Data processing agreement

Classification : Public	Date : 30 octobre 2024	Version : 17

Entre

……,

ayant son siège social situé ……,

immatriculée au registre du commerce et des sociétés de ……,

représentée par ……,

(ci-après, « le responsable de traitement») d'une part,

Et
Talkspirit, Société à Actions Simplifiées au capital de 16.000,00 €, ayant son siège social situé 72, rue du Faubourg Saint-Honoré à Paris (75008), immatriculée au registre du commerce et des sociétés de Paris sous le numéro d'identification 479 109 332,
(ci-après, « ***le sous-traitant***») d'autre part,

I. Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le sous-traitant s'engage à effectuer pour le compte du responsable de traitement les opérations de traitement de données à caractère personnel définies ci-après.

Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 (ci-après, « **le règlement européen sur la protection des données** » ou "**RGPD**").

II. Description du traitement faisant l'objet de la sous-traitance

Le sous-traitant est autorisé à traiter pour le compte du responsable de traitement les données à caractère personnel nécessaires pour fournir le ou les service(s) suivant(s) : administration et hébergement d'un réseau social d'entreprise.

Les traitements de données à caractère personnel confiés au sous-traitant par le responsable de traitement au titre des services sont décrits en Annexe A.

III. Durée du contrat

Le présent contrat entre en vigueur à compter de l'entrée en vigueur et pour toute la durée du contrat principal de service signé entre les Parties.

IV. Obligations du sous-traitant vis-à-vis du responsable de traitement

Le sous-traitant s'engage à :

1. traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet de la sous-traitance.

2. traiter les données conformément aux instructions documentées du responsable de traitement et selon les stipulations du présent contrat. Si le sous-traitant considère qu'une instruction constitue une violation du règlement européen sur la protection des données ou de toute autre disposition du droit de l'Union ou du droit des Etats membres relative à la protection des données, il en informe immédiatement le responsable de traitement.

3. garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent contrat.

4. veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent contrat :

- s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité
- reçoivent la formation nécessaire en matière de protection des données à caractère personnel

5. prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception et de protection des données par défaut.

6. Sous-traitance / Transferts de données hors Europe

Le sous-traitant peut faire appel à un autre sous-traitant (ci-après, « le sous-traitant ultérieur ») pour mener des activités de traitement spécifiques. La liste des sous-traitants ultérieurs utilisés par le sous-traitant à la date de signature du présent contrat est renseignée en Annexe C. Le sous-traitant pourra faire appel à un autre sous-traitant ultérieur pendant le contrat pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le responsable de traitement de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance. Le responsable de traitement dispose d'un délai minimum de 3 semaines à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le responsable de traitement n'a pas émis d'objection pendant le délai convenu.

Le sous-traitant ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du responsable de traitement. Il appartient au sous-traitant initial de s'assurer que le sous-traitant ultérieur présente les mêmes 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 règlement européen sur la protection des données. Si le sous-traitant ultérieur ne remplit pas ses obligations en matière de protection des données, le sous-traitant demeure pleinement responsable devant le responsable de traitement de l'exécution par le sous-traitant ultérieur de ses obligations.

Certains des sous-traitants ultérieurs utilisés par le sous-traitant peuvent être situés dans un pays hors de l'Espace Economique Européen, plus spécifiquement les Etats-Unis, comme indiqué au sein de l'Annexe C au regard des sous-traitants ultérieurs actuellement utilisés. Dans une telle situation, le sous-traitant devra conclure avec le sous-traitant ultérieur concerné les clauses contractuelles types

approuvées par la Commission Européenne encadrant le transfert des données personnelles vers un pays tiers à l'Espace Économique Européen. Le cas échéant, le sous-traitant s'engage également à vérifier que le sous-traitant ultérieur concerné a bien mis en place toutes les mesures additionnelles permettant de garantir le respect par ce dernier d'un niveau de protection des données à caractère personnel transférées équivalent à celui applicable en vertu du RGPD.

7. Droit d'information des personnes concernées

Le sous-traitant, au moment de la collecte des données, doit fournir aux personnes concernées par les opérations de traitement l'information relative aux traitements de données qu'il réalise. La formulation et le format de l'information doit être convenue avec le responsable de traitement avant la collecte de données.

8. Exercice des droits des personnes

Dans la mesure du possible, le sous-traitant doit aider le responsable de traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).

A ce titre, lorsque les personnes concernées exercent directement auprès du sous-traitant des demandes d'exercice de leurs droits, le sous-traitant doit adresser ces demandes dans les meilleurs délais par courrier électronique au responsable de traitement afin que ce dernier puisse les traiter dans les délais requis par le RGPD.

