



SIGILIUM

VOTRE SIGNATURE EMAIL, UN ESPACE PRIVILÉGIÉ DE COMMUNICATION

Contrat de traitement des données Data Processing Agreement

Première version décembre 2018
Mise à jour en février 2021 - décembre 2021

1 - Addendum relatif au traitement des données

Contrat de sous-traitance de données personnelles.

Le présent contrat est conclu entre les personnes désignées ci-dessous.

Nom et adresse du Client :

ci-après désigné le Responsable du traitement

Et : Sigilium SARL au capital de 7 000 euros - 809 637 382 R.C.S. Nanterre

11 rue René Weill - 92210 Saint Cloud

ci-après désigné le Sous-traitant.

Cet accord comporte les annexes suivantes:

1. Catégories et types de données personnelles

Préambule

Le responsable du traitement est responsable d'un traitement de données personnelles régi par le 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). Ce règlement est ci-après désigné le RGPD.

Le traitement de données personnelles est également régi par la loi française n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (modifiée).

Le responsable du traitement souhaite confier au sous-traitant un traitement de données personnelles, conformément à l'article 28 du RGPD. Les parties s'engagent à se conformer strictement au RGPD, qui s'appliquera en toute circonstance, nonobstant toute éventuelle stipulation contraire.

Déclaration du sous-traitant

Le sous-traitant déclare qu'il présente les garanties nécessaires quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD et garantisse la protection des droits de la personne concernée.

Caractéristiques du traitement de données personnelles

Le responsable du traitement en définit comme suit les caractéristiques :

Objet du traitement – Le traitement a pour objet la bonne exécution du service proposé par Sigilium, à savoir la gestion centralisée des signatures emails du Client.



VOTRE SIGNATURE EMAIL, UN ESPACE PRIVILÉGIÉ DE COMMUNICATION

Durée du traitement – Le traitement est effectué à compter de la mise en place du service et jusqu'à 9 mois après la résiliation par le client, ce afin de pouvoir répondre en cas de demande des autorités compétentes.

Nature et finalité du traitement – Le service de Sigilium repose sur une plateforme Web qui contient les coordonnées des employés ayant une signature email Sigilium. Le traitement vise à ce que cette signature soit à jour sur le poste de chaque collaborateur. Le traitement vise aussi à connaître le nombre de clic que reçoit chaque annonce relayée ; enfin le traitement des données est nécessaire pour la bonne application du service, notamment la remontée d'une alerte en cas de mauvais fonctionnement du logiciel.

Type de données à caractère personnel - Les données à caractères personnelles recueillies sont celles fournies par le Client:

- L'adresse email du collaborateur
- Les autres informations usuelles, si elles sont fournies par le Client : le nom, l'intitulé de poste, les numéros de téléphone, de fax, l'adresse skype, l'adresse postale de l'entreprise, le portrait.
- Les adresses IP des personnes ayant cliqué sur l'annonce d'un collaborateur dans sa signature ou sa fiche de contact. Nous ne stockons pas de cookies supplémentaires pouvant identifier cette personne. Cette base d'IP est à usage strictement interne à Sigilium et n'est partagée avec aucun autre partenaire. Ces IPs sont conservées 6 mois.
- Toute autre information fournie par le client sous sa responsabilité, dans la limite de leur intérêt pour l'utilisation du service. Toute donnée à caractère sensible de type opinion religieuse, appartenance ethnique etc... sont prosrites dans l'utilisation de notre service.

Catégories de personnes concernées – Les personnes concernées par ce traitement sont celles décidées par le client, en général les collaborateurs de l'entreprise/la filiale utilisant le service.

Encryption des données

Afin de réduire au maximum les risques de perte d'information, en décembre 2021 Sigilium a mis en place l'encryption des intitulés de poste. Ainsi en cas d'accès à une sauvegarde, ou aux données du serveur, ces données sans la clef de décryptage sont totalement indéchiffrables.

La clef de cryptage n'est pas conservée sur le disque dur des serveurs (Bring your Own Key)

Obligations et droits du responsable du traitement

Le responsable du traitement détermine les finalités et les moyens du traitement de données personnelles.

