Accord sur le traitement des données

Version 3.0, mise à jour au 13.12.2023

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

1. Clauses contractuelles types

Les Parties s'accordent sur le texte de la Décision d'Exécution (UE) 2021/915 de la Commission du 4 juin 2021 relative aux Clauses Contractuelles Types entre les responsables du traitement et les sous-traitants au titre de l'article 28, paragraphe 7, du règlement (UE) 2016/679 du Parlement européen et du Conseil et de l'article 29, paragraphe 7, du règlement (UE) 2018/1725 du Parlement européen et du Conseil.

SECTION I

Clause 1

Objet et champ d'application

(a) Les présentes Clauses Contractuelles Types (ci-après les «Clauses») ont pour objet de garantir la conformité avec l'article 28, paragraphes 3 et 4, du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).

(b) Les responsables du traitement et les sous-traitants énumérés à l'annexe I ont accepté ces Clauses afin de garantir le respect des dispositions de l'article 28, paragraphes 3 et 4, du règlement (UE) 2016/679 et/ou des dispositions de l'article 29, paragraphes 3 et 4, du règlement (UE) 2018/1725.

(c) Les présentes Clauses s'appliquent au traitement des données à caractère personnel tel que décrit à l'annexe II.

(d) Les annexes I à IV font partie intégrante des Clauses.

(e) Les présentes Clauses sont sans préjudice des obligations auxquelles le responsable du traitement est soumis en vertu du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725.

(f) Les Clauses ne suffisent pas à elles seules pour assurer le respect des obligations relatives aux transferts internationaux conformément au chapitre V du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725.

Clause 2

Invariabilité des Clauses

(a) Les Parties s'engagent à ne pas modifier les Clauses, sauf en ce qui concerne l'ajout d'informations aux annexes ou la mise à jour des informations qui y figurent.

(b) Les Parties ne sont pour autant pas empêchées d'inclure les clauses contractuelles types définies dans les présentes Clauses dans un contrat plus large, ni d'ajouter d'autres clauses ou des garanties supplémentaires, à condition que celles-ci ne contredisent pas, directement ou indirectement, les Clauses ou qu'elles ne portent pas atteinte aux libertés et droits fondamentaux des personnes concernées.

Clause 3

Interprétation

(a) Lorsque des termes définis respectivement dans le Règlement (UE) 2016/679 ou dans le Règlement (UE) 2018/1725 figurent dans les Clauses, ils s'entendent comme dans le Règlement en question.

(b) Les présentes Clauses doivent être lues et interprétées à la lumière des dispositions du Règlement (UE) 2016/679 et du Règlement (UE) 2018/1725 respectivement.

(c) Les présentes Clauses ne doivent pas être interprétées d'une manière contraire aux droits et obligations prévus par le Règlement (UE) 2016/679 / le Règlement (UE) 2018/1725 ou d'une manière qui porte atteinte aux libertés ou droits fondamentaux des personnes concernées.

Clause 4

Hiérarchie

En cas de contradiction entre les présentes Clauses et les dispositions des accords connexes qui existent entre les Parties au moment où les présentes Clauses sont convenues ou qui sont conclus ultérieurement, les présentes Clauses prévaudront.

Clause 5

Clause d'amarrage

(a) Toute entité qui n'est pas Partie aux présentes Clauses peut, avec l'accord de toutes les Parties, y adhérer à tout moment, en qualité soit de responsable du traitement soit de sous-traitant, en complétant les annexes et en signant l'Annexe I.

(b) Une fois que les Annexes mentionnées au point a) sont complétées et signées, l'entité adhérente est considérée comme une Partie aux présentes Clauses et jouit des droits et est soumise aux obligations d'un responsable du traitement ou d'un sous-traitant, conformément à sa désignation à l'Annexe I.

(c) Les présentes Clauses ne créent pour la Partie adhérente aucun droit ni aucune obligation pour la période précédant l'adhésion.

SECTION II

OBLIGATIONS DES PARTIES

Clause 6

Description du ou des traitements

Les détails des opérations de traitement, et notamment les catégories de données à caractère personnel et les finalités du traitement pour lesquelles les données à caractère personnel sont traitées pour le compte du responsable du traitement, sont précisés à l'Annexe II.

