin d'assurer une disponibilité constante.	(see Annex 2) in order to ensure constant availability.
7. Récupération après incident	**7. Reproduction following incident**
Les serveurs et les systèmes de production sont assurés en permanence chaque jour par des sauvegardes complètes. Les sauvegardes sont cryptées et stockées sur des systèmes de serveurs distincts du prestataire de services. L'accès est accordé aux administrateurs du Prestataire. Chaque sauvegarde est conservée pendant 30 jours.	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. Évaluation régulière des mesures techniques et organisationnelles	**8. Regular assessment of technical and organizational measures**
Un employé du Prestataire est désigné pour être responsable de la gestion des réponses aux incidents. Aux fins de l'amélioration continue de la sécurité des informations du Prestataire, les mesures techniques et organisationnelles visant à assurer la protection et la sécurité des données sont continuellement contrôlées, examinées et améliorées par la direction du Prestataire.	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.
Annexe 2 - Sous-traitants agréés	**Annex 2 – Approved subcontractors**
Amazon Web Services EMEA SARL (Amazon Web Services, Inc. en tant que partie contractante des clauses contractuelles types de l'UE) 38 avenue John F. Kennedy, L-1855, Luxembourg **Hébergement de tous les composants actuels et futurs nécessaires à la fourniture du service, y compris l'interface API, le système de base de données ainsi que le serveur de messagerie pour la simulation d'hameçonnage.** Nous avons pris les mesures suivantes pour protéger les données : • Stockage et traitement de toutes les données dans des centres de données	**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.).

certifiés en Allemagne (Francfort-sur-le-Main). • Cryptage de toutes les données des clients à l'aide d'une clé maîtresse générée par le Processeur, de sorte que ni AWS ni aucun autre tiers ne puisse accéder aux données des clients, que ce soit à l'intérieur ou à l'extérieur de l'UE / EEE. • Conclusion d'un accord de traitement des données ainsi que la conclusion des clauses contractuelles types de l'UE ((EU) 2021/915, 4.6.2021, module 2 et 3), y compris les nombreuses obligations d'AWS en matière de traitement et de transparence en cas de demandes potentielles des autorités. • Évaluation de l'impact du transfert (TIA) réalisée par un expert externe en protection des données. • Avis d'un expert en protection des données sur l'utilisation d'AWS par le Processeur, qui peut être fourni sur demande. **Hetzner Online GmbH** Industriestr. 25, 91710 Gunzenhausen **Utilisation des services de messagerie pour la simulation de phishing de SoSafe GmbH.** Si cela a été explicitement convenu avec le contrôleur individuellement : Mise à disposition de l'interface API. Certificat ISO27001 pour les centres de données : https://www.hetzner.de/pdf/FOX_Zertifikat.pdf **salesforce.com Germany GmbH** Courrier : Salesforce.com Sarl, Route de la Longeraie 9, Morges, 1110, Suisse, attn : Director, EMEA Sales Operations, Legal Department: Erika-Mann-Strasse 31-37, 80636, Munich, Allemagne. **Fourniture d'un logiciel d'assistance (Customer Service Cloud) pour le service**	• 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 e-mail to support@sosafe.de). This provider is only

clientèle (formulaire d'assistance ou e-mail à support@sosafe.de). Ce fournisseur n'est pertinent pour le contrôleur que si ce dernier utilise le support client de SoSafe. Plus d'informations : https://trust.salesforce.com/ Le certificat ISO27001 peut être consulté ici : https://compliance.salesforce.com/en/iso-27017. En outre, les mesures suivantes ont été prises : • Stockage et traitement de toutes les données dans des centres de données certifiés en Allemagne (Francfort-sur-le-Main). • Cryptage de toutes les données avec des produits de cryptage standard de l'industrie pendant les transferts ainsi qu'au repos. • Conclusion d'un accord de traitement des données intégrant les règles d'entreprise contraignantes approuvées (BCR) conclues par Salesforce pour les sociétés de son groupe et ses sous-traitants, ainsi que les 2021 clauses contractuelles types de l'UE avec de nombreuses obligations vis-à-vis de l'autorité de surveillance compétente, ainsi que d'autres engagements volontaires. • Évaluation de l'impact du transfert (TIA) réalisée par un expert externe en protection des données.	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	**Microsoft Ireland Operations Ltd** One Microsoft Place, South County Business Park Leopardstown Dublin 18, D18 P521
Fourniture d'une infrastructure de serveur de messagerie pour la communication avec les clients dans les cas d'assistance via le logiciel d'assistance (formulaire d'assistance ou courriel à support@sosafe.de). Ce fournisseur n'est pertinent pour le contrôleur	**Provision of an e-mail server infrastructure for customer communication in support cases via the support software** (support form or e-mail 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:

que si ce dernier utilise le support client de SoSafe. Les mesures suivantes ont été prises : • Toutes les données sont traitées et stockées exclusivement au sein de l'Union européenne dans le cadre du cloud Azure EU. • Tous les centres de données sont certifiés ISO27001 et ISO27018 : https://docs.microsoft.com/de-de/azure/security/fundamentals/infrastructure. • Chiffrement de toutes les données à l'aide de produits de chiffrement conformes aux normes du secteur pendant les transferts ainsi qu'au repos. • Mise en œuvre de la "Customer Lockbox", qui garantit que Microsoft ne peut pas accéder au contenu sans le consentement explicite du processeur. • Conclusion d'un accord de traitement des données ainsi que des clauses contractuelles types de l'UE ((EU) 2021/915, 4.6.2021, module 2 et 3). • Évaluation de l'impact du transfert (TIA) réalisée par un expert externe en protection des données.	• 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.

Annexe 3 - Personnes autorisées à donner des instructions		**Annex 3 – Persons authorized to issue instructions**	
Les personnes suivantes sont autorisées à émettre et à recevoir des instructions.		The following persons are authorized to issue and receive instructions.	
DU CÔTÉ DU CLIENT:	DU CÔTÉ DU PRESTATAIRE:	CLIENT SIDE:	CONTRACTOR SIDE:
Conseil d'administration ou de direction	Felix Schürholz, directeur général	Board of directors or management	Felix Schürholz, Managing Director
Autres personnes explicitement désignées par le Client (par exemple, les responsables de la protection des données).	Lukas Schaefer, Directeur général	Other persons explicitly named by the Client (e.g., data protection officers)	Lukas Schaefer, Managing Director

	Dr. Niklas Hellemann, Directeur général		Dr. Niklas Hellemann, Managing Director
	Felix Fichtl, directeur général		Felix Fichtl, Managing Director