9. Notification des violations de données à caractère personnel

Le sous-traitant notifie au responsable de traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance. Cette notification est accompagnée de toute documentation utile afin de permettre au responsable de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

Cette notification est accompagnée de toute documentation utile afin de permettre au responsable de traitement et si cela est nécessaire, de notifier cette violation à l'autorité de contrôle compétente et aux personnes concernées.

Compte tenu de la nature des traitements qu'il opère et dans les limites des informations à sa disposition, le sous-traitant collaborera de bonne foi afin d'aider le responsable de traitement à :

- Notifier la violation à l'autorité de contrôle compétente, lorsque cela est nécessaire ;
- Informer les personnes concernées de la violation, lorsque cela est nécessaire.

10. Aide du sous-traitant dans le cadre du respect par le responsable de traitement de ses obligations

Le cas échéant, le sous-traitant aide le responsable de traitement pour la réalisation d'analyses d'impact relative à la protection des données.
Le cas échéant, le sous-traitant aide le responsable de traitement pour la réalisation de la consultation préalable de l'autorité de contrôle.

11. Mesures de sécurité

Le sous-traitant s'engage à mettre en œuvre les mesures de sécurité décrites en annexe B.

12. Sort des données

Au terme de la prestation de services relatifs au traitement de ces données, le sous-traitant s'engage à :
Au choix des parties :

- détruire toutes les données à caractère personnel ou
- à renvoyer toutes les données à caractère personnel au responsable de traitement ou
- à renvoyer les données à caractère personnel au sous-traitant désigné par le responsable de traitement

Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du sous-traitant. Une fois détruites, le sous-traitant doit justifier par écrit de la destruction.

13. Délégué à la protection des données

Le sous-traitant communique au responsable de traitement le nom et les coordonnées de son délégué à la protection des données, s'il en a désigné un conformément à l'article 37 du règlement européen sur la protection des données.

Le DPO est :
Charles Bayle
privacy@talkspirit.com

14. Documentation

Le sous-traitant met à la disposition du responsable de traitement la documentation nécessaire pour démontrer le respect de toutes ses obligations 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.

Il est toutefois précisé que tout audit sera réalisé aux frais du responsable de traitement et strictement limité à l'audit des mesures prises en matière de protection des données à caractère personnel, dans la limite d'un audit par an notifié au moins un (1) mois à l'avance au sous-traitant.

V. Obligations du responsable de traitement vis-à-vis du sous-traitant

Le responsable de traitement s'engage à :

- 1. fournir au sous-traitant les données visées au II des présentes clauses
- 2. documenter par écrit toute instruction concernant le traitement des données par le sous-traitant
- 3. veiller, au préalable et pendant toute la durée des traitements, au respect des obligations prévues par le RGPD, notamment vis-à-vis des personnes concernées par les traitements.

Fait en deux (2) exemplaires originaux,

A Paris le ……

Le Responsable de Traitement	Le Sous-Traitant
Pour ……	Pour la Société,
	Philippe PINAULT

TALKSPIRIT
72, rue du Faubourg Saint-Honoré 75008 Paris
Tél : +33 970 19 90 00
SAS au capital de 16 000 euros
SIRET 479 109 332 00052 - APE 6201Z
TVA : FR 50 479 109 332
http://www.talkspirit.com

Annexe A. Vue d'ensemble des données personnelles à traiter

Les différentes catégories de données traitées par le sous-traitant sont :

- Données collectées: pour être membre de la plateforme, des informations personnelles tel que le nom, prénom, email, mot de passe, photo sont enregistrées. L'utilisateur peut renseigner des informations additionnelles telles que son poste, sa bio, ses compétences ou ses expertises, ses collègues, son responsable,des liens vers ses profils de réseaux sociaux (Linkedin, Twitter) ainsi que toute information additionnelle demandée par le responsable du traitement par le biais de champs personnalisés sur le profil
- Données de la plateforme: Lors de l'utilisation de la Plateforme, les serveurs enregistrent de manière systématique les informations de session et les actions sur le logiciel
- Les fichiers de logs enregistrent l'adresse IP, les informations sur l'ordinateur (OS) et le navigateur web

Les traitements effectués sur ces données ont pour finalités de :

- de fournir le service aux utilisateurs, incluant une assistance en ligne et un support
- permettre au responsable de traitement, via le logiciel, d'administrer un réseau social d'entreprise
- respecter les obligations légales et réglementaires

Catégories de personnes concernées par les traitements :

Les différentes catégories de personnes impactées par la gestion des données personnelles sont:

- les stagiaires et les étudiants embauchés
- les salariés (les employés, stagiaires, freelances)
- Les fournisseurs et sous-traitants

La nature des traitements opérés sont la collecte, l'hébergement et la suppression des données.

