

# Traitement des données à caractère personnel (DPA)

La présente annexe (« Data Processing Agreement » ou « DPA ») fait partie intégrante du contrat conclu entre le prestataire et le client, et ayant pour objet de définir les conditions applicables aux services fournis. Le DPA et le contrat sont complémentaires et s'expliquent mutuellement. Toutefois, en cas de contradiction, le DPA prévaut.

La finalité du présent DPA conclu conformément à l'article 28 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 (« Règlement général sur la protection des données » ou « RGPD »), est de définir les conditions dans lesquelles le prestataire, en qualité de sous-traitant et dans le cadre des services définis dans le contrat, traite, sur instruction du client, des données à caractère personnel telles que définies dans le RGPD (« Données à caractère personnel »).

## •Note

Le traitement des données à caractère personnel par le prestataire en tant que responsable du traitement n'entre pas dans le champ d'application du présent DPA.

Aux fins du présent DPA, le prestataire agit en tant que « Sous-traitant » et le client est présumé agir en tant que « Responsable du traitement ». Les termes « Sous-traitant » et « Responsable du traitement » ont le sens qui leur est donné au sein du RGPD.

## Client agissant en tant que sous-traitant

Si le client agit en tant que sous-traitant pour le compte d'un tiers responsable du traitement, les parties conviennent expressément que les conditions suivantes s'appliquent :

### Obligations du client

Le client doit s'assurer que :

- Toutes les autorisations nécessaires pour conclure le présent DPA, y compris la nomination par le client du prestataire en tant que sous-traitant ultérieur, ont été obtenues du Responsable du traitement;
- Un contrat, qui est en parfaite adéquation avec les termes et conditions du contrat (y compris le présent DPA), a été conclu avec le Responsable du traitement conformément à l'article 28 du RGPD;
- Toutes les instructions reçues par le prestataire de la part du client en exécution du contrat et du présent DPA sont parfaitement conformes aux instructions du Responsable du traitement;
- Toutes les informations communiquées ou mises à disposition par le prestataire

en vertu du présent DPA sont, lorsque cela est requis, communiquées de manière appropriée au Responsable du traitement.

### Engagements du prestataire

Le prestataire :

- Traite les données à caractère personnel uniquement sur instruction du client ;
- Ne reçoit aucune instruction directement du Responsable du traitement, sauf dans les cas où le client a matériellement disparu ou a cessé d'avoir une existence juridique sans que les droits et obligations du client n'aient été transférés à une entité tierce.

### Responsabilité du client

Le client, qui est entièrement responsable envers le prestataire de la bonne exécution des obligations du Responsable du traitement conformément au présent DPA, indemnise et dégage le prestataire de toute responsabilité pour :

- Tout manquement du Responsable du traitement à se conformer à la loi applicable ;
- Toute action, réclamation ou plainte du Responsable du traitement concernant les dispositions du contrat (y compris le présent DPA) ou concernant les instructions reçues par le prestataire de la part du client.

### Champ d'application

Le prestataire est autorisé, en tant que sous-traitant agissant selon les instructions du client, à traiter les données à caractère personnel du Responsable du traitement dans la mesure nécessaire à la fourniture des services.

La nature des opérations menées par le prestataire concernant les données à caractère personnel peut être le calcul de données, le stockage et/ou tout autre service tel que décrit dans le contrat.

Le type de données à caractère personnel et les catégories de personnes concernées sont déterminés et contrôlés par le client, à sa seule discrétion.

Les activités de traitement sont effectuées par le prestataire pour la durée prévue au contrat.

### Conformité

Chaque partie respecte la réglementation applicable en matière de protection des données, y compris le Règlement Général sur la Protection des Données, à compter de sa date d'application dans l'Union européenne.

### Délégué à la protection des données

Le prestataire a désigné un délégué à la protection des données (DPO) joignable à l'adresse : [dpo@treelogie.com](mailto:dpo@treelogie.com)

Le client peut contacter le DPO pour toute question relative au traitement de ses données à caractère personnel dans le cadre du contrat.