Clause7

Obligations des Parties

7.1. **Instructions**

(a) Le sous-traitant ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel il est soumis. Dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si la loi le lui interdit pour des motifs importants d'intérêt public. Des instructions peuvent également être données ultérieurement par le responsable du traitement pendant toute la durée du traitement des données à caractère personnel. Ces instructions doivent toujours être documentées.

(b) Le sous-traitant informe immédiatement le responsable du traitement si, selon lui, une instruction donnée par le responsable du traitement constitue une violation du règlement (UE) 2016/679 / du Règlement (UE) 2018/1725 ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données.

7.2. **Limitation de la finalité**

Le sous-traitant traite les données à caractère personnel uniquement pour la ou les finalités spécifiques du traitement, telles que définies à l'Annexe II, sauf instruction complémentaire du responsable du traitement.

7.3. **Durée du traitement des données à caractère personnel**

Le traitement par le sous-traitant n'a lieu que pendant la durée précisée à l'Annexe II.

7.4. **Sécurité du traitement**

(a) Le sous-traitant met au moins en œuvre les mesures techniques et organisationnelles précisées à l'Annexe III pour assurer la sécurité des données à caractère personnel. Figure parmi ces mesures la protection des données contre toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel ou l'accès non autorisé à de telles données (violation de données à caractère personnel). Lors de l'évaluation du niveau de sécurité approprié, les Parties tiennent dûment compte de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement, ainsi que des risques pour les personnes concernées.

(b) Le sous-traitant n'accorde aux membres de son personnel l'accès aux données à caractère personnel faisant l'objet du traitement que dans la mesure strictement nécessaire à l'exécution, à la gestion et au suivi du contrat. Le sous-traitant veille à ce que les personnes autorisées à traiter les données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité.

7.5. **Données sensibles**

Si le traitement porte sur des données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que des données génétiques ou des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique, ou des données relatives aux condamnations pénales et aux infractions («données sensibles»), le sous-traitant applique des limitations spécifiques et/ou des garanties supplémentaires.

7.6. **Documentation et conformité**

(a) Les Parties doivent pouvoir démontrer la conformité avec les présentes Clauses.

(b) Le sous-traitant traite de manière rapide et adéquate les demandes du responsable du traitement concernant le traitement des données conformément aux présentes Clauses.

(c) Le sous-traitant met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations énoncées dans les présentes Clauses et découlant directement du Règlement (UE) 2016/679 et/ou du Règlement (UE) 2018/1725. À la demande du responsable du traitement, le sous-traitant permet également la réalisation d'audits des activités de traitement couvertes par les présentes Clauses et y contribue, à intervalles raisonnables ou en présence d'indices de non-conformité. Lorsqu'il décide d'un examen ou d'un audit, le responsable du traitement peut tenir compte des certifications pertinentes en possession du sous-traitant.

(d) Le responsable du traitement peut décider de procéder lui-même à l'audit ou de mandater un auditeur indépendant. Les audits peuvent également comprendre des inspections dans les locaux ou les installations physiques du sous-traitant et sont, le cas échéant, effectués moyennant un préavis raisonnable.

(e) Les Parties mettent à la disposition de l'autorité de contrôle compétente/des autorités de contrôle compétentes, dès que celles-ci en font la demande, les informations énoncées dans la présente Clause, y compris les résultats de tout audit.

7.7. **Recours à des sous-traitants ultérieurs**

(a) AUTORISATION ÉCRITE GÉNÉRALE : Le sous-traitant dispose de l'autorisation générale du responsable du traitement pour ce qui est du recrutement de sous-traitants ultérieurs sur la base d'une liste convenue. Le sous-traitant informe spécifiquement par écrit le responsable du traitement de tout projet de modification de cette liste par l'ajout ou le remplacement de sous-traitants ultérieurs au moins 14 jours calendaires à l'avance, donnant ainsi au responsable du traitement suffisamment de temps pour pouvoir s'opposer à ces changements avant le recrutement du ou des sous-traitants ultérieurs concernés. Le sous-traitant fournit au responsable du traitement les informations nécessaires pour lui permettre d'exercer son droit d'opposition.

