

10^e anniversaire

SOLUTIONS numériques

www.solutions-numeriques.com

Le CLOUD HYBRIDE

P.36

n°19 Mars-Avril 2018

La DÉMAT des FACTURES

P.30

RGPD

Tout savoir pour être en règle
dans 2 mois !

P.10

TROPHÉES de la TRANSFORMATION NUMÉRIQUE

P.57

Les 20 gagnants

- Adecco
- APMH
- ARPA
- Cdiscount
- Citya
- Decathlon
- ENGIE
- Gendarmerie Nationale
- IBM
- Maillage
- Ministère de l'Intérieur
- Montgenèvre
- Oscaro
- Pau
- PMU
- ShareIT
- Société Générale
- Store-et-Rideaux.com
- Total
- WoWW



P.58

L'ambitieuse stratégie de Hub One

Wireless, édition logicielle
et cybersécurité



Le pôle d'activité Silk Road Paris s'équipe
d'une solution de connectivité sur-mesure



P.8

Patrice Bélie,
Directeur Général,
Hub One



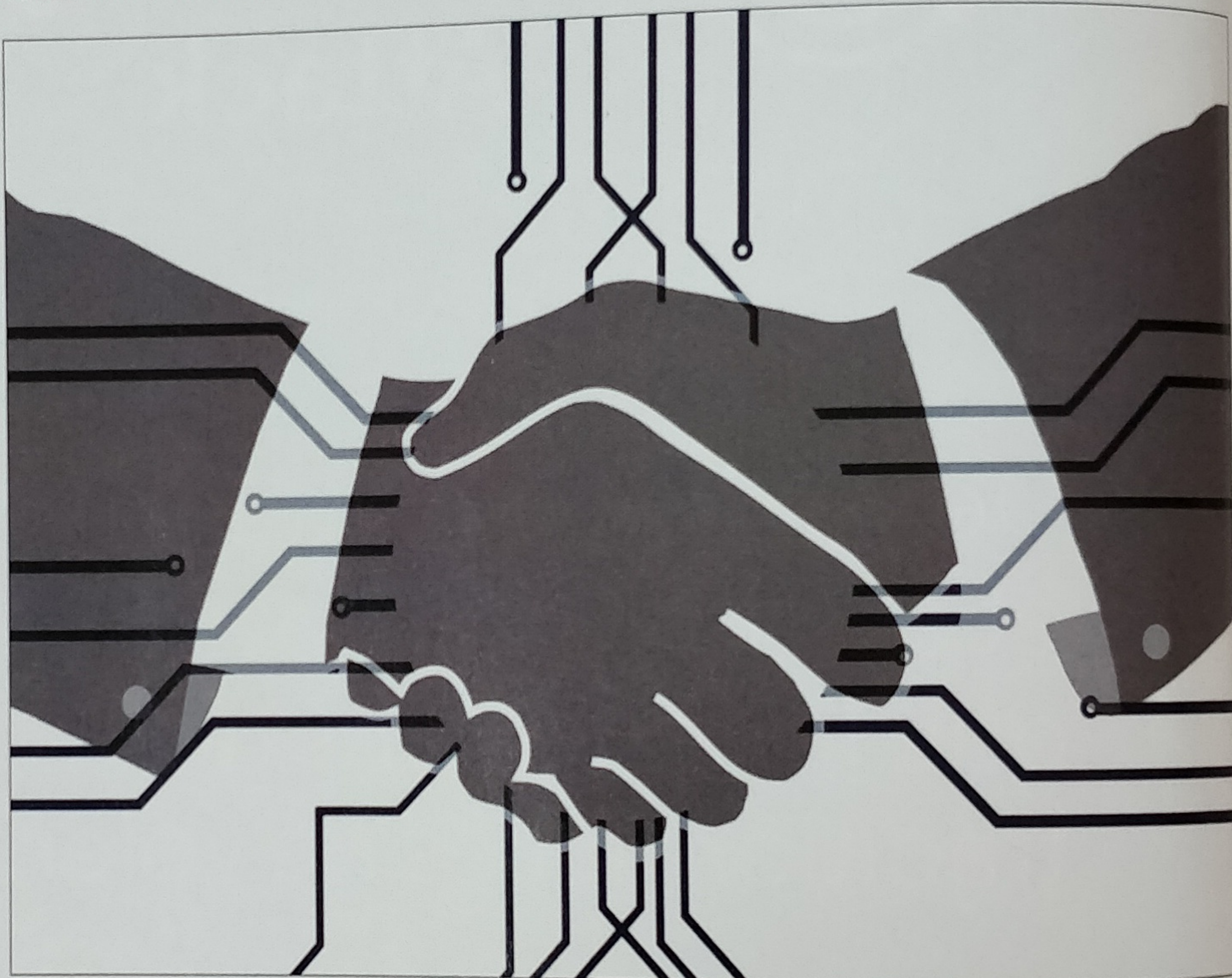
RGPD: qui est responsable d'une donnée dans le Cloud ?

L'entrée en application effective du RGPD implique une remise à plat des relations entre la DSI et les prestataires qui participent de près ou de loin aux traitements des données personnelles. Un bras de fer engagé avec les prestataires Cloud.

Conséquence directe de la mise en application du RGPD, la relation entre la DSI et ses prestataires va être profondément impactée par le règlement européen. A l'heure du Cloud roi, de plus en plus de données personnelles sont stockées par les entreprises chez des tiers, qu'il s'agisse d'éditeurs d'applications SaaS, de bases de données