Le responsable du traitement garantit que le traitement est licite et que les données personnelles sont collectées et traitées par ses soins conformément au RGPD et à la loi française. Le responsable du traitement garantit en particulier qu'il fournit les informations requises aux personnes concernées par les opérations de traitement, au moment de la collecte de données lorsque des données à caractère personnel sont collectées auprès de la personne concernée, ou dans les délais requis lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée, conformément aux articles 12 à 14 du RGPD. Le responsable du traitement garantit le sous-traitant contre les conséquences d'un éventuel manquement du responsable du traitement à ses obligations au titre du RGPD.

Le responsable du traitement communiquera au sous-traitant toutes les informations nécessaires pour lui permettre d'effectuer ses services en conformité avec le RGPD et la loi française.

Obligations du sous-traitant

Le sous-traitant ne détermine en aucun cas les finalités et les moyens du traitement. À défaut, il est considéré comme un responsable du traitement pour ce qui concerne le traitement concerné.



VOTRE SIGNATURE EMAIL, UN ESPACE PRIVILÉGIÉ DE COMMUNICATION

Le sous-traitant et toute personne agissant sous son autorité ayant accès à des données à caractère personnel, ne peuvent pas traiter ces données, excepté sur instruction du responsable du traitement, à moins d'y être obligés par le droit de l'Union européenne ou le droit d'un État membre.

Le sous-traitant ne traite les données à caractère personnel que sur instruction documentée du responsable du traitement, y compris en ce qui concerne les transferts de données à caractère personnel vers un pays tiers à l'Union européenne ou à une organisation internationale, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union européenne ou du droit de l'État membre de l'Union européenne auquel le sous-traitant est soumis ; dans ce cas, le sous-traitant informe le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

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.

Le sous-traitant prend toutes les mesures requises en vertu de l'article 32 du RGPD.

Notamment en :

- Limitant l'accès aux données aux personnes (ci-après nommées gestionnaires déléguées), requises pour le bon fonctionnement du service, et dont le nom et les motivations sont disponibles sur simple demande. Et en gardant un registre à jour si une nouvelle personne a besoin d'accéder aux données pendant l'exécution du contrat.
- Sauvegardant de manière sécurisée les données fournies par le client
- Mettant à jour régulièrement les mesures de protection

Le sous-traitant tient compte de la nature du traitement, aide le responsable du traitement, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées par le traitement le saisissent en vue d'exercer leurs droits prévus au chapitre III du RGPD.

Le sous-traitant aide le responsable du traitement à garantir le respect des obligations prévues aux articles 32 à 36 du RGPD, compte tenu de la nature du traitement et des informations à la disposition du sous-traitant.

Le sous-traitant informe immédiatement le responsable du traitement si, selon lui, une instruction constitue une violation du RGPD ou d'autres dispositions du droit de l'Union ou du droit des États membres relatives à la protection des données.

Gestionnaires délégués de Sigilium ajoutés après la Date d'entrée en vigueur.

Sigilium informera le Client au préalable en cas de changement de gestionnaires délégués, par le biais de moyens de communication classiques, tels que les e-mails, les sites Web et les portails. Si le Client s'oppose de manière raisonnable à l'ajout de nouveaux gestionnaires délégués, (p. ex., si ledit changement entraîne la non-conformité du Client aux Lois et réglementations sur la protection des données en vigueur), le Client informera Sigilium par écrit de ses objections spécifiques dans un délai de trente (30) jours après avoir reçu la nouvelle notification. Si le Client ne s'y oppose pas dans les délais impartis, l'ajout de tout nouveau gestionnaire délégué et, le cas échéant, l'accord donné au titre du présent DPA seront réputés acceptés. Si le Client s'oppose à l'ajout d'un nouveau gestionnaire délégué, mais que Sigilium ne peut tenir compte de l'objection du Client, ce dernier peut résilier les Services et Logiciels par écrit, dans un délai de soixante (60) jours après avoir reçu la notification de Sigilium.

