

CONTRAT DE SOUS-TRAITANCE DES DONNÉES PERSONNELLES (RGPD, ARTICLE 28)

Ce contrat lie le client, responsable du traitement, et EASYTEL, editrice du service Nolia (« Nolia »), sous-traitant, pour les données personnelles que Nolia traite pour le compte du client dans le service. Il fait partie du contrat décrit à l'article 1 des conditions générales de vente et d'utilisation de Nolia, dont les définitions s'appliquent ici. Il s'applique tant que Nolia traite des données pour le client, jusqu'à leur suppression.

1. LES CLAUSES TYPES

Les parties appliquent, telles quelles, les clauses contractuelles types entre responsables du traitement et sous-traitants de la décision d'exécution (UE) 2021/915 de la Commission du 4 juin 2021

(<https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32021D0915>), ci-après les « clauses ». Elles retiennent l'option 2 de la clause 7.7 : autorisation générale écrite des sous-traitants ultérieurs figurant sur la liste convenue (annexe IV), avec un délai d'information de 30 jours.

Les clauses prévalent sur toute stipulation contraire des conditions générales et de tout autre document contractuel. Les annexes I à IV ci-dessous en font partie. L'article 2 précise les clauses sans les contredire.

2. PRÉCISIONS CONVENUES

- Instructions (clause 7.1) : les instructions du client sont les documents contractuels, les réglages qu'il fait dans son espace et ses instructions écrites ultérieures. Nolia l'informe sans délai si une instruction lui paraît contraire à la réglementation sur la protection des données.
- Personnel de Nolia (clause 7.4) : il n'accède au contenu de l'espace (fiches, plannings, heures, arrêts de travail, documents, messages, signalements) que dans trois cas : sur instruction écrite du client, limitée à son objet et à sa durée ; dans la mesure strictement nécessaire à l'exploitation technique du service (sauvegarde, restauration, correction d'un incident) ; pour examiner un contenu précis qui lui est signalé comme illicite. Il est tenu à la confidentialité. Chaque geste de Nolia sur l'espace (prolongation, suspension, changement d'administrateur, par exemple) est annoncé à l'administrateur et noté dans la page « Interventions de Nolia ».
- Données sensibles (clause 7.5) : les arrêts de travail et les signalements ne sont accessibles qu'aux rôles prévus à l'annexe II et sont protégés comme le décrit l'annexe III.
- Violation de données (clause 9.2) : Nolia alerte le client, par e-mail à l'administrateur, au plus tard 48 heures après en avoir eu connaissance. Elle lui transmet ensuite, au fur et à mesure, les éléments de l'article 33, paragraphe 3, du RGPD : nature de la violation, catégories et nombre approximatif de personnes et d'enregistrements concernés, conséquences probables, mesures prises ou proposées, personne à contacter.
- Demandes des personnes (clause 8) : Nolia transmet sans délai au client toute demande reçue d'une personne concernée ; le client y répond. Nolia ne communique de données directement à une personne que sur instruction écrite du client. Elle l'aide à répondre, notamment en lui fournissant les données d'une personne dans un format lisible par une machine.
- Analyse d'impact (clause 8) : Nolia fournit au client les informations dont il a besoin sur le service et ses mesures de sécurité pour son analyse d'impact et, le cas échéant, la consultation de la CNIL.
- Audits (clause 7.6) : Nolia met à la disposition du client les informations nécessaires pour démontrer le respect de ses obligations. Le client peut faire un audit une fois par an au plus, avec un préavis écrit de 30 jours, lui-même ou par un auditeur indépendant tenu au secret professionnel et qui n'est pas un concurrent de Nolia, à ses frais. Cette limite ne s'applique pas après une violation de données ni en cas d'indice sérieux de manquement. L'audit ne doit ni compromettre la sécurité du service, ni donner accès aux données des autres clients.
- Sous-traitants ultérieurs (clause 7.7) : la liste convenue figure à l'annexe IV. Nolia informe le client par e-mail de tout ajout ou remplacement au moins 30 jours avant que le nouveau sous-traitant ne traite des données, avec son nom, son rôle, les données concernées, son lieu et les garanties. Le client peut s'y opposer pendant ce délai, par un e-mail motivé à contact@noliagroupe.fr. Si les parties ne trouvent pas de solution, le client peut résilier le contrat sans frais avant l'arrivée du nouveau sous-traitant.
- Transferts (clause 7.8) : les données sont hébergées en France. Seuls ont lieu hors de l'Union européenne les transferts décrits à l'annexe IV, vers les services de notification des navigateurs, quand un utilisateur active les notifications sur son appareil.
- Conservation : pendant le contrat, Nolia applique les durées de conservation décrites sur la page Confidentialité du site de Nolia. Une autre durée demandée par le client se convient par écrit.

