

ANNEXE RELATIVE AU TRAITEMENT DES DONNÉES D'INFOMANIAK

ou

"DPA"

L'annexe relative au Traitement des Données (ci-après désigné "DPA"), fait partie intégrante des Conditions Générales d'Utilisation (ci-après désignées "CGU") conclues entre Infomaniak SA (ci-après désignée "Infomaniak") et toute personne physique ou morale de droit privé ou de droit public ayant un compte client auprès d'Infomaniak (ci-après nommée "Client").

Le but du présent accord conclu entre Infomaniak et le Client, 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 ci-après désigné "RGPD"), est de définir les conditions dans lesquelles Infomaniak a le droit, en tant que sous-traitant et dans le cadre des services définis dans le contrat, de traiter, sur instruction du Client, des données à caractère personnel telles que définies dans le RGPD.

Le traitement des données à caractère personnel par Infomaniak en tant que responsable du traitement n'entre pas dans le cadre du présent contrat.

1. Traitement

La nature des opérations menées par Infomaniak concernant les données à caractère personnel peut par exemple être le calcul de données, le stockage et/ou tout autre service correspondant aux prestations de service proposé par Infomaniak.

Le Client désigne Infomaniak en tant que sous-traitant pour traiter les données à caractère personnel du Client. Infomaniak est autorisée, 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.

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

infomaniak Annexe relative au traitement des données d'Infomaniak

La durée du traitement correspond à la durée du service. La finalité et l'objet du traitement sont la fourniture du service tel que décrit dans nos conditions générales et particulières.

Le Client est le seul responsable de la légalité du traitement des données à caractère personnel. Il n'utilisera pas les services de pair avec des données à caractère personnel si une telle utilisation avait pour effet de violer les Lois sur la protection des données applicables.

Le Client doit s'assurer que les services choisis ont les caractéristiques et les conditions requises pour se conformer aux activités et aux objectifs de traitement du responsable de traitement. Il s'assure aussi du type de données à caractère personnel à traiter dans le cadre des services, y compris, mais sans s'y limiter, lorsque les services sont utilisés pour traiter des données à caractère personnel soumises à des réglementations ou des normes spécifiques (par exemple, liées à la législation d'un pays, aux réglementations des données relatives à la santé ou à la réglementation sur les données bancaires).

Si le traitement effectué par le responsable du traitement est susceptible d'entraîner un risque élevé pour les droits et libertés des personnes physiques, le Client doit choisir ses services avec précaution.

Dans le cas où le Client agit en tant que sous-traitant pour le compte d'un tiers responsable du traitement, le Client s'engage à :

- s'assurer que toutes les autorisations nécessaires pour conclure le présent DPA, y compris la nomination par le client d'Infomaniak en tant que sous-traitant, ont été obtenues du responsable du traitement avant de fournir leurs données à caractère personnel.
- d'établir un contrat conforme aux termes et conditions incluant le présent DPA, entre le Responsable du traitement et le client conformément à l'article 28 du RGPD.

2. Conformité à la réglementation applicable

Chaque partie respecte la réglementation applicable en matière de protection des données, y compris le Règlement Général sur la Protection des Données (RGPD).

3. Obligations d'Infomaniak

Infomaniak s'engage à mettre en place les mesures organisationnelles et de sécurité technique suivante :

infomaniak Annexe relative au traitement des données d'Infomaniak

- a) Ne jamais transférer vos données en dehors de nos propres infrastructures.
- b) Mettre en œuvre des standards de sécurité élevés, et maintenir des processus d'amélioration continue afin de vous fournir un haut niveau de sécurité dans le cadre de nos services.
- c) Maintenir et développer nos mesures de sécurité physique afin d'empêcher l'accès aux infrastructures sur lesquelles sont stockées vos données par des personnes non autorisées.
- d) Avoir des systèmes d'isolation physique et/ou logique (en fonction des services) afin d'isoler les hébergements des clients entre eux, et réaliser une fois par année des tests d'intrusion dans le but de s'assurer de l'étanchéité des données entre les clients.
- e) Être exemplaire en termes de réactivité dans les mises à jour de sécurité sur les systèmes dont nous avons la gestion.
- f) Garantir des mesures de sécurité physiques destinées à empêcher les personnes non autorisées d'accéder aux infrastructures dans lesquelles les données du client sont stockées.
- g) Procéder à des contrôles d'identité et d'accès au moyen d'un système d'authentification et d'une politique en matière de mots de passe.
- h) Système de gestion des accès qui limite l'accès aux locaux, aux personnes ayant besoin d'y accéder dans l'exercice de leurs fonctions et dans le cadre de leurs responsabilités.
- i) Protéger l'accès aux fonctions d'administration par des processus d'authentification des utilisateurs et des administrateurs.
- j) Appliquer un système de gestion de l'accès pour les opérations de soutien et d'entretien qui fonctionne selon les principes du moindre privilège et du besoin de savoir.