Les données sont traitées par le sous-traitant pour la durée du contrat principal de service conclu avec le responsable de traitement.

Annexe B. Mesures techniques et organisationnelles visant à assurer la sécurité du traitement

A. Mesures pour assurer la confidentialité

1. Contrôle d’accès physique

Seul le personnel d’OVH habilité peut accéder aux datacenters et à la connectivité réseau.

2. Contrôle d'accès logique
Mesures visant à empêcher les personnes non autorisées de traiter ou d'utiliser des données protégées par la législation sur la protection des données.

Description du système de contrôle d'accès logique:

- Chaque membre possède un haut niveau de qualification Chaque membre est formé aux bonnes pratiques en matière de confidentialité et de sécurité
- Seuls les rôles Infrastructure et DevOps peuvent accéder aux serveurs de production. L'accès à distance aux serveurs par nos équipes n'est possible qu'avec des clés via SSH. L'accès SSH par mot de passe est désactivé.

3. Contrôle d’accès

Toutes les données sensibles sont enregistrées dans le Cloud. Les accès ne sont possibles que via certaines adresses IP et un nom d'utilisateur qui sont enregistrés. Les PC sont protégés avec un mot de passe connu de l'employé uniquement.
OVH propose un service de protection Anti-DDOS à la pointe. De plus, les pare-feu sont configurés conformément aux normes de l'industrie approuvées, conformément aux règles UFW IPTABLES. De plus, les ports inutiles sont bloqués pour autoriser uniquement le trafic sur les ports 80 (http) et 443 (https).

4. Contrôle d’accès aux données

Talkspirit fournit des journaux d'accès détaillés qui enregistrent chaque connexion établie à un compte. De plus, des attributs tels que le type de périphérique utilisé et l'adresse IP de connexion respective sont également enregistrés automatiquement.
Les accès client sont protégés par TLS 1.1 ou supérieur
Les journaux d'applications sont sauvegardés tous les 3 jours sur la solution de stockage d'objets d'OVH.

5. Contrôle de séparation

- Le cloisonnement des données est garanti par le logiciel
- Notre API est faite en PHP sur le framework Symfony 4
- L'API s'appuie sur un l’ODM (Object Document Mapper) Doctrine pour accéder à la base de données. La brique Doctrine fournit un mécanisme dit de "filtre" pour la gestion de données multi-clients.

6. Pseudonymisation

Talkspirit ne fait aucun traitement sur les données. Lorsque les données doivent être utilisées sur un environnement de transfert, nous les anonymisons. Les statistiques sont consolidées chaque jour afin d'éviter d'utiliser les données client.

7. Cryptage

Talkspirit prend en charge les dernières suites de chiffrement sécurisé et les protocoles recommandés pour chiffrer tout le trafic. Le transfert des données entre les serveurs et les postes de travail des utilisateurs est sécurisé via un certificat SSL AES-256 bits.

Nous surveillons de près l'évolution du paysage cryptographique et nous nous efforçons de mettre à niveau rapidement pour répondre aux menaces émergentes au fur et à mesure de leur découverte, tout en mettant en œuvre les meilleures pratiques au fur et à mesure de leurs évolutions.
Les mots de passe de l'utilisateur sont cryptés à l'aide de l'algorithme Bcrypt avec un facteur coût de 10.

Pour les applications frontales (applications de site Web, de bureau et mobiles), l'authentification auprès de l'API afin d'accéder aux données se fait via le protocole OAuth 2

Les administrateurs peuvent également intégrer leur plateforme avec différents fournisseurs d'authentification unique: Google ou un service fournissant une authentification unique SAML (telle que OneLogin, Okta).

B. Mesures pour assurer l'intégrité

1. Contrôle de relais

Talkspirit prend en charge les dernières suites de chiffrement sécurisé et les protocoles recommandés pour chiffrer tout le trafic. Le transfert des données entre les serveurs et les postes de travail des utilisateurs est sécurisé via un certificat SSL AES-256 bits.
talkspirit configure TLS pour la sécurité, et un rapport mis à jour sur notre configuration est accessible sur https://www.ssllabs.com/ssltest/analyze.html?d=www.talkspirit.com&hideResults=on&latest.
Nous surveillons de près l'évolution du paysage cryptographique et nous nous efforçons de mettre à niveau rapidement les menaces émergentes au fur et à mesure de leur découverte, tout en mettant en œuvre les meilleures pratiques au fur et à mesure de leur évolution.
talkspirit utilise le cryptage fort pour toutes les autres transmissions de données personnelles en dehors du centre de données de production.
Un réseau privé virtuel a été configuré pour permettre à certains membres du personnel d'administrer les serveurs

