Accord de traitement de données à caractère personnel

Version 3.2, mise à jour au 02.01.2025

SoSafe SE I Lichtstr. 25a I 50825 Cologne I 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

La personne de contact désignée par le Client dans le SoSafe Manager après la signature du Contrat principal sera le destinataire principal des communications.

Jusqu'à ce que cette personne soit désignée, les communications seront adressées à l'Administrateur du Client tel que spécifié dans le SoSafe Manager, au plus tard au début de l'implémentation des Services de Sensibilisation.

Sous-traitant

SoSafe SE
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

Note: Veuillez envoyer une copie de toute communication à privacy@sosafe.de

Annexe II – Description du traitement

1. Objet

Les services du Sous-traitant qui constituent la base des activités de traitement de ce dernier en vertu du présent Accord de traitement de données à caractère personnel sont spécifiés en détail dans le Contrat Principal. Le traitement de données à caractère personnel selon les instructions du Responsable de traitement, dans le cadre du présent Accord concerne spécifiquement ce qui suit :

Mise à disposition d'une SaaS (Software-as-a-Service) de gestion des risques humains, de formation et de tests utilisateurs. Conformément à la sélection par le Responsable de traitement des Services de Sensibilisation de SoSafe, les Utilisateurs du Responsable de traitement ou de ses affiliés dans le cadre du Contrat principal auront accès à des simulations d'ingénierie sociale (par exemple, phishing, smishing, vishing), questionnaires, tests, chatbots et outils optionnels alimentés par l'IA et autres mécanismes de profilage des risques centrés sur l'Utilisateur. La formation à la sensibilisation à la sécurité, les analyses, les mécanismes de retour d'information et les interventions techniques et procédurales peuvent être déclenchés automatiquement ou manuellement, tels que configurés par le Responsable du traitement, ou autrement fournis à la suite de l'interaction de l'Utilisateur avec la Plateforme ou des données ingérées par la Plateforme via des intégrations techniques avec d'autres systèmes commerciaux du Responsable de traitement, tels que mis en œuvre ou autrement spécifiés par le Responsable de traitement. La Plateforme peut établir un profil personnalisé d'un Utilisateur et cibler des actions automatisées pour signaler ou améliorer les comportements sécurisés de l'Utilisateur, sous réserve des paramètres d'anonymisation sélectionnés par le Responsable du traitement.

2. Durée

La durée du traitement par le Sous-traitant 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 (y compris la phase de rétention application après le terme du Contrat conformément au concept de suppression des données) 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.

3. Finalité du traitement

Le traitement a pour but de permettre au Responsable de traitement de fournir aux utilisateurs les Services de sensibilisation achetés auprès du Sous-traitant.

4. Types de données

Les types de données personnelles suivantes, toutes en relations avec les Utilisateurs, sont traitées par le Sous-traitant pour le compte du Responsable de traitement dans le cadre de la fourniture des Services de sensibilisation et tel spécifié dans le Contrat Principal :

(1) Données de connexion et de gestion de compte.
Tous les Services de sensibilisation traitent certains types de données demandées aux Utilisateurs pour se connecter aux Services de sensibilisation et gérer les Services de sensibilisation et les comptes pour le Responsable de traitement ("Données de connexion et de gestion de compte"), qui comprennent notamment :

- Nom et prénom
- Adresses électroniques professionnelles
- Groupes d'Utilisateurs assignés (par exemple, unité organisationnelle, localisation, rôle), niveaux d'accès ;
- *En option* : préférences des Utilisateurs telles que la langue et les formules de politesse

(2) Données d'utilisation
En complément des Données de connexion et de gestion de compte, et en fonction du Service de sensibilisation choisi, d'autres types de données des Utilisateurs peuvent être traitées pour opérer et fournir les Services de sensibilisation, tel que spécifié au Contrat Principal, incluant notamment :

- Informations sur le champ d'application et d'adaptation de l'expérience telles que le poste, le département, le niveau de connaissance initial, les réponses aux questionnaires introductifs ;
- Activité de l'Utilisateur sur la plateforme, telle que l'initiation et l'achèvement de formations, les résultats aux tests, l'interaction avec les tests ;
- *Escalation Manager* (par exemple la relation avec les supérieurs hiérarchiques)
- Modules IA en option : interactions avec des chatbots entraîné par l'IA et autres outils dans la mesure où ils contiennent des données à caractère personnel basées sur les données reçues par le Sous-traitant de la part de d'Utilisateur du Responsable du traitement utilisant le module d'IA.
- Module PhishFeedback en option : paramètres régionaux de l'utilisateur (par exemple, langue, fuseau horaire) et courrier électronique indiqué, qui peuvent tous deux contenir des données personnelles.