## Obligations du prestataire

Le prestataire s'engage à :

- Traiter les données à caractère personnel téléchargées, stockées et utilisées par le client dans le cadre des services uniquement dans la mesure nécessaire à la fourniture des services tels que définis dans le contrat;
- Ne pas accéder à ou utiliser des données à caractère personnel à d'autres fins que celles nécessaires à l'exécution des services (en particulier dans le cadre de la gestion des incidents);
- Mettre en place les mesures techniques et organisationnelles décrites dans le contrat, afin d'assurer la sécurité des données à caractère personnel dans le cadre du service;
- S'assurer que les employés du prestataire autorisés à traiter les données à caractère personnel dans le cadre du contrat sont soumis à une obligation de confidentialité et reçoivent une formation appropriée concernant la protection des données à caractère personnel;
- Informer le client si, à son avis et compte tenu des informations dont il dispose, une des instructions du client enfreint les dispositions du RGPD ou d'autres dispositions de l'Union européenne ou d'un État membre de l'Union européenne en matière de protection des données personnelles;
- Dans le cas de demandes reçues d'une autorité compétente et relatives aux données à caractère personnel traitées en vertu du contrat, informer le client (à moins que les lois applicables ou l'injonction d'une autorité compétente ne l'interdisent), et limiter la communication des données à ce que l'autorité a expressément demandé.

### •Assistance AIPD

Sur demande écrite du client, le prestataire fournit au client une assistance raisonnable dans la réalisation d'analyses d'impact relatives à la protection des données et la consultation de l'autorité de contrôle compétente, dans la mesure où le client est tenu de le faire en vertu de la loi applicable en matière de protection des données, et si une telle assistance est nécessaire et se rapporte aux traitements de données à caractère personnel opérés par le prestataire en vertu du contrat.

Cette assistance consiste à assurer la transparence des mesures de sécurité mises en œuvre par le prestataire pour ses services.

## Mesures de sécurité techniques et organisationnelles

Le prestataire s'engage à mettre en place les mesures de sécurité techniques et organisationnelles appropriées conformément à l'article 32 du RGPD. Ces mesures comprennent notamment :

- Des mesures de sécurité et notamment d'authentification forte;
- Un système qui isole physiquement et/ou de façon logique les clients les uns des autres;
- Des systèmes de filtrage tels que pare-feu;
- Des processus d'authentification des utilisateurs et des administrateurs, ainsi que des mesures visant à protéger l'accès aux fonctions d'administration;

- Le chiffrement systématique des flux d'échanges lorsque cela est possible ;
- Le chiffrement des données au repos avec des algorithmes reconnus (AES-256 ou équivalent).

Le prestataire s'engage dans une démarche de certification ISO 27001 (Système de management de la sécurité de l'information) et, le cas échéant, HDS (Hébergeur de données de santé). Le détail des mesures techniques est disponible dans le Plan d'Assurance Sécurité (PAS) communiqué sur demande.

### Atteintes à la protection des données à caractère personnel

Si le prestataire a connaissance d'un incident affectant les données à caractère personnel du Responsable du traitement (accès non autorisé, perte, divulgation ou altération de données), le prestataire en informe le client dans un délai maximum de **48 heures** suivant la découverte de l'incident, afin de permettre au client de respecter, le cas échéant, son obligation de notification à l'autorité de contrôle dans le délai de 72 heures prévu à l'article 33 du RGPD.

#### La notification doit :

- Décrire la nature de l'incident ;
- Décrire les conséquences probables de l'incident ;
- Décrire les mesures prises ou proposées par le prestataire en réponse à l'incident ;
- Préciser l'interlocuteur du prestataire.

### Localisation et transfert des données à caractère personnel

Les données à caractère personnel sont hébergées au sein de l'Union européenne ou en Suisse, pays reconnu comme offrant un niveau de protection adéquat par la Commission européenne. La localisation effective est précisée dans les conditions particulières du service ou, à défaut, communiquée sur demande au client. La liste des sous-traitants ultérieurs et leur localisation figure en annexe du présent DPA.

Dans le cas où les données à caractère personnel traitées en vertu des présentes sont transmises hors de l'Union européenne vers un pays qui ne fait pas l'objet d'une décision d'adéquation, un accord de transfert de données conforme aux clauses contractuelles types adoptées par la Commission européenne ou, à la discrétion du prestataire, toute autre mesure de protection reconnue comme suffisante par la Commission européenne est mise en œuvre.

Le Responsable du traitement doit accomplir toutes les formalités et obtenir toutes les autorisations nécessaires (y compris, le cas échéant, auprès des personnes concernées et des autorités compétentes en matière de protection des données) pour transférer des données à caractère personnel dans le cadre du contrat.

### Sous-traitance

Le client autorise expressément le prestataire à engager ses sociétés apparentées en tant que sous-traitants ultérieurs.

Sous réserve des dispositions contraires des conditions de service applicables, le prestataire ne fait pas intervenir sans le consentement préalable du client de sous-traitant ultérieur n'ayant pas la qualité de société apparentée. Lorsque les conditions de ser-

vice applicables prévoient la possibilité d'engager des sous-traitants ultérieurs tiers, la validation de ces conditions de service par le client est considérée comme une approbation des sous-traitants ultérieurs listés.

Le prestataire reste vis-à-vis du client entièrement responsable de l'exécution de toute obligation que le sous-traitant ultérieur ne remplit pas.

