REGLES INTERNES AU TRANSFERT DE DONNEES A CARACTERE PERSONNEL

L'important développement à l'international du groupe OVH et de ses filiales, conduit à l'adoption des présentes règles internes en matière de transfert de données à caractère personnel, dans la mesure où le groupe OVH est amené à proposer ses services dans plus en plus de pays, y compris hors Union Européenne.

De même ses clients souhaitent bénéficier d'un accès à leurs services dans les plages horaires de plus en plus larges.

L'ensemble de ces éléments a conduit à l'organisation de la société avec une présence physique dans différents états et à ce qu'une partie des services d'assistance et de maintenance soit opérée par des filiales étrangères du groupe OVH, telles que visées en annexe 8.

La société OVH SAS se porte fort du respect par l'ensemble de ses filiales visées en annexe 8 des présentes règles internes. Les filiales concernées remettent par écrit à la société OVH un engagement unilatéral par lequel elles s'engagent à respecter les présentes règles internes.

Le président de la société OVH SAS a également pris l'engagement, d'assurer le respect des règles décrites dans le présent document.

Les présentes règles internes sont également rendues contraignantes à l'ensemble des salariés du groupe OVH du fait de leur insertion dans le règlement intérieur. En cas de violation des présentes règles, les sanctions prévues dans le règlement intérieur s'appliqueront.

L'objectif des présentes règles internes est de fournir une protection adéquate pour les transferts et le traitement automatique ou manuel des données personnelles effectués par les différentes filiales françaises du groupe.

Elles se basent sur les directives européennes 95/46/CE et 2002/58/CE, relatives à la protection des données personnelles et ont pour objectif de mettre les pratiques du groupe OVH en matière de protection des données personnelles en conformité avec lesdites directives.

ARTICLE 1 CHAMP D'APPLICATION

Les présentes règles internes s'appliquent à l'ensemble des transferts et traitements automatiques ou manuels mis en œuvre au sein du groupe, depuis la France vers des pays tiers, sur toutes les données traitées relatives aux clients du groupe OVH.

Les données clients visées par les présentes règles internes correspondent à l'ensemble des données visées en annexe 1, traitées à des fins de gestion de la relation client au sein du groupe OVH et de conformité au regard des obligations légales et règlementaires liant la société OVH SAS..

Les données visées par ces présentes règles internes constituent des données relatives à l'identification du client, au mode de paiement, aux données de connexion du client au compte utilisateur, ses services, la gestion de son compte et de ses services,…

Il relève de la responsabilité des employés du groupe OVH de veiller au bon respect de ces règles. Ceux-ci y sont tenus en application du règlement intérieur de la société OVH SAS et de ses filiales.

ARTICLE 2 DEFINITIONS

Clients ou personnes concernées : Toute personne physique ou morale, signataire des conditions contractuelles générales et particulières d'OVH pour tout service souscrit auprès de la société OVH. Le Client garantit être habilité aux fins des présentes.

Service: Service devant être fourni par OVH conformément aux dispositions du bon de commande.

Utilisateurs : Utilisateur habilité par le Client, utilisant le Service. Selon les Services, les utilisateurs peuvent être multiples.

Filiale : Société appartenant au groupe OVH et détenue à majoritairement par la société OVH.

Exportateur de données : Il s'agit de la société OVH située en France.

Importateur de données : Toute société du groupe OVH située hors Union Européenne, accédant à la base de données clients du groupe OVH.

Données à caractère personnel : Toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres

Traitement de données à caractère personnel : Toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé et, notamment, la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

Fichier de données à caractère personnel : Tout ensemble structuré et stable de données à caractère personnel accessibles selon des critères déterminés.

Responsable du traitement : Entité déterminant les finalités et les moyens du traitement.

Destinataire du traitement : Toute personne habilitée à recevoir communication des données à caractère personnel traitées, autre que la personne concernée, le responsable du traitement, le sous-traitant et les personnes qui, en raison de leur fonction, sont chargées de traiter les données.

Données sensibles : Données à caractère personnel faisant apparaître, directement ou indirectement, les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses ou l'appartenance syndicale des personnes ou qui sont relatives à la santé ou à la vie sexuelle de celles-ci.

Les termes ainsi définis doivent être interprétés conformément aux directives européennes 95/46/CE et 2002/58/CE.