Conservation et destruction des données

Selon le choix du responsable du traitement, le sous-traitant supprime toutes les données à caractère personnel ou les renvoie au responsable du traitement au terme de la prestation de services relatifs au traitement, et détruit les copies existantes, à moins que le droit de l'Union européenne ou le droit applicable d'un État membre n'exige la conservation des données à caractère personnel.

L'ensemble des données de Sigilium sont stockées au sein de l'Union Européenne.



VOTRE SIGNATURE EMAIL, UN ESPACE PRIVILÉGIÉ DE COMMUNICATION

Audit

Le sous-traitant met à la disposition du responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations prévues au présent contrat et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits. Etant donné le rapport entre le temps demandé par un audit et le coût du service, l'audit sera facturé au temps passé, avec un tarif horaire de 150€HT.

Autre sous-traitant

Le sous-traitant respecte les conditions suivantes pour recruter un autre sous-traitant.

Le client autorise de manière générale le sous-traitant à choisir ses prestataires, ceux-ci respectant le RGPD, le sous-traitant informe le responsable du traitement de tout changement prévu concernant l'ajout ou le remplacement d'autres sous-traitants, donnant ainsi au responsable du traitement la possibilité d'émettre des objections à l'encontre de ces changements.

Lorsqu'un sous-traitant recrute un autre sous-traitant pour mener des activités de traitement spécifiques pour le compte du responsable du traitement, les mêmes obligations en matière de protection de données que celles fixées dans le présent contrat, sont imposées à cet autre sous-traitant par contrat ou le cas échéant au moyen d'un autre acte juridique au titre du droit de l'Union européenne ou du droit d'un État membre, en particulier pour ce qui est de présenter des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD. Lorsque cet autre sous-traitant ne remplit pas ses obligations en matière de protection des données, le sous-traitant initial demeure pleinement responsable devant le responsable du traitement de l'exécution par l'autre sous-traitant de ses obligations.

La liste des sous-traitant étant lié aux données personnelles est disponible sur demande.

Durée

Le présent contrat sera en vigueur pendant toute la durée de détention des données personnelles par le sous-traitant. Il régira la sous-traitance des données personnelles visées ici, à toute époque y compris après son terme.

Droit applicable et clause attributive de compétence

Le présent contrat est soumis au droit français et à la compétence exclusive des juridictions territorialement compétentes pour la ville de Saint-Cloud 92210, France.

Annexe 1 : Catégories et types de données personnelles

Nom de famille

Prénom

Adresse postale professionnelle complète

Téléphone fixe et gsm professionnelle

Poste occupée dans l'entreprise

Adresse email professionnelle

Annexe 2 : Liste des sous-traitants agréés

- Hébergement des serveurs

Les serveurs sont hébergés par la société Amazon (service AWS) dans son data-center Parisien 67 Boulevard du Général Leclerc à Clichy, filiale de Amazon 410 Terry Avenue North P.O. Box 81226 Seattle, WA 98108-1226 - USA. Représentée Frédéric Duval (Amazon AWS France)

- Rénald Koch (Siret 79828545800013) est amené à améliorer la configuration des serveurs en cas de problème.



VOTRE SIGNATURE EMAIL, UN ESPACE PRIVILÉGIÉ DE COMMUNICATION

- HoneyBadger (Honeybadger Industries LLC 11410 NE 124th Street #246 Kirkland, WA 98034), représenté par Ben Curtis, est amené à remonter des alertes d'erreur.
- Mailjet, représenté par Darine Fayed (Head of legal & DPO), est amené à envoyer des emails d'installation aux collaborateurs.

Annexe 3 : Liste des personnes pouvant traiter les données personnelles

Thomas Darde, Xavier Trannoy et Tristan Belin (chacun étant associé ou employé à temps complet de Sigilium)

Annexe 4 : Lieux de stockage des données personnelles

Les données du Responsable de traitements sont stockées sur une ferme de serveurs loués par le Sous-traitant. Ces serveurs sont géographiquement obligatoirement situés en France Métropolitaine.

Annexe 5 : Mesures de sécurité informatique complémentaires

Tous les mots de passe sont sécurisés en obligeant l'utilisation de caractères complexes et avec une longueur de 12 caractères minimum.

L'accès aux données des client est crypté à l'aide de certificat SSL