Infomaniak s'engage de plus à :

- a) Traiter les données à caractère personnel téléchargées, stockées et utilisées par le Client uniquement à la fourniture des services tels que définis dans le Contrat.
- b) Ne pas accéder 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).
- c) Mettre en place les mesures techniques et organisationnelles, afin d'assurer la sécurité des données à caractère personnel dans le cadre de ces services.

infomaniak Annexe relative au traitement des données d'Infomaniak

d) S'assurer que les employés d'Infomaniak 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.

e) Informer le Client si, à son avis et compte tenu des informations dont il dispose Infomaniak constaterait qu'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.

f) Dans le cas de demandes reçues d'une autorité compétente et relatives aux données à caractère personnel traitées en vertu du présent contrat, à informer le Client (à moins que les lois applicables ou l'injonction d'une autorité compétente ne l'interdisent), et à limiter la communication des données à ce que l'autorité a expressément demandé.

4. Violation de données à caractère personnel

Infomaniak s'engage à notifier au Client toute violation de données à caractère personnel dans le cadre des services dans les meilleurs délais après en avoir pris connaissance. Infomaniak s'engage à enquêter rapidement sur une telle violation de données à caractère personnel du Client si elle a été constatée sur l'infrastructure d'Infomaniak ou dans une zone dont Infomaniak est responsable, et à assister le Client comme indiqué dans l'article 5.

5. Assistance

Infomaniak s'engage à aider le Client, dans la mesure du possible, par des mesures techniques et organisationnelles, pour que le Client se conforme à ses obligations vis-à-vis des droits des personnes concernées, et pour qu'il s'assure de sa conformité à la sécurité du traitement, à son obligation de notifier une violation de données à caractère personnel et à son obligation de procéder à une analyse d'impact relative à la protection des données, compte tenu des informations à la disposition d'Infomaniak.

Le Client soumettra une demande écrite pour toute aide mentionnée dans le présent DPA. Infomaniak facturera au Client un prix raisonnable pour ladite aide ou pour les Instructions supplémentaires, ce prix devant soit donner lieu à un devis approuvé par les parties, soit être traité dans le cadre de la procédure de gestion des changements définie dans le Contrat.

6. Sous-traitants ultérieurs

Le Client autorise Infomaniak à faire appel à des sous-traitants pour traiter ses données à caractère personnel (« sous- traitants ultérieurs »). Les sous-traitants ultérieurs peuvent être engagés

infomaniak Annexe relative au traitement des données d'Infomaniak

uniquement dans le cadre de l'exécution des services s'ils figurent dans les conditions particulières des services qui pourraient être concernées.

En cas de changement ou d'ajout d'un sous-traitant extérieur, Infomaniak informera le Client par avance des changements de sous-traitants. Le Client dispose d'un délai de 30 jours à compter de cette information pour émettre une objection à l'encontre de ces changements qui le placeraient en situation de violation de ses obligations légales applicables. L'objection du Client doit être formulée par écrit et doit inclure ses motifs spécifiques et les alternatives proposées, le cas échéant. Si le Client n'émet pas d'objections dans ledit délai, le sous-traitant ultérieur concerné peut être chargé de traiter les données à caractère personnel du Client.

Infomaniak veille à ce que le sous-traitant ultérieur soit, au minimum, en mesure de remplir les obligations mises à la charge d'Infomaniak dans le présent DPA concernant le traitement des données à caractère personnel. À cette fin, Infomaniak conclut un accord avec le sous-traitant ultérieur. Infomaniak reste vis-à-vis du Client entièrement responsable de l'exécution de toute obligation que le sous-traitant ultérieur ne remplit pas.

7. Obligations du Client et du responsable du traitement

Le Client peut fournir des instructions supplémentaires qui sont légalement requises. Si Infomaniak pense qu'une instruction supplémentaire a pour effet de violer le RGPD ou d'autres règlements de protection des données applicables, elle en avisera le Client dans les meilleurs délais et pourra suspendre la prestation du service jusqu'à ce que le Client ait modifié l'instruction supplémentaire ou qu'il en ait confirmé la légalité par écrit. Si Infomaniak avise le Client qu'il n'est pas possible de mettre en œuvre une instruction supplémentaire, ou si le Client avise Infomaniak qu'il n'accepte pas la proposition de prix pour l'instruction supplémentaire, le Client peut résilier le service visé en fournissant à Infomaniak un préavis écrit dans le mois qui suit la réception de l'avis d'Infomaniak. En cas de besoin, Infomaniak remboursera au prorata les frais prépayés pour la période qui suit la date de résiliation des services. Le Client reste seul responsable du traitement des informations et instructions communiquées à Infomaniak.