(b) Lorsque le sous-traitant recrute un sous-traitant ultérieur pour mener des activités de traitement spécifiques (pour le compte du responsable du traitement), il le fait au moyen d'un contrat qui impose au sous-traitant ultérieur, en substance, les mêmes obligations en matière de protection des données que celles imposées au sous-traitant en vertu des présentes Clauses. Le sous-traitant veille à ce que le sous-traitant ultérieur respecte les obligations auxquelles il est lui-même soumis en vertu des présentes Clauses et du Règlement (UE) 2016/679 et/ou du Règlement (UE) 2018/1725.

(c) À la demande du responsable du traitement, le sous-traitant lui fournit une copie de ce contrat conclu avec le sous-traitant ultérieur et de toute modification qui y est apportée ultérieurement. Dans la mesure

nécessaire à la protection des secrets d'affaires ou d'autres informations confidentielles, y compris les données à caractère personnel, le sous-traitant peut expurger le texte du contrat avant d'en diffuser une copie.

(d) Le sous-traitant demeure pleinement responsable, à l'égard du responsable du traitement, de l'exécution des obligations du sous-traitant ultérieur conformément au contrat conclu avec le sous-traitant ultérieur. Le sous-traitant informe le responsable du traitement de tout manquement du sous-traitant ultérieur à ses obligations contractuelles.

(e) Le sous-traitant convient avec le sous-traitant ultérieur d'une clause du tiers bénéficiaire selon laquelle — dans le cas où le sous-traitant a matériellement disparu, a cessé d'exister en droit ou est devenu insolvable — le responsable du traitement a le droit de résilier le contrat conclu avec le sous-traitant ultérieur et de donner instruction au sous-traitant ultérieur d'effacer ou de renvoyer les données à caractère personnel.

7.8. **Transferts internationaux**

(a) Tout transfert de données vers un pays tiers ou une organisation internationale par le sous-traitant n'est effectué que sur la base d'instructions documentées du responsable du traitement ou afin de satisfaire à une exigence spécifique du droit de l'Union ou du droit de l'État membre à laquelle le sous-traitant est soumis et s'effectue conformément au chapitre V du Règlement (UE) 2016/679 ou du Règlement (UE) 2018/1725.

(b) Le responsable du traitement convient que lorsque le sous-traitant recrute un sous-traitant ultérieur conformément à la Clause 7.7 pour mener des activités de traitement spécifiques (pour le compte du responsable du traitement) et que ces activités de traitement impliquent un transfert de données à caractère personnel au sens du Chapitre V du Règlement (UE) 2016/679, le sous-traitant et le sous-traitant ultérieur peuvent garantir le respect du Chapitre V du Règlement (UE) 2016/679 en utilisant les clauses contractuelles types adoptées par la Commission sur la base de l'Article 46, paragraphe 2, du Règlement (UE) 2016/679, pour autant que les conditions d'utilisation de ces clauses contractuelles types soient remplies.

Clause 8

Assistance au responsable du traitement

(a) Le sous-traitant informe sans délai le responsable du traitement de toute demande qu'il a reçue de la part de la personne concernée. Il ne donne pas lui-même suite à cette demande, à moins que le responsable du traitement des données ne l'y ait autorisé.

(b) Le sous-traitant prête assistance au responsable du traitement pour ce qui est de remplir l'obligation qui lui incombe de répondre aux demandes des personnes concernées d'exercer leurs droits, en tenant compte de la nature du traitement. Dans l'exécution de ses obligations conformément aux points a) et b), le sous-traitant se conforme aux instructions du responsable du traitement.

(c) Outre l'obligation incombant au sous-traitant d'assister le responsable du traitement en vertu de la clause 8, point b), le sous-traitant aide en outre le responsable du traitement à garantir le respect des obligations suivantes, compte tenu de la nature du traitement et des informations dont dispose le sous-traitant :

(1) l'obligation de procéder à une évaluation de l'incidence des opérations de traitement envisagées sur la protection des données à caractère personnel («analyse d'impact relative à la

protection des données») lorsqu'un type de traitement est susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques;

(2) l'obligation de consulter l'autorité de contrôle compétente/les autorités de contrôle compétentes préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque;

(3) l'obligation de veiller à ce que les données à caractère personnel soient exactes et à jour, en informant sans délai le responsable du traitement si le sous-traitant apprend que les données à caractère personnel qu'il traite sont inexactes ou sont devenues obsolètes;

(4) les obligations prévues à l'Article 32 du Règlement (UE) 2016/679.