- Fin du contrat (clause 10) : dans les 30 jours qui suivent la fin du contrat, Nolia remet au client l'export complet de ses données, dans les formats prévus à l'article 20 des conditions générales, sauf si le client a choisi la suppression sans restitution. Dans les 30 jours suivants, soit au plus tard 60 jours après la fin du contrat, elle supprime toutes les données traitées pour le client ; les sauvegardes qui les contiennent sont effacées au terme de leur rotation. Nolia remet au client une attestation écrite de suppression. Elle ne garde que ce que la loi lui impose de conserver.
- Note d'information des salariés : le client la remet ; Nolia fournit le modèle et garde la trace de sa remise.
- Registre : Nolia tient le registre des traitements qu'elle effectue pour le compte de ses clients (article 30, paragraphe 2, du RGPD).

ANNEXE I – LES PARTIES

Responsable du traitement : chaque société cliente au nom de laquelle l'administrateur accepte ce contrat, désignée par sa raison sociale, son SIREN, son siège et son contact tels qu'ils sont enregistrés dans son espace et copiés dans la preuve de son acceptation. Signataire : l'administrateur, avec la fonction qu'il déclare.

Sous-traitant : EASYTEL, société à responsabilité limitée, 20 avenue Foch, 57000 Metz, RCS Metz 498 434 448, editrice du service Nolia. Contact pour la protection des données : contact@noliagroupe.fr.

ANNEXE II – DESCRIPTION DU TRAITEMENT

Personnes concernées : les salariés du client, y compris les extras, les apprentis, les stagiaires, les intérimaires et les anciens salariés, ainsi que ses managers, sa direction et ses ressources humaines.

Catégories de données :

- identité et coordonnées professionnelles, date de naissance, matricule de paie ;
- mentions du registre unique du personnel : nationalité, sexe, emploi, qualification, dates d'entrée et de sortie, titre de travail et sa validité pour un salarié étranger ;
- contrat : type, durée, horaire, société employeuse ; taux horaire brut ;
- planning prévu et publié, heures réalisées, badges, visas, contestations, clôtures, compteurs ;
- demandes d'absence et congés ; arrêts de travail, réduits au volet destiné à l'employeur, sans motif médical ;
- documents déposés : contrats, avenants, conventions, justificatifs, bulletins de paie ;
- messages et signalements ;
- données de connexion et de sécurité : adresse IP, navigateur, appareils connus, journal d'audit, abonnements aux notifications.

Données sensibles : le fait qu'un salarié soit en arrêt de travail, qui est une donnée de santé ; les signalements, qui peuvent en révéler d'autres. Le numéro de sécurité sociale figure sur les bulletins de paie déposés. Garanties : accès limité aux rôles qui en ont besoin (un manager opérationnel ne voit pas les arrêts de travail ; un signalement n'est lu que par la direction et les ressources humaines, jamais par la personne signalée), chiffrage au repos et mesures de l'annexe III.

Nature des opérations : hébergement, enregistrement, consultation, calcul (règles de durée du travail, compteurs, paie, coût du personnel), mise en forme (PDF, Word, exports), envoi d'e-mails et de notifications, sauvegarde, restitution et suppression.

Finalité : fournir au client le service décrit à l'article 4 des conditions générales : organisation du travail, décompte et preuve du temps de travail, préparation de la paie, communication interne, gestion administrative du personnel.