ARTICLE 3 LIMITATION DES FINALITES

Les traitements visés par les présentes règles internes, de même que les transferts de données mis en place, sont effectués dans le cadre des finalités visées en annexe 9 des présentes.

Les données personnelles sont transférées et traitées dans le cadre exclusif de ces finalités légitimes.

Les données personnelles ne doivent subir aucun traitement ultérieur incompatible avec ces finalités.

ARTICLE 4 QUALITE DES DONNEES ET PROPORTIONNALITE

Les données personnelles doivent être exactes et, au besoin, mises à jour.

Elles doivent, en outre, être adéquates et pertinentes et leur volume ne doit pas être excessif au regard de la finalité pour laquelle elles sont transférées et traitées.

Le traitement de ces données personnelles ne doit, en aucun cas, être effectué plus longtemps que nécessaire au regard de la finalité précitée de gestion de la relation client.

Le détail des données est précisé en annexe 1.

ARTICLE 5 BASE JURIDIQUE DU TRAITEMENT DES DONNEES A CARACTERE PERSONNEL

L'ensemble des données personnelles n'est traité qu'avec l'accord explicite du client ou, éventuellement, sans son accord explicite lorsque le traitement mis en œuvre est indispensable à l'exécution d'un contrat que la personne concernée a conclu avec le groupe OVH ou ses filiales.

La conservation des données de connexion du compte client est inscrite dans le cadre de l'obligation légale de tout opérateur de services de communication électronique.

L'ensemble des données collectées proviennent directement du client ou de l'utilisateur du service du client.

ARTICLE 6 DONNEES SENSIBLES

Aucune donnée sensible n'est traitée, mais il sera rappelé qu'aucune donnée sensible ne peut être traitée sans le consentement explicite de la personne concernée ou lorsque ces données ont manifestement été rendues publiques par la personne concernée ou encore, lorsque le traitement de ces données est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice.

ARTICLE 7 TRANSPARENCE ET DROIT A INFORMATION

Les présentes règles internes sont rendues accessibles à toute personne concernée, dans le cadre de l'article relatif aux données personnelles du contrat liant le client à la société OVH, ainsi que dans le cadre de la Charte déontologique proposée par OVH à son client.

Il est précisé que le client peut, à tout moment, accéder à l'ensemble des documents contractuels le liant à la société OVH, par le biais de son compte client, à partir duquel ces documents sont accessibles.

De même, il est fait mention de l'adresse email du CIL (Correspondant Informatique et Libertés) de la société OVH, accessible à tout moment et qui s'engage au titre de sa mission à apporter une réponse aux demandes qui lui seraient présentées.

Les personnes concernées sont informées du transfert et du traitement de leurs données personnelles par une mention apposée sur le site Internet de la société OVH et par une indication dans les contrats souscrits par les clients.

Il est par ailleurs communiqué aux personnes concernées :

- l'identité du responsable du traitement et le cas échéant de son représentant,
- les finalités du traitement auxquelles les données sont soumises,
- les destinataires ou catégories de destinataires des données,
- L'existence d'un droit d'accès aux données les concernant,d'un droit de rectification et d'opposition sur lesdites données.
- La personne à contacter : Correspondant Informatique et Libertés.

Les présentes règles internes sont également accessibles librement sur le site internet du groupe OVH.

ARTICLE 8 DROIT D'ACCES, DE RECTIFICATION, D'OPPOSITION, D'EFFACEMENT ET DE VERROUILLAGE DES DONNEES

En application des présentes règles internes, l'ensemble des sociétés du groupe OVH doit permettre :

- De laisser à toute personne le droit d'obtenir une copie de toutes les données traitées la concernant, sans contrainte, à des intervalles raisonnables et sans délai ou frais excessifs,
- Le droit, pour toute personne concernée, d'obtenir la rectification, l'effacement ou le verrouillage de données, notamment au motif que les données sont incomplètes ou inexactes,
- Le droit, pour toute personne concernée, de s'opposer à tout moment, pour des raisons impérieuses et légitimes tenant à sa situation particulière, à ce que des données la concernant fassent l'objet d'un traitement, sauf en cas de dispositions contraires du droit national. Dans toutes les hypothèses où l'opposition est justifiée, le traitement doit être interrompu sans délai,
- Le droit, pour toute personne concernée, de s'opposer, sur simple demande et sans frais, aux traitements de données à la concernant à des fins de démarchage direct.

