OVH
ET LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

OVH
Innovation is Freedom

Créé en 1999, OVH est aujourd'hui l'un des acteurs majeurs du cloud avec une présence dans 18 pays dans le monde. La satisfaction de nos plus d'un million de clients et la sécurité de leurs données personnelles nous tiennent particulièrement à cœur.

Lorsque vous choisissez d'externaliser tout ou partie de l'hébergement de vos données auprès d'OVH, vous nous confiez une part de votre patrimoine informationnel. Nous sommes conscients des enjeux que cela peut représenter pour votre organisation, notamment en matière de conformité réglementaire. C'est pourquoi nous mettons à votre disposition l'information la plus complète possible, à propos des enjeux en matière de protection des données à caractère personnel.

1 DE L'IMPORTANCE DU CHOIX DE SON FOURNISSEUR DE CLOUD

1.1. Un critère de conformité

La sélection d'un fournisseur de solutions cloud ne peut pas répondre uniquement à des enjeux techniques. L'émergence de réglementations de plus en plus contraignantes, à l'instar du règlement européen 2016/679 dit règlement général sur la protection des données (RGPD), ainsi que la prise de conscience des enjeux éthiques et économiques liés à la localisation des données d'une entité, poussent chaque acteur à voir au-delà des capacités technologiques. En plus de proposer des services performants et sécurisés, OVH s'engage à ce que ces solutions soient conformes et transparentes dans leur fonctionnement.

Cette détermination est cruciale pour l'ensemble des entités souhaitant externaliser leur système d'information : leur propre conformité est conditionnée par celle de leur sous-traitant. C'est donc en partie grâce aux engagements fournis par OVH que vous serez en mesure de respecter vos propres obligations réglementaires. Cette exigence est notamment présente au sein de l'article 28 du RGPD, indiquant qu'un « *responsable de traitement* » doit uniquement faire « *appel à des sous-traitants qui présentent 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 présent règlement*[1] ».

La Commission nationale de l'informatique et des libertés (CNIL), autorité française chargée de veiller au respect des dispositions relatives à la protection des données personnelles, recommande d'ailleurs « *qu'une entreprise [...] qui envisage de recourir à un service de* **cloud computing** *réalise une analyse de risques et soit très rigoureuse dans le choix de son prestataire. En particulier, l'entreprise devra prendre en considération les garanties offertes par un prestataire en matière de protection des données personnelles et s'assurer que ce dernier lui fournira toutes les garanties nécessaires au respect de ses obligations au regard de la loi*[2] ».

1.2. Un critère d'intelligence économique

OVH est un *pure player* exerçant une activité unique : la fourniture d'infrastructures IT et, en particulier, de cloud. Nous n'avons pas, directement ou à travers d'autres entités ou filiales, d'activités concurrentes à celles de nos clients, qu'il s'agisse de vente en ligne ou d'édition de logiciels. En effet, nous estimons dommageable que des organisations financent, à travers leur fournisseur de cloud, une entreprise rivale en raison de la diversification de ses activités.

[1] 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 : http://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A32016R0679

[2] CNIL, Recommandations pour les entreprises qui envisagent de souscrire à des services de Cloud computing : https://www.cnil.fr/sites/default/files/typo/document/Recommandations_pour_les_entreprises_qui_envisagent_de_souscrire_a_des_services_de_Cloud.pdf

2 LES ENGAGEMENTS D'OVH, EN SA QUALITÉ DE SOUS-TRAITANT, CONCERNANT LE TRAITEMENT DES DONNÉES PERSONNELLES

OVH est qualifié de « *sous-traitant* » lorsqu'il traite des données à caractère personnel pour le compte d'un responsable. C'est typiquement le cas lorsque vous stockez des informations à caractère personnel sur nos infrastructures.

Engagement n° 1 : la non-réutilisation des données hébergées sur nos services

OVH s'engage à traiter les données à caractère personnel du client aux seules fins de la bonne exécution des services et selon ses seules instructions.

Les informations hébergées dans le cadre de nos services restent la propriété du client.

Nous nous interdisons toute revente desdites données, de même que toute utilisation à des fins commerciales (telles des activités de profilage ou de marketing direct).

Engagement n° 2 : permettre la réversibilité de vos données

« *Donner ses données, reprendre c'est possible.* »

La réversibilité des informations – c'est-à-dire le fait de pouvoir migrer ou rapatrier ses données sous un format standard – n'est pas possible avec toutes les offres cloud du marché. Du moins, elle peut être rendue complexe par l'existence de verrous technologiques. Or, le cloud est devenu un sujet stratégique pour les entreprises. Trop stratégique pour prendre des risques ou s'engager à vie avec un opérateur. Défendre un cloud ouvert, c'est empêcher un acteur dominant d'imposer ses règles simplement parce qu'il contrôle une partie du secteur.

Chez OVH, 100 % de nos solutions de cloud sont basées sur des standards, dont un certain nombre de technologies *open source*. Vous pouvez donc récupérer vos données facilement : la réversibilité et l'interopérabilité sont toujours possibles.

Engagement n °3 : savoir précisément où sont stockées et traitées vos données

Lorsque vous sélectionnez un service permettant de stocker du contenu et, notamment, des données à caractère personnel, la localisation ou la zone géographique du ou des datacenters est précisée sur notre site internet. Et si plusieurs localisations ou zones géographiques sont disponibles, vous pouvez même opter pour celle de votre choix au moment de la commande.

Le « *stockage des données* » n'est cependant pas synonyme de « *traitement des données* ». Le RGPD fixe en effet des règles applicables en matière de « *traitement* » et non de simple « *stockage* ». Il convient donc d'être particulièrement attentif lors de l'utilisation de ces deux termes.