#### •Note

Le prestataire est expressément autorisé à engager des fournisseurs tiers (tels que des fournisseurs de matériel et de logiciels, des transporteurs, des fournisseurs techniques, des sociétés de sécurité), sans devoir informer le client ou obtenir son autorisation préalable, à condition que ces fournisseurs tiers n'aient pas accès aux données à caractère personnel.

### Obligations du client et du Responsable du traitement

Pour le traitement des données à caractère personnel conformément au contrat, le client doit fournir au prestataire par écrit :

- Toute instruction pertinente;
- Toute information nécessaire à la création du registre des activités de traitement du sous-traitant.

Le client reste seul responsable du traitement des informations et instructions communiquées au prestataire.

### Responsabilités du Responsable du traitement

Le Responsable du traitement a la responsabilité de s'assurer que :

- Le traitement des données personnelles du Responsable du traitement dans le cadre de l'exécution du service a une base juridique appropriée (par exemple, le consentement de la personne concernée, les intérêts légitimes du Responsable du traitement, etc.);
- Toutes les procédures et formalités requises (telles qu'une analyse d'impact relative à la protection des données, une notification et une demande d'autorisation à l'autorité de contrôle compétente en matière de traitement de données personnelles ou à tout autre organisme compétent, le cas échéant) ont été effectuées;
- La personne concernée est informée du traitement de ses données à caractère personnel de façon concise, transparente, intelligible et facilement accessible, en utilisant un langage clair et simple, comme le prévoit le RGPD;
- Les personnes concernées sont informées et ont à tout moment la possibilité d'exercer facilement les droits relatifs aux données prévus par le RGPD directement auprès du client ou du Responsable du traitement.

Le client est responsable de la mise en œuvre des mesures techniques et organisationnelles appropriées pour assurer la sécurité des ressources, systèmes, applications et opérations qui ne relèvent pas du périmètre de responsabilité du prestataire tel que prévu au contrat (notamment tous les systèmes et logiciels déployés et exploités par le client ou les utilisateurs au sein des services).

## Droits des personnes concernées

Le Responsable du traitement est pleinement responsable de l'information des personnes concernées concernant leurs droits et du respect de ces droits, y compris les droits d'accès, de rectification, d'effacement, de limitation ou de portabilité.

Le prestataire fournit la coopération et l'assistance raisonnablement nécessaire pour répondre aux demandes des personnes concernées. Cette assistance raisonnable comprend la mise à disposition des informations techniques nécessaires et la réalisation d'opérations d'extraction ou de suppression de données dans la limite de **2 heures** de prestation par demande. Au-delà, l'assistance pourra faire l'objet d'une facturation selon les tarifs en vigueur, après accord préalable du client.

**Cette coopération et cette assistance raisonnable peuvent consister à :**

- Communiquer au client toute demande reçue directement de la personne concernée;
- Permettre au Responsable du traitement de concevoir et de déployer les mesures techniques et organisationnelles nécessaires pour répondre aux demandes des personnes concernées.

Le Responsable du traitement est seul responsable des réponses à ces demandes.

### •Attention

Le client reconnaît et convient que, dans l'éventualité où une telle coopération et assistance nécessiterait des ressources importantes de la part du prestataire, cela pourra être facturé au client à condition de le lui notifier et d'obtenir son accord au préalable.

## Restitution et suppression des données à caractère personnel

À la fin du service (notamment en cas de résiliation ou de non-renouvellement), le prestataire s'engage à :

### Restitution

Le prestataire fournit au client une archive contenant :

- Les bases de données;
- Les fichiers utilisateurs.

Cette archive est mise à disposition dans un format standard et exploitable, dans un délai de **quinze (15) jours** suivant la date effective de fin du contrat, sauf accord différent entre les parties.

### •Note

Toute prestation de réversibilité au-delà de cette archive standard (migration vers un autre prestataire, conversion de formats, extraction de données spécifiques, etc.) peut donner lieu à facturation selon les conditions de services complémentaires en vigueur.

## Suppression

À l'issue d'un délai de **trente (30) jours** suivant la mise à disposition de l'archive, ou plus tôt sur confirmation écrite du client, le prestataire procède à la suppression définitive de l'ensemble des contenus du client par effacement cryptographique (destruction des clés de chiffrement), sauf si une obligation légale ou une demande émise par une autorité judiciaire compétente impose leur conservation.

### •Attention

Le client est responsable de télécharger l'archive et de vérifier son intégrité dans le délai imparti. Passé ce délai, les données sont supprimées de manière irréversible, y compris les documents transmis par le client au prestataire dans le cadre de la prestation (spécifications, fichiers sources, etc.).