Ces droits peuvent être exercés auprès du Correspondant Informatique et Libertés du Groupe OVH à l'adresse cil@ovh.net.

ARTICLE 9 DECISION INDIVIDUELLE AUTOMATISEE

Le groupe OVH et l'ensemble de ses filiales s'engagent à ce qu'aucune évaluation ou décision en rapport avec la personne concernée et de nature à l'affecter de manière significative ne soit fondée uniquement sur le traitement automatisé de ces données, en dehors des hypothèses où la décision en question est prise en vue de la conclusion ou de l'exécution d'un contrat, à condition que la demande de conclusion et d'exécution des contrats introduite par la personne concernée ait été satisfaite ou que des mesures appropriées, telles que la possibilité de faire valoir son point de vue, garantissent la sauvegarde de son intérêt légitime.

ARTICLE 10 SECURITE ET CONFIDENTIALITE

Le groupe OVH et ses filiales prennent l'engagement de prendre l'ensemble des mesures d'ordre technique et organisationnel appropriées, afin de protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisé, notamment lorsque le traitement comporte des transmissions de données via un réseau, ainsi que contre toute autre forme de traitement illicite.

En particulier, le groupe OVH a mis en place, conformément à la politique de sécurité visée à l'annexe 6, les mesures de sécurité suivantes :

- Sécurité physique des locaux assurant l'hébergement des serveurs. Cet accès est réalisé par badge d'accès pour toute personne y compris les visiteurs, les intervenants extérieurs, les locaux donnant accès aux serveurs ne sont accessibles que par biométrie, l'accès aux serveurs est limité aux personnes habilitées,
- Protection contre les intrusions extérieures utilisant le canal des réseaux informatiques : routeur, par feu,
- Mesures destinées à assurer la confidentialité des données : développement de l'application dans un environnement informatique distinct de celui de la production,
- Mesures destinées à assurer la confidentialité des données lors des opérations de maintenance des équipements informatiques : intervention de maintenance des matériels enregistrés dans une main courante, support de stockage destiné à la destruction faisant l'objet d'une procédure de formatage bas niveau.
- Mesures destinées à assurer la confidentialité des données lors des opérations de maintenance des logiciels informatiques : rédaction d'une charte administrateur, intervention de maintenance des logiciels dans l'environnement de production enregistré par le biais de logs,
- Authentification et identification des personnes habilitées à accéder à l'application : accès par mot de passe, définition de profil d'habilitation pour chaque utilisateur en fonction des fonctions autorisées et catégories d'information accessible, accès à l'application faisant l'objet d'une journalisation (date, heure de connexion, identifiant d'utilisateur).
- Mise en place de proxy et firewall.
- Conservation des supports de stockage en interne même en cas de réparation.
- Des mesures particulières sont prises, s'agissant de données bancaires.

ARTICLE 11 RELATIONS AVEC LES SOUS-TRAITANTS QUI SONT DES FILIALES DU GROUPE

Il est rappelé aux filiales du groupe OVH qu'il leur appartient de mettre en œuvre des garanties suffisantes au regard des mesures de sécurité technique et d'organisation relatives au traitement à effectuer.

Le groupe OVH veille particulièrement au respect de ces mesures.

Il est également rappelé que les filiales n'agissent que sur instruction du groupe OVH et que les obligations en matière de sécurité et de confidentialité incombent aux filiales.

Il est enfin rappelé que ces obligations en matière de sécurité et de confidentialité qui sont imposées aux sous-traitants filiales du groupe OVH sont contenues dans un contrat de prestation de services.

ARTICLE 12 RESTRICTION AU TRANSFERT

Aucun transfert de données n'est effectué vers des responsables de traitement ou sous-traitants externes au groupe OVH à l'exception de mesures d'audit (audit de sécurité, notamment)

Il s'agit, notamment, du transfert d'informations vers les registres aux fins d'enregistrements des noms de domaine (exemple : auprès de l'AFNIC pour le .fr) et vers le prestataire chargé de la politique SSL pour la protection des données.

Ces transferts sont encadrés, dans le cas de transfert hors Union Européenne, par l'utilisation des clauses contractuelles types élaborées par la Commission Européenne afin d'assurer en toutes circonstances un niveau de protection adéquat aux données transférées.