(d) Les Parties définissent à l'Annexe III les mesures techniques et organisationnelles appropriées par lesquelles le sous-traitant est tenu de prêter assistance au responsable du traitement dans l'application de la présente Clause, ainsi que la portée et l'étendue de l'assistance requise.

Clause 9

Notification de violations de données à caractère personnel

En cas de violation de données à caractère personnel, le sous-traitant coopère avec le responsable du traitement et lui prête assistance aux fins de la mise en conformité avec les obligations qui lui incombent en vertu des Articles 33 et 34 du Règlement (UE) 2016/679 ou des Articles 34 et 35 du Règlement (UE) 2018/1725, selon celui qui est applicable, en tenant compte de la nature du traitement et des informations dont dispose le sous-traitant.

9.1 **Violation de données en rapport avec des données traitées par le responsable du traitement**

En cas de violation de données à caractère personnel en rapport avec des données traitées par le responsable du traitement, le sous-traitant prête assistance au responsable du traitement :

(a) aux fins de la notification de la violation de données à caractère personnel à l'autorité de contrôle compétente/aux autorités de contrôle compétentes, dans les meilleurs délais après que le responsable du traitement en a eu connaissance, le cas échéant (sauf si la violation de données à caractère personnel est peu susceptible d'engendrer un risque pour les droits et libertés des personnes physiques);

(b) aux fins de l'obtention des informations suivantes qui, conformément à [OPTION 1] l'article 33, paragraphe 3, du règlement (UE) 2016/679, doivent figurer dans la notification du responsable du traitement, et inclure, au moins :

(1) la nature des données à caractère personnel, y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données à caractère personnel concernés;

(2) les conséquences probables de la violation de données à caractère personnel;

(3) les mesures prises ou les mesures que le responsable du traitement propose de prendre pour remédier à la violation de données à caractère personnel, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Lorsque, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et, à mesure qu'elles deviennent disponibles, des informations supplémentaires sont communiquées par la suite dans les meilleurs délais;

(c) aux fins de la satisfaction, conformément à l'Article 34 du Règlement (UE) 2016/679 de l'obligation de communiquer dans les meilleurs délais la violation de données à caractère personnel à la personne concernée, lorsque la violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

9.2 **Violation de données en rapport avec des données traitées par le sous-traitant**

En cas de violation de données à caractère personnel en rapport avec des données traitées par le sous-traitant, celui-ci en informe le responsable du traitement dans les meilleurs délais après en avoir pris connaissance. Cette notification contient au moins :

(a) une description de la nature de la violation constatée (y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et d'enregistrements de données à caractère personnel concernés);

(b) les coordonnées d'un point de contact auprès duquel des informations supplémentaires peuvent être obtenues au sujet de la violation de données à caractère personnel;

(c) ses conséquences probables et les mesures prises ou les mesures qu'il est proposé de prendre pour remédier à la violation, y compris pour en atténuer les éventuelles conséquences négatives.

Lorsque, et dans la mesure où, il n'est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et, à mesure qu'elles deviennent disponibles, des informations supplémentaires sont communiquées par la suite dans les meilleurs délais.

Les Parties définissent à l'Annexe III tous les autres éléments que le sous-traitant doit communiquer lorsqu'il prête assistance au responsable du traitement aux fins de la satisfaction des obligations incombant à ce dernier en vertu des Articles 33 et 34 du Règlement (UE) 2016/679.

SECTION III

DISPOSITIONS FINALES

Clause 10

Non-respect des Clauses et résiliation

(a) Sans préjudice des dispositions du Règlement (UE) 2016/679 et/ou du Règlement (UE) 2018/1725, en cas de manquement du sous-traitant aux obligations qui lui incombent en vertu des présentes Clauses, le responsable du traitement peut donner instruction au sous-traitant de suspendre le traitement des données à caractère personnel jusqu'à ce que ce dernier se soit conformé aux présentes Clauses ou jusqu'à ce que le contrat soit résilié. Le sous-traitant informe rapidement le responsable du traitement s'il n'est pas en mesure de se conformer aux présentes Clauses, pour quelque raison que ce soit.