2. Intégrité des données

Talkspirit a une approche de défense en profondeur pour assurer la confidentialité et l'intégrité, et de nombreuses mesures décrites dans d'autres sections de ce document préservent la confidentialité et l'intégrité. Parmi les autres mesures qui y contribuent :

- Une procédure formelle de vérification des antécédents d'un collaborateur
- talkspirit forme ses ingénieurs en logiciel aux pratiques de sécurité des applications et de codage sécurisé.
- Un référentiel centralisé et sécurisé du code source sur Github, accessible uniquement au personnel autorisé.
- Les tests de sécurité incluent la révision du code et l'utilisation périodique d'outils d'analyse de code statique pour identifier les failles.
- Toutes les modifications apportées au logiciel sont publiées dans un environnement intermédiaire, complètement séparé de l'environnement de production. Les mêmes processus s'appliquent au déploiement et aux installations logicielles pour les deux environnements.

- Des tests d'intrusions annuels sont effectués par une entreprise indépendante afin d'assurer l'intégrité de la plateforme

3. Contrôle d'entrée

Toutes les demandes de l'application sont consignées dans une base de données Elasticsearch hébergée par OVH (solution LogsDataPlatform) pendant 45 jours. Il n'est pas possible de supprimer ou de modifier les données. L'accès est limité à l'équipe technique.
Les accès aux serveurs sont également enregistrés pendant 4 semaines.

C. Mesures visant à assurer la disponibilité et la résilience

1. Contrôle de disponibilité control

L'application est hébergée sur le cloud privé OVH avec un SLA de 99,99%
En ce qui concerne les sauvegardes, une sauvegarde quotidienne de la base de données est effectuée sur 7 jours glissants sur le serveur, c'est-à-dire que le 8e jour remplacera alors la sauvegarde la plus ancienne. Une autre sauvegarde est effectuée quotidiennement sur le cloud de stockage d'objets d'OVH, ce qui permet une conservation de 6 mois.
Les fichiers client sont répliqués quotidiennement dans la solution de stockage d'objets d'OVH. Ils sont enregistrés sur des sites distants.
Nos serveurs sont mis à jour en permanence avec les derniers correctifs de sécurité. Les installations de serveur, les mises à jour et les déploiements de logiciels sont entièrement automatisés.
Les serveurs sont installés via des scripts Ansible. Les scripts sont testés régulièrement via une machine Vagrant.
Le logiciel est automatiquement déployé sous forme de paquet Debian envoyé par le service CircleCi lorsque divers tests automatiques ont été effectués. Chaque déploiement génère un artefact qui permet une restauration sur une version spécifique du logiciel.
La mise en production est tracée.

2. Rétablissement d'urgence

Talkspirit s'appuie sur l'offre private cloud SDDC d'OVH et a configuré son infrastructure en mode HA. Ainsi en cas de défaillance matérielle d'un serveur, notre prestataire OVH peut nous fournir un nouveau serveur en une ½ heure. En cas de problème matériel ponctuel l'outil de virtualisation VMWARE redémarre les machines virtuelles de manière automatique afin de réduire le temps d'indisponibilité.
Enfin talkspirit a crée une infrastructure as code, c'est-à-dire que l'ensemble des installations de serveurs et des mises à jour sont codées à l'aide de scripts Ansible. Les temps de mise à jour ou création étant réduit à l'exécution des scripts.
En cas de perte du datacenter principal pendant une durée significative, il est possible remonté une infrastructure temporaire sur le cloud d'OVH sous 1 jour. L'ensemble des données étant sauvegardé sur un autre datacentre d'OVH.
De manière régulière les scripts de restauration des base de données sont exécutés dans le cadre de tests d'exécution des scripts de migration.

3. Fiabilité

Le monitoring est assuré par plusieurs outils complémentaires.

- L'outil Vsphere de VMWARE permet un 1er niveau de monitoring des serveurs

- L’outil Prometheus, associé à Grafana, permet à l’équipe d’infrastructure de monitorer l’état de bon fonctionnement des serveurs.
- Enfin le service Pingdom est également utilisé pour surveiller le site à travers différents endroits du monde. La surveillance de Pingdom est accessible via https://talkspirit.status.io

Les deux outils ont des applications mobiles permettant une notification immédiate et une réaction aux problèmes potentiels. L'équipe d'infrastructure dispose de toutes les applications déployées.
La page talkspirit.status.io est le principal moyen de communication que nous utilisons en cas d’incident majeur ou de maintenance sur la plate-forme.