ARTICLE 13 PROGRAMME DE FORMATION

Le groupe OVH dispense à ses différentes filiales et aux salariés de celles-ci ayant un accès permanent ou régulier aux données personnelles et associés à la collecte des données personnelles ou au développement d'outils servant au traitement des données personnelles, une formation adéquate sur l'application des présentes règles internes.

Le programme de formation est décrit en annexe 2.

La formation est proposée une fois par an aux personnes susceptibles de gérer des données personnelles.

ARTICLE 14 PROGRAMME D'AUDIT

De manière régulière de sa propre initiative ou à la demande d'un délégué à la protection des données d'une filiale, le groupe OVH peut demander à sa direction juridique la réalisation d'un audit sur le respect des présentes règles internes ; Ces audits sont menés selon le programme joint en annexe 10..

Les résultats des audits sont communiqués au Conseil d'Administration du groupe, ainsi qu'au CIL.

Le groupe OVH tient, par ailleurs, à la disposition des autorités nationales de protection des données des filiales concernées et du groupe OVH, une copie de ces audits, sur simple demande de ces dernières.

Les filiales consentent, dans le cadre des présentes règles internes, à se soumettre, sans restriction, aux audits réalisés par le groupe OVH, ainsi que par les autorités de protection des données et s'engagent à suivre les conseils desdites autorités sur tout ce qui touche à ces règles.

Il est enfin rappelé que le programme d'audit couvre tous les aspects des présentes règles internes, y compris les méthodes visant à garantir la mise en œuvre des mesures correctives.

Dans l'hypothèse où les audits effectuées feraient apparaître des failles, des actions correctives seront mises en œuvre dans les plus brefs délais afin d'y remédier.

ARTICLE 15 RESPECT DES REGLES ET CONTROLE DE LEUR APPLICATION

L'ensemble de ces opérations liées au transfert de données sont pilotées par la société OVH SAS et notamment sa direction juridique et informatique, en collaboration avec un cabinet d'avocats spécialisé par ailleurs désigné comme correspondant Informatique et Libertés auprès de la CNIL.

Un réseau de personnes en charge de la protection des données est mis en place par le groupe OVH, organisé dans les conditions précisées en annexe 3.

ARTICLE 16 ACTIONS DANS LE CAS OU LA LEGISLATION ENTRAVE LE RESPECT DES REGLES INTERNES

Lorsqu'une filiale du groupe a des raisons de croire que la législation qui lui est applicable risque de l'empêcher de remplir ses obligations en vertu de ces règles internes et d'avoir un impact négatif sur les garanties souscrites, elle s'engage à informer immédiatement la société OVH SAS ou le correspondant Informatique et Libertés.

Le correspondant Informatique et Libertés se réunira alors avec le service juridique de la société OVH SAS pour prendre une décision responsable sur l'action à entreprendre et en cas de doute, consultera la Commission Nationale Informatique et Libertés.

ARTICLE 17 MECANISMES INTERNES DE RECLAMATION

Le groupe OVH met en place un système interne de traitement des plaintes qui est le suivant :

Toute personne concernée peut introduire une réclamation indiquant qu'une filiale du groupe ne respecte pas les présentes règles, en contactant le correspondant Informatique et Libertés du groupe OVH SAS, par tout moyen écrit et notamment par email à l'adresse cil@ovh.net.

Il lui appartient de préciser la filiale concernée ainsi que le manquement constaté, de la manière la plus détaillée possible, en accompagnant, le cas échéant, sa plainte de tout document qu'elle pourrait juger utile.

Le correspondant Informatique et Libertés dispose alors de toute latitude pour mener l'enquête appropriée et alerter le Conseil d'Administration de toutes difficultés liées à la non application totale ou partielle des présentes règles, par les filiales.

Toute plainte déposée recevra une réponse écrite détaillée aux coordonnées communiquées par le plaignant, dans un délai maximum de trois mois à compter de sa réception.

ARTICLE 18 DROITS DE TIERS BENEFICIAIRES

Tout tiers bénéficiaire dispose d'un droit de recours en cas de violation des présentes règles, ainsi que d'un droit à réparation.

La personne concernée dispose du droit d'introduire une plainte auprès de la juridiction française compétente de la société OVH SAS ou de la filiale française considérée comme exportateur des données concernées.