Lorsque vous sélectionnez une zone de stockage située dans l'Union européenne, OVH vous garantit qu'il ne traite pas vos informations en dehors de l'Union européenne ou de tout pays reconnu par la Commission européenne comme disposant d'un niveau de protection des données à caractère personnel suffisant (au regard de la protection de la vie privée, des libertés et droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants [décision d'adéquation]). De plus, nous nous engageons à ne jamais traiter vos données aux États-Unis.

Engagement n° 4 : garantir une transparence totale en matière de recours à des sous-traitants

OVH maîtrise toute la chaîne de l'hébergement, de la création des serveurs à la gestion des datacenters. À l'exception de nos sociétés apparentées, et sauf stipulations spécifiques au sein des conditions particulières d'un service, aucune autre entreprise n'est amenée à pouvoir visualiser ou accéder aux données de nos clients.

La liste des sociétés apparentées d'OVH est disponible sur notre site internet ou sur simple demande auprès de notre équipe Support. Il s'agit essentiellement des filiales du groupe implantées à l'international : OVH Allemagne, OVH Espagne, etc.

Dans notre volonté de protéger au maximum les données de nos clients, OVH US n'est pas considéré comme une société apparentée. Notre entité américaine est strictement séparée de ses homologues européennes. Tout ajout de société apparentée fait également l'objet d'un délai de prévenance de 30 jours préalablement à son recours.

Enfin, si OVH était amené dans le futur à sous-traiter des activités impliquant une visualisation ou un accès à des données, cette démarche serait conditionnée à l'accord de nos clients.

Engagement n° 5 : vous informer en cas de violation de données

OVH met en œuvre d'importantes mesures en matière de sécurité. Nous anticipons aussi tous les scénarios, y compris ceux incluant une violation d'informations.

Dans cette éventualité, nous nous engageons à informer les clients concernés dans les meilleurs délais. Cette notification précisera la nature de l'incident, ses conséquences prévisibles, ainsi que les mesures prises pour résoudre ou minimiser la violation..

Engagement n° 6 : fournir une documentation complète sur nos services

Il est essentiel que votre prestataire de cloud présente des garanties appropriées, eu égard à la criticité des traitements de vos informations. C'est l'un des critères permettant d'assurer votre conformité face aux réglementations relatives à la protection des données personnelles.

Afin d'être en mesure de réaliser un tel choix, puis de pouvoir le justifier auprès des autorités de contrôle, vous devez disposer d'une documentation complète sur les services offerts par vos sous-traitants. C'est pourquoi OVH s'engage à vous communiquer l'ensemble des pièces adéquates : description des mesures de sécurité mises en œuvre sur vos services, attestation de localisation du stockage des données, etc.

Engagement n° 7 : vous garantir contractuellement nos engagements

Les engagements d'OVH ne sont pas de belles promesses : ils sont intégrés contractuellement à notre Data Processing Agreement (DPA). Ce document prend la forme d'une annexe à nos contrats. Il est disponible sur simple demande pour tous nos clients.

3 LES ENGAGEMENTS D'OVH EN MATIÈRE DE SÉCURITÉ

OVH prend toutes les précautions afin de préserver la sécurité et la confidentialité des données à caractère personnel traitées. Notre objectif est notamment d'empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés y aient accès.

3.1. Répartition des actions de sécurité à mettre en œuvre

Il est essentiel de faire la distinction entre la sécurité des données hébergées par le client et la sécurité des infrastructures sur lesquelles ces informations sont stockées.

- Sécurité des données hébergées : le client est seul responsable de la sécurisation des ressources et des systèmes applicatifs qu'il déploie, dans le cadre de l'utilisation de nos services. Des outils sont toutefois mis à disposition par OVH afin de l'accompagner dans la sécurisation de ses données.
- Sécurité des infrastructures : OVH s'engage à sécuriser ses infrastructures de façon optimale. Nous avons notamment mis en place une politique de sécurité des systèmes d'information (PSSI) et nous répondons aux exigences de plusieurs normes et certifications : certification PCI-DSS, certification ISO/IEC 27001, attestations SOC 1 type 2 et SOC 2 type 2, etc. Nous disposons aussi d'un agrément pour l'hébergement de données de santé (HDS) pour notre offre Healthcare.

3.2. Les mesures de sécurité garanties par OVH

Nos mesures de sécurité garanties dépendent des services souscrits. Pour chacun d'eux, nous nous engageons à fournir l'ensemble de la documentation idoine. Cela permet à nos clients de déterminer si une solution est adaptée aux traitements de données personnelles qu'il met en œuvre.

Pour l'ensemble de ses services, OVH s'engage à mettre en place :

- des mesures de sécurité physique afin d'empêcher l'accès aux infrastructures par des personnes non autorisées ;
- un personnel de sécurité chargé de veiller à la sécurité physique de nos locaux 24 heures sur 24 et 7 jours sur 7 ;
- un système de gestion des permissions permettant de limiter l'accès aux locaux et aux données aux seules personnes habilitées, dans le cadre de leurs fonctions et de leurs périmètres d'activité ;
- un système d'isolation physique et/ou logique (selon les services) des clients entre eux ;
- des processus d'authentification forts des utilisateurs et administrateurs grâce, notamment, à une politique stricte de gestion des mots de passe et au déploiement de certaines mesures de double authentification comme YubiKey ;
- des processus et dispositifs permettant de tracer l'ensemble des actions réalisées sur notre système d'information et d'effectuer, conformément à la réglementation en vigueur, des rapports en cas d'incident affectant les données de nos clients.

WWW.OVH.COM