Durée : celle du contrat, puis jusqu'à la restitution et à la suppression prévues à l'article 2.

ANNEXE III – MESURES DE SÉCURITÉ

- Hébergement en France ; toutes les connexions chiffrées (TLS).
- Cloisonnement de chaque client, et de chaque rôle, appliqué par le moteur de la base de données (sécurité au niveau des lignes) ; l'application s'y connecte avec un rôle sans privilège d'administration.
- Documents, messages et signalements chiffrés (AES-256-GCM), avec une clé conservée hors de la base ; sauvegardes chiffrées.
- Tables de preuve (visas, contestations, clôtures, acceptations, textes) en ajout seul, avec des empreintes calculées par la base ; dossiers de preuve signés.
- Mots de passe d'au moins 12 caractères, hachés, refusés s'ils sont connus d'une fuite ; nombre d'essais limité et verrouillage après des essais répétés.

- Double authentification obligatoire pour la direction, les ressources humaines et les managers (clé d'accès, clé de sécurité ou application d'authentification) ; vérification en deux étapes des salariés sur un appareil nouveau ; avis par e-mail de chaque connexion depuis un appareil nouveau.
- Sessions bornées : 12 heures pour la direction, 30 jours pour un salarié, 24 heures sur un appareil partagé ; cookie de session inaccessible aux scripts.
- Fichiers vérifiés à leur dépôt (type reconnu, métadonnées retirées) ; notifications sans contenu lisible par un tiers.
- Journal d'audit en ajout seul ; journal des interventions de Nolia, consultable par le client.
- Administration de la plateforme hors d'internet, depuis le réseau privé de Nolia, par mot de passe puis clé de sécurité ; chaque connexion et chaque geste sont notés au journal.

ANNEXE IV – SOUS-TRAITANTS ULTÉRIEURS

Liste convenue à la date de cette version. Toute modification est annoncée au client 30 jours avant (article 2).

- OVH SAS (OVHcloud), société par actions simplifiée au capital de 50 000 000 €, 2 rue Kellermann, 59100 Roubaix, RCS Lille Métropole 424 761 419. Rôle : hébergement du service (serveur de l'application et de la base de données). Données : toutes celles de l'annexe II. Lieu : France. Garanties : contrat de sous-traitance prévu par les conditions d'OVHcloud (article 28 du RGPD) ; centre de données situé en France.
- Brevo, société par actions simplifiée, 17 rue Salneuve, 75017 Paris, RCS Paris 498 019 298. Rôle : envoi des e-mails du service. Données : adresse e-mail et nom du destinataire ; contenu des e-mails (invitations, codes et avis de connexion, avis de sécurité, confirmations de visa et de contestation avec les heures concernées, notifications sans le texte des messages) ; journaux d'envoi. Lieu : Union européenne. Garanties : accord de traitement des données de Brevo (article 28 du RGPD) ; hébergement dans l'Union européenne.
- Services de notification des navigateurs (Web Push), seulement si un utilisateur active les notifications sur son appareil : celui de son navigateur, selon le cas Google LLC (Chrome, Android), Apple Inc. (Safari, iPhone, iPad), Mozilla Corporation (Firefox) ou Microsoft Corporation (Edge). Rôle : acheminer la notification jusqu'à l'appareil. Données : l'adresse d'abonnement de l'appareil, l'heure et la taille de la notification ; son contenu est chiffré de bout en bout, seul l'appareil le déchiffre, et ne contient ni texte de message ni nom. Lieu : États-Unis. Garanties : décision d'adéquation de la Commission européenne du 10 juillet 2023 (cadre de protection des données UE-États-Unis), pour celles de ces sociétés qui y sont certifiées ; chiffrement de bout en bout ; l'utilisateur peut refuser ou couper les notifications à tout moment et être prévenu par e-mail à la place.

Empreinte SHA-256 du texte : 8255fa8a36e39f804ce44546aefa94ce3c891326cf16dcf912ed0a114f5c2cc3