Cette clause est rappelée dans le Guide de Déontologie accessible à tout client.

La personne concernée dispose également de la faculté de saisir l'autorité la Commission Nationale de l'Informatique et des Libertés (CNIL).

ARTICLE 19 RESPONSABILITE

La société OVH SAS endosse l'entière responsabilité, par délégation, de la protection des données personnelles échangées au sein du groupe et prendra les mesures nécessaires pour réparer les actes commis par ses filiales et, le cas échéant, versera une indemnité pour tout préjudice résultant de la violation par les filiales des règles contraignantes du groupe.

Dans cette hypothèse, les filiales seront invitées à faire parvenir à la société OVH SAS l'ensemble des éléments et informations en leur possession, de nature à démontrer, le cas échéant, leur absence de responsabilité dans la violation ayant abouti à la demande de réparation.

La charge de la preuve du respect, par le groupe OVH, des présentes règles internes lui incombe sans qu'il puisse renverser cette charge pour la faire supporter aux personnes concernées par le traitement de leurs données à caractère personnel.

ARTICLE 20 ENTRAIDE ET COOPERATION AVEC LES AUTORITES DE PROTECTION DES DONNEES

Aux termes des présentes règles internes, les filiales du groupe OVH coopèrent et s'entraident pour la gestion des demandes ou des plaintes de particuliers ou des enquêtes ou demandes d'information émanant de la CNIL.

Les filiales s'engagent également à appliquer les conseils des autorités de protection des données portant sur l'interprétation des présentes règles internes.

Le groupe OVH s'engage à coopérer avec les autorités chargées de la protection des données en ce qui concerne toute décision prise par l'autorité de contrôle et il suivra l'avis de l'autorité chargée de la protection des données sur l'interprétation et l'application des présentes règles internes.

ARTICLE 21 MISE A JOUR DES REGLES

Le groupe OVH s'engage à communiquer, à l'ensemble de ses filiales, ainsi qu'aux autorités de protection des données, toute modification significative apportée aux présentes règles internes ou à la liste des filiales, visant à prendre en compte les modifications de l'environnement règlementaire et de la structure du groupe.

Selon les modifications apportées, une nouvelle autorisation délivrée par les autorités de protection des données pourra être rendue nécessaire.

Le groupe OVH a désigné le service juridique afin de tenir à jour la liste des filiales soumises aux présentes règles internes, enregistrer et consigner toute mise à jour de ces règles et fournir aux personnes concernées ou aux autorités de protection des données, à leur demande, l'ensemble des informations requises.

Le groupe OVH précise également, qu'aucun transfert de données ne pourra être effectué vers une nouvelle filiale tant que celle-ci ne sera pas en mesure de garantir le respect des présentes règles internes.

Le groupe OVH prend également l'engagement de notifier, une fois par an, à la CNIL, toute modification des règles ou de la liste des filiales, avec un bref exposé des motifs justifiant cette mise à jour.

Le groupe OVH informera également les personnes concernées de toute modification substantielle des présentes règles internes.

ARTICLE 22 LIENS ENTRE LEGISLATION NATIONALE ET REGLES INTERNES

Le groupe OVH rappelle que, dans toutes les hypothèses où la législation locale offre un niveau supérieur de protection des données personnelles, supérieure aux présentes règles internes, celle-ci primera sur les présentes règles internes. Dans l'hypothèse inverse, les règles internes plus protectrices s'appliqueront.

En tout état de cause, les données personnelles traitées le sont, d'une manière conforme au droit applicable visé à l'article 4 de la directive 95/46/CE, ainsi qu'à la législation locale pertinente.

ARTICLE 23 DISPOSITIONS FINALES

Les présentes règles internes entrent en vigueur à compter du 1er septembre 2013 (période de transition au 1er mars 2014).

LISTE DES ANNEXES

Annexe 1 :

Données Clients visés par le présent transfert

Annexe 2:

Programme de formation.

Annexe 3:

Organisation du réseau de personnes chargées de la protection des données

Annexe 4:

Respect de la protection de la vie privée par type de traitement
.

Annexe 5:

Description du système interne de réclamation

Annexe 6:

Politique de sécurité

Annexe 7:

Processus de certification concernant les nouvelles applications logicielles

Annexe 8:

Liste des filiales du groupe OVH

Annexe 9 :

Finalités

Annexe 10 :

Programme d'audit