(3) Données techniques

Données relatives aux Utilisateurs nécessaires au fonctionnement de l'application et de l'infrastructure et répondant aux engagements de nos Mesures Techniques et Organisationnelles, qui comprennent notamment :

- Les informations sur le système de l'utilisateur requises par l'application, telles que la version du navigateur et de la plate-forme, les informations sur le User Agent ;

- Les données réseau telles que l'adresse IP, l'horodatage, l'URL et les points de terminaison de l'API consultés ;
- Les données de courriers électroniques telles que les adresses de l'expéditeur et du destinataire, les informations d'acheminement et les horodatages ;
- Les données recueillies à partir des intégrations demandées ou mises en œuvre par le Responsable du traitement peuvent inclure des données d'organisation ou d'utilisateur, telles que des alertes provenant d'outils de prévention des pertes de données (DLP), de détection des points de terminaison et d'agents de réponse.

5. Catégories de personnes concernées

Les personnes concernées sont, sauf définition contraire dans le Contrat Principal, tous les Utilisateurs désignés par le Responsable de traitement pour participer. Le Responsable de traitement 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 Sous-traitant 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 configurable et accès aux données en fonction des finalités

Tous les services du Sous-traitant peuvent être configurés de manière à fournir aux administrateurs du Responsable de traitement un accès anonyme et agrégé aux données de l'utilisateur uniquement par défaut. L'accès pour le personnel spécifique du Responsable de traitement à un niveau individuel peut être configuré lorsque le Responsable de traitement le demande clairement et explicitement

2. Chiffrement

2.1 Données en cours de transfert (In transfer)

Tous les transferts de données (aussi bien entre le Responsable de traitement et le Sous-traitant qu'entre tous les employés du Sous-traitant) sont solidement chiffrés conformément aux standards de l'industrie, tels que ECC avec Curve25519, RSA avec une clé de 2048bits ou plus, mise à jour en fonction de l'évolution de l'état de l'art. Le réseau interne et administratif de SoSafe est solidement chiffré. La communication avec les points de terminaison du service nécessite une connexion sécurisée.

2.2 Données au repos (At rest)

Toutes les données personnelles identifiables du Responsable de traitement et de l'utilisateur sont adéquatement chiffrées sur la Plateforme lors du stockage par l'utilisation d'algorithmes et l'implémentation de bonnes et solides pratiques industrielles tels que AES-256-GCM ou plus.

2.3 Données en cours d'utilisation

La solution du Sous-traitant 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 chiffrement.

3. Confidentialité

3.1 Contrôle des accès physiques

Les bureaux du Sous-traitant 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 Sous-traitant. Des alarmes anti-intrusion, une couverture de vidéosurveillance et des procédures d'intervention appropriées sont en place. Les bureaux du Responsable de traitement n'offrent aucun droit d'accès spécial au réseau au-delà de l'accès à Internet.

La plateforme du Responsable de traitement est hébergée par des Fournisseurs de Services Cloud hyperscale leaders du secteur. Ces fournisseurs opèrent à partir de centres de données mettant en œuvre des contrôles de sécurité physique et environnementaux appropriés, tels que, mais sans s'y limiter :

- Suivi et surveillance de tous les accès des visiteurs et des mouvements du personnel
- Videosurveillance avec période de conservation de 90 jours
- Contrôle d'accès fort à tous les espaces d'hébergement de données, de mise en réseau et mécaniques et environnementales
- Au moins N+1 de redondance de l'énergie, des réseaux et des services environnementaux

Les Fournisseurs de Services Cloud doivent disposer d'un certificat ISO 27001 et/ou d'une accréditation SOC2, ou similaire. Le Responsable de traitement évalue leur sécurité physique en examinant les documents d'audit et d'accréditation.

3.2 Contrôle des accès numériques

Tout accès logique nécessite une connexion VPN authentifiée multifacteur. Les réseaux de bureau ne confèrent aucun privilège de réseau spécial au-delà de l'accès à Internet. L'authentification aux systèmes d'entreprisedu Responsable de traitement se fait via l'authentification SSO nécessitant une authentification multifactorielle et des mots de passe forts et définis par des politiques, conformément aux bonnes pratiques de l'industrie. Tous les accès aux systèmes, y compris l'accès aux données du Responsable de traitement, sont fournis sur une base vérifiable, étendue et selon le besoin d'en connaître uniquement. Les droits d'accès des utilisateurs internes sont régulièrement révisés.

3.3 Sécurité des points d'accès

Tous les appareils des utilisateurs finaux sont configurés en toute sécurité par la Gestion des appareils mobiles, qui applique tous les contrôles et utilise des agents de détection et de réponse des points de terminaison. Le chiffrement complet du disque est en place. Les appareils des utilisateurs finaux expirent après un maximum de cinq (5) minutes d'inactivité. Tous les appareils des utilisateurs finaux disposent d'un antivirus et d'un pare-feu individuels avec une fonction de mise à jour automatique. Les mises à jour du système d'exploitation de l'appareil de l'utilisateur final et des versions clés des progiciels sont gérées de manière appropriée.