(b) Le responsable du traitement est en droit de résilier le contrat dans la mesure où il concerne le traitement de données à caractère personnel conformément aux présentes Clauses si :

(1) le traitement de données à caractère personnel par le sous-traitant a été suspendu par le responsable du traitement conformément au point a) et le respect des présentes Clauses n'est pas rétabli dans un délai raisonnable et, en tout état de cause, dans un délai d'un mois à compter de la suspension;

(2) le sous-traitant est en violation grave ou persistante des présentes Clauses ou des obligations qui lui incombent en vertu du Règlement (UE) 2016/679 et/ou du Règlement (UE) 2018/1725;

(3) le sous-traitant ne se conforme pas à une décision contraignante d'une juridiction compétente ou de l'autorité de contrôle compétente/des autorités de contrôle compétentes concernant les obligations qui lui incombent en vertu des présentes Clauses ou du Règlement (UE) 2016/679 et/ou du Règlement (UE) 2018/1725.

(c) Le sous-traitant est en droit de résilier le contrat dans la mesure où il concerne le traitement de données à caractère personnel en vertu des présentes Clauses lorsque, après avoir informé le responsable du traitement que ses instructions enfreignent les exigences juridiques applicables conformément à la Clause 7.1, point b), le responsable du traitement insiste pour que ses instructions soient suivies.

(d) À la suite de la résiliation du contrat, le sous-traitant supprime, selon le choix du responsable du traitement, toutes les données à caractère personnel traitées pour le compte du responsable du traitement et certifie auprès de celui-ci qu'il a procédé à cette suppression, ou renvoie toutes les données à caractère personnel au responsable du traitement et détruit les copies existantes, à moins que le droit de l'Union ou le droit national n'impose de les conserver plus longtemps. Le sous-traitant continue de veiller à la conformité aux présentes Clauses jusqu'à la suppression ou à la restitution des données.

Annexe I – Liste des Parties

Responsable du traitement

[Identité et coordonnées du ou des responsables du traitement et, le cas échéant, du délégué à la protection des données du responsable du traitement]

Nom : Indiquez ici le nom du responsable du traitement

Adresse : Indiquez ici l'adresse du responsable du traitement

Nom, fonction et coordonnées de la personne de contact : Signature et date d'adhésion :

Indiquez ici les nom, fonction et coordonnées de la personne de contact

Sous-traitant

SoSafe GmbH
Lichtstr. 25a
50825 Köln

Délégué à la protection des données :

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

Felix Schürholz, Managing Director Signature et date d'adhésion : ...

22 April 2024 | 08:37 PDT

DocuSigned by:
Felix Schürholz
6459695B96B249C...

Annexe II – Description du traitement

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 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 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. Les données enregistrées seront anonymisées et seules les données anonymisées seront envoyées au Client. 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.

(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.

(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 1.1 (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.

2. Durée

La durée du traitement par le Prestataire dépend de la durée du Contrat Principal. Le traitement et le présent Contrat relatif au traitement spécifique à la commande prennent donc fin lorsque le contrat principal prend fin, à condition qu'il n'y ait pas d'obligations continues découlant des conditions du présent Contrat relatif au traitement spécifique à la commande ou que le présent Contrat ne prenne pas fin prématurément. Les obligations découlant du présent Contrat au-delà du traitement spécifique de la commande s'appliquent pour la période correspondante dans le cas où un "ancien" Contrat Principal est remplacé ou modifié par un "nouveau" Contrat Principal, avec des exigences similaires en matière de protection des données, associé au présent Contrat sur le traitement spécifique de la commande, et le traitement des informations à caractère personnel se poursuit donc de manière transitoire en l'absence d'un Contrat Principal. Le traitement ininterrompu de la commande par le Prestataire est convenu, à moins que les Parties n'en décident autrement dans le Contrat Principal "remplaçant" ou "modifié". La durée du traitement est alors basée sur le Contrat Principal "remplaçant" ou "modifié".