## Responsabilité et audit

Le prestataire met à la disposition du client toutes les informations nécessaires pour :

- Démontrer la conformité aux exigences du RGPD;
- Mener des audits.

Des informations supplémentaires peuvent être communiquées au client sur demande faite au support.

Si les informations et les rapports s'avèrent insuffisants pour permettre au client de démontrer que les obligations prévues par le RGPD sont remplies, le prestataire et le client se réunissent alors pour convenir des conditions opérationnelles, sécuritaires et financières d'une inspection technique.

### •Note

En toutes hypothèses, les conditions de cette inspection ne doivent pas affecter la sécurité des autres clients du prestataire.

L'inspection susmentionnée, ainsi que la communication des rapports peuvent donner lieu à une facturation supplémentaire raisonnable.

Toute information communiquée au client en vertu de la présente clause et qui n'est pas disponible publiquement est considérée comme une information confidentielle du prestataire en vertu du contrat. Avant de communiquer ces informations, le prestataire peut exiger la signature d'un accord de confidentialité spécifique.

### •Demandes de l'autorité de contrôle

Le client est autorisé à répondre aux demandes de l'autorité de contrôle compétente à condition que toute divulgation d'informations soit strictement limitée à ce qui est demandé par ladite autorité.

Dans un tel cas, et à moins que la loi applicable ne l'interdise, le client doit d'abord consulter le prestataire au sujet de toute divulgation requise.

## Annexe : Liste des sous-traitants ultérieurs

Conformément à l'article 28.2 du RGPD, le prestataire communique au client la liste des sous-traitants ultérieurs autorisés à traiter des données à caractère personnel dans le cadre des services.

Sous-traitant	Activité	Localisation	Décision d'adéquation
OVHcloud	Hébergement infrastructure	France (UE)	N/A (UE)
Scaleway	Hébergement infrastructure	France (UE)	N/A (UE)
Infomaniak	Hébergement infrastructure	Suisse	Oui (décision 2000/518/CE)
Treelogie	Services support groupe	France (UE)	N/A (UE)
Gestionnaire de secrets	Stockage sécurisé de secrets	Canada / États-Unis	Non (voir ci-dessous)

### •Note

Le sous-traitant ultérieur effectivement utilisé pour un service donné est précisé dans les conditions particulières. Le prestataire informe le client **avec un préavis minimal de trente (30) jours** de tout changement prévu concernant l'ajout ou le remplacement de sous-traitants ultérieurs, donnant ainsi au client la possibilité d'émettre des objections à l'encontre de ces changements conformément à l'article 28.2 du RGPD.

### Sous-traitants soumis à des législations extra-européennes

Conformément à l'article 48 du RGPD, le prestataire porte à la connaissance du client les informations suivantes relatives aux sous-traitants soumis à des législations extra-européennes.

#### Réglementations applicables

Le prestataire utilise, dans le cadre de la fourniture des services, des sous-traitants dont le siège social est situé en Amérique du Nord et qui sont soumis au **Cloud Act** (18 U.S.C. § 2713). Cette législation permet aux autorités américaines de requérir la communication de données stockées par des fournisseurs de services de communication électronique, y compris lorsque ces données sont hébergées hors des États-Unis.

Les sous-traitants concernés sont :

- Un **gestionnaire de secrets** (chiffrement et stockage sécurisé d'identifiants), basé au Canada et aux États-Unis;
- Un **fournisseur de gestion des identités (IAM)**, basé aux États-Unis, utilisé exclusivement pour les identités internes du prestataire.

L'identité précise de ces sous-traitants est communiquée au client sur demande adressée au DPO (dpo@treelogie.com).

#### Mesures d'atténuation

Le prestataire met en œuvre les mesures techniques suivantes pour réduire le risque d'accès non autorisé :

- **Gestionnaire de secrets** : chiffrement de bout en bout avec clé secrète détenue exclusivement par le prestataire. Le fournisseur ne dispose d'aucune capacité technique de déchiffrement des coffres, y compris en cas de réquisition judiciaire;
- **Fournisseur IAM** : usage strictement limité à la gestion des identités internes du prestataire. Aucune donnée à caractère personnel du client n'est traitée par ce service.

#### Risques résiduels

Après application des mesures d'atténuation, le risque résiduel d'accès aux données du client par des autorités étrangères est évalué comme suit :

- **Vraisemblance** : très improbable;
- **Conséquence** : élevée;
- **Niveau de risque** : acceptable.

Cette évaluation est documentée dans le registre des risques du prestataire (réf. R.24) et fait l'objet d'une réévaluation annuelle. Le détail de l'analyse est communiqué au client sur demande.

Dernière mise à jour : avril 2026