8. Restitution ou suppression des données à caractère personnel du Client

À la fin du service (notamment en cas de non-renouvellement ou résiliation), Infomaniak s'engage à supprimer aux termes du Contrat et dans les conditions prévues, tout contenu (y compris les informations, données, fichiers, systèmes, applications, sites Web et autres éléments) qui est reproduit, stocké, hébergé ou autrement utilisé par le Client dans le cadre des services, sauf demande d'une autorité légale ou judiciaire compétente, ou si la législation applicable de l'Union européenne ou d'un État membre de l'Union européenne l'exige autrement.

infomaniak Annexe relative au traitement des données d'Infomaniak

Le Client est seul responsable de s'assurer que les opérations nécessaires (telles que la sauvegarde, le transfert à une solution tierce, les snapshots, etc) à la conservation des données personnelles à caractère personnel sont effectuées, en particulier avant la résiliation ou l'expiration des services, et avant de procéder à toute opération de suppression, de mise à jour ou de réinstallation des services.

A cet égard, le Client est informé que la résiliation et l'expiration d'un service pour quelque raison que ce soit (y compris, mais sans s'y limiter, le non-renouvellement), ainsi que certaines opérations de mise à jour peuvent automatiquement entraîner la suppression irréversible de tout contenu (y compris les informations, données, fichiers, systèmes, applications, sites Web et autres éléments) qui est reproduit, stocké, hébergé ou autrement utilisé par le Client dans le cadre des services, y compris toute sauvegarde potentielle.

9. Responsabilité

Infomaniak ne peut être tenu responsable que des dommages causés par un traitement pour lequel (i) il n'a pas respecté les obligations du RGPD concernant spécifiquement les sous-traitants en charge des données ou pour lequel, (ii) il a agi contrairement aux instructions écrites légales du Client. Dans de tels cas, la disposition du Contrat relative à la responsabilité s'applique.

Lorsqu'Infomaniak et le Client sont impliqués dans un traitement dans le cadre du présent Contrat qui a causé un dommage à la personne concernée, le Client prend en charge, dans un premier temps, l'indemnisation intégrale (ou toute autre compensation) due à la personne concernée et, dans un second temps, réclame à Infomaniak la partie de l'indemnisation de la personne concernée correspondant à la partie de la responsabilité d'Infomaniak dans le dommage, à condition cependant que les clauses limitatives de responsabilité prévues par le Contrat soient appliquées.

10. Audits

Infomaniak a le droit de répondre aux demandes de l'autorité de surveillance compétente à condition que toute divulgation d'informations soit strictement limitée à ce qui est demandé par ladite autorité de surveillance. Dans ce cas, et sauf interdiction légale, Infomaniak doit d'abord consulter le client au sujet de toute divulgation requise.

Infomaniak fournit au Client toutes les informations nécessaires pour permettre au Client ou à d'autres auditeurs de réaliser des audits pour prouver la conformité aux exigences de la RGPD.

infomaniak Annexe relative au traitement des données d'Infomaniak

Ces informations sont disponibles dans la documentation standard sur le site Web d'Infomaniak. Des informations supplémentaires peuvent être communiquées au Client sur demande adressée à l'équipe support d'Infomaniak.

Si un service est agréé et qu'il respecte un code de conduite précis ou qu'il fait l'objet de certifications ou procédures de contrôle spécifiques, Infomaniak met à disposition, sur demande écrite du Client, les certificats de contrôle et rapports correspondants.

Si les informations, le rapport et le certificat mentionnés ci-dessus s'avèrent insuffisants pour permettre au Client de démontrer que les obligations prévues par le DGPS sont remplies, Infomaniak et le Client se rencontreront pour convenir des conditions opérationnelles, sécuritaires et financières d'une inspection technique sur site. Dans tous les cas, les conditions de cette inspection ne doivent pas affecter la sécurité des autres clients d'Infomaniak.

L'inspection sur place mentionnée ci-dessus, ainsi que la fourniture de certificats et de rapports des contrôles peuvent entraîner des frais supplémentaires raisonnables. Toute information communiquée au Client en vertu de cette clause et qui n'est pas disponible sur le site d'Infomaniak est considérée comme une information confidentielle d'Infomaniak dans le cadre du Contrat. Avant de communiquer ces informations, Infomaniak peut exiger la signature d'un accord de confidentialité spécifique.

Révision du 20/06/2018