3. Finalité du traitement

Le traitement a pour but de permettre au Client de fournir aux utilisateurs les services de sensibilisation achetés auprès du Prestataire.

4. 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
- Genre des utilisateurs (facultatif)
- Groupes d'utilisateurs assignés (par exemple, unité organisationnelle, emplacement, rôle) par le Client.
- Autres critères de catégorisation si nécessaire (voir section 1.1)
- Langue des utilisateurs
- Navigateur/version du navigateur et plateforme des utilisateurs
- Participation à la sensibilisation (= pas d'opt-out selon la section 5)

Ces données sont stockées dans une base de données sécurisée (voir Annexe III) à des fins d'envoi personnalisé. Après l'achèvement des services du Contrat Principal, ces données sont irrévocablement supprimées.

(2) Retour d'information 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) 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
- Genre 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)

(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)

(5) Journaux du serveur

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

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

5. 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

Annexe III – Mesures techniques et organisationnelles, y compris les mesures techniques et organisationnelles visant à garantir la sécurité des données

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.

1. Anonymisation

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).

2. Cryptage

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 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.

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.

2.3 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 exploitée. Cela n'offre aucune possibilité de cryptage.

3. Confidentialité

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 assurent un contrôle d'accès supplémentaire. Une surveillance vidéo de tous les points d'accès est également présente.

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), 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.

3.3 Contrôle d’accès interne

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.

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.

Les employés du Prestataire sont tenus de respecter l'interdiction de divulguer les secrets commerciaux et d'affaires conformément à la loi applicable.

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.

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.

3.6 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.

4. Intégrité

L'accès aux bases de données des systèmes de production est enregistré et conservé pendant douze (12) mois.

5. Disponibilité

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 garantit la disponibilité même en cas de panne d'un centre de données complet. Les données sont sauvegardées quotidiennement. Toutes les applications sont conteneurisées et peuvent être reconstruites et déployées à la demande.

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.

6. Durabilité des systèmes

Les systèmes de production et les serveurs sont surveillés en permanence par le prestataire de services afin d'assurer une disponibilité constante.

7. Récupération après 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.

8. Évaluation régulière des mesures techniques et organisationnelles

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.

Annexe IV – Liste des sous-traitants ultérieurs

- 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 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 Responsable du traitement 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 clientèle (formulaire d'assistance ou e-mail à support@sosafe.de). Ce fournisseur n'est pertinent pour le Responsable du traitement 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 clauses contractuelles types de l'UE de 2021 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.

- 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 Responsable du traitement 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 Sous-traitant.
- 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.

- Kombo Technologies GmbH (Optional)

Lohmühlenstraße 65, 12435 Berlin, Germany

Intégration de l'Active Directory du client. Ce fournisseur n'est requis que dans la mesure où le client demande l'intégration de l'Active Directory pour le téléchargement automatisé et la mise à jour régulière des données de l'utilisateur final sur la plateforme de l'entrepreneur. Les mesures suivantes ont été prises :

- Toutes les données sont traitées et stockées exclusivement dans l'Union européenne. Fournisseur d'hébergement du serveur : Google Cloud EMEA Limited.
- Kombo Technologies GmbH est certifié ISO27001. L'accès peut être demandé ici : https://security.kombo.dev/?itemUid=1fed9faa-4a87-427c-9a95-96b4d6bf66b7&source=click/ . De plus amples informations sur les mesures de sécurité techniques et organisationnelles de Kombo Technologies GmbH sont disponibles sur security.kombo.dev.
- Cryptage
  - Toutes les données des clients sont cryptées en utilisant le cryptage symétrique AES-256 au repos, y compris les copies de sauvegarde.
  - Données en transit : Tout le trafic sortant (vers les API d'intégration) utilise la version TLS la plus élevée disponible par l'API de l'intégration concernée (par exemple, Google Workspace). Tout le trafic entrant via l'API de Kombo est contraint d'utiliser TLS 1.3. Les connexions des charges de travail des applications de Kombo à la base de données de Kombo utilisent également TLS 1.3 avec un chiffrement AES-256.
- Conclusion d'un accord sur le traitement des données.

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