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 Sous-traitant, seul le personnel nécessaire et habilité dispose d'un accès limité aux renseignements personnels (selon le principe Need-to-Know).

Un politique sur le télétravail est en place. Les informations personnelles ne peuvent être stockées sur les appareils des utilisateurs finaux. Tous les employés sont contractuellement tenus de préserver la confidentialité et de protéger les secrets d'affaires.

Une analyse des risques "bring-your-own-device" (BYOD) a été instauré en verty de ISO 27001 et une politique appropriée est en place pour limiter l'utilisation et les risques posés par le BYOD. Des contrôles appropriés gérés centralement sont en place.

3.5 Suppression des données

La destruction logique des données est assurée par nos Fournisseurs de Services Cloud sous-jacents, conformément aux bonnes pratiques de l'industrie.

Les System Logs et les données de sécurité peuvent être conservés jusqu'à 12 mois à compter de leur création afin de permettre une réponse appropriée aux incidents de sécurité et autres analyses. Les sauvegardes du système sont protégées de manière appropriée et toutes les données de l'utilisateur qu'elles contiennent seront supprimées dans les 12 mois suivant leur création, conformément aux politiques de sauvegarde.

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 Responsables de traitement dans le logiciel, imposé par la logique de base de données.

4. Intégrité

L'accès aux bases de données des systèmes de production est enregistré et conservé pendant douze (12) mois. Des procédures de sauvegarde et de récupération appropriées sont en place pour protéger l'intégrité des données. L'accès à la base de données est limité en fonction du rôle.

5. Disponibilité

5.1 Continuité des activités

Les systèmes de production et les serveurs sont surveillés en permanence par le Sous-traitant de services afin d'assurer une disponibilité constante. Le Sous-traitant exploite une architecture appropriée et un système de continuité des activités dans le cadre d'un audit ISO 27001 et accréditation suffisants pour répondre aux SLA définis dans le Contrat principal. Les serveurs et les systèmes de production sont assurés en permanence chaque jour par des sauvegardes complètes. Les sauvegardes sont chiffrées et stockées sur des systèmes de serveurs distincts du Sous-traitant de services. L'accès est accordé aux administrateurs du Sous-traitant.

5.2 Sensibilisation et formation à la sécurité

Tous les employés du Sous-traitant reçoivent une formation continue et complète (séminaires, e-learning 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 de l'information

6. Gestion des incidents

Le Sous-traitant met en œuvre des mesures appropriées de surveillance de la sécurité, de détection des incidents et de réponse, y compris l'enregistrement technique et des audits automatisés, une équipe opérationnelle de sécurité et une capacité de gestion et de réponse aux incidents à l'échelle de l'organisation. Tous les incidents de sécurité importants, y compris les incidents évités de justesse, nécessitent une analyse formelle rétrospective et des causes profondes.

7. Système de management de la sécurité de l'information

Le Sous-traitant exploite un système de mangement de la sécurité de l'information (SMSI) conformément aux exigences de la norme ISO 27001 et fait l'objet d'un audit externe d'un organisme accrédité auprès de cette dernière. Le Sous-traitant détient également d'autres accréditations, selon les standards de l'industrie, telles que TISAX, tel que requis. Les politiques et procédures formelles d'évaluation et de gestion des risques sont mises en œuvre par l'organisation de sécurité, avec des contributions et des rapports réguliers transmis au Comité Sécurité composé des membres concernés de l'équipesécurité et de l'équipe de direction. Le SMSI est officiellement parrainé et soutenu par l'équipe de direction et le CEO.

Le SMSI et toutes les fonctions de sécurité sont exploités par une organisation de sécurité dotée de ressources appropriées, dirigée par un responsable de la sécurité des systèmes d'information.

8. Évaluation régulière des mesures techniques et organisationnelles

L'ensemble des processus en matière de sécurité, de respect de la vie privée et d'exploitation font l'objet d'un audit interne annuel réalisé par des auditeurs experts et qualifiés, avec la participation du comité SMSI et du comité de sécurité. Le SMSI du Sous-traitant fait l'objet d'un audit externe formel par une société professionnelle crédible au moins une fois par an.

Annexe IV – Liste des sous-traitants ultérieurs

Veuillez consulter https://sosafe-awareness.com/fr/legal/sub-processors/ pour obtenir une liste à jour de nos Sous-traitants, des activités de traitement et des protections en place.

SoSafe SE I Lichtstr. 25a I 50825 Cologne I Directeurs généraux: Dr. Niklas Hellemann, Felix Fichtl I HRB 121629 I Tribunal de Cologne I TVA intracommunautaire: DE322382415 I
Adresse: Lichtstr. 25a I 50825 Cologne I Tel: +49 (0) 221 6508 3800 I
Email: info@sosafe.de I Site internet: sosafe.de