D. Mesures d’évaluation régulière

1. Gestion de la confidentialité

Nous n’accédons pas aux données personnelles du client, sauf
- pour fournir des services au client que talkspirit est obligé de fournir à l’appui de l’expérience client,
- pour le fonctionnement général et la surveillance de l’application de talkspirit, à des fins de correctifs et de maintenance,
- pour des raisons de sécurité, comme requis par loi, ou sur demande du client.

Nous utilisons un nombre limité de prestataires pour le fonctionnement du service. Des sociétés tierces utilisées en tant que prestataires sont disponibles à l’Annexe C.

2. Gestion des réponses en cas d’incident

Nous maintenons une page décrivant l’état du service et les incidents. Nous communiquons avec les clients via https://talkspirit.statuspage.io.

Annexe C. Liste des prestataires

Voici la liste des sous-traitants de talkspirit

Entreprise: **Fibery**
Activité de traitement de données: Pilotage du produit
Localisation: Chypre
Mesures / garanties pour assurer un niveau approprié de protection des données :
https://fibery.io/cloud-security
https://fibery.io/privacy-policy

Entreprise: **Google Firebase**
Activité de traitement de données : Notifications Mobile Push
Localisation : Etats-Unis
Certifications : ISO27001
Mesures / garanties pour assurer un niveau approprié de protection des données
https://policies.google.com/privacy?hl=en

Entreprise: **Intercom**
Activité de traitement de données: Support en temps réel et intégration des utilisateurs
Localisation : Etats-Unis

Certifications : SOC2
Mesures / garanties pour assurer un niveau approprié de protection des données :
https://www.intercom.com/fr/security
https://docs.intercom.com/pricing-privacy-and-terms/data-protection/how-were-preparing-for-gdpr

Entreprise: **Mailgun**
Activité de traitement de données : Publication par mail
Localisation: Etats-Unis
Mesures / garanties pour assurer un niveau approprié de protection des données :
https://www.mailgun.com/gdpr

Entreprise: **Outscale**
Activité de traitement de données : Fournisseur d'hébergement
Localisation : France
Certifications : SecNumCloud, ISO27001
Mesures / garanties pour assurer un niveau approprié de protection des données :

Entreprise: **OVH**
Activité de traitement de données : Fournisseur d'hébergement
Localisation : France
Certifications : SOC1/2/3, SecNumCloud, ISO27001
Mesures / garanties pour assurer un niveau approprié de protection des données :
https://www.ovh.com/fr/private-cloud/documentation/certifications.xml
https://www.ovh.com/fr/protection-donnees-personnelles/

Entreprise : **PingDom**
Activité de traitement de données : Monitoring applications web
Localisation: Etats-Unis
Mesures / garanties pour assurer un niveau approprié de protection des données :
https://www.solarwinds.com/general-data-protection-regulation-cloud

Entreprise: **Postmark**
Activité de traitement de données : Emails transactionnels
Localisation: Etats-Unis
Certifications : SOC1
Mesures / garanties pour assurer un niveau approprié de protection des données :
https://postmarkapp.com/security
https://postmarkapp.com/eu-privacy

Entreprise: **Satismeter**
Activité de traitement de données: Mesure du NPS (Net Promoter Score), satisfaction client
Localisation: République Tchèque
Mesures / garanties pour assurer un niveau approprié de protection des données :
https://www.satismeter.com/security-policy
https://www.satismeter.com/privacy-policy

Entreprise: **Sentry**
Activité de traitement de données: logs applicatif frontend
Localisation: Etats-Unis
Certifications : ISO27001, SOC2
Mesures / garanties pour assurer un niveau approprié de protection des données :

https://sentry.io/security/
https://sentry.io/privacy/

Entreprise: **Sparkpost**
Activité de traitement de données: Emails non transactionnels
Localisation: Etats-Unis
Certifications : SOC2
Mesures / garanties pour assurer un niveau approprié de protection des données :
https://www.sparkpost.com/policies/security/
https://www.sparkpost.com/policies/privacy/

Entreprise: **Startdeliver**
Activité de traitement de données: Accompagnement, support et onboarding client
Localisation: Suède
Mesures / garanties pour assurer un niveau approprié de protection des données :
https://support.startdeliver.com/en/articles/4782038-privacy-policy
https://support.startdeliver.com/en/articles/7845368-startdeliver-compliance-with-eu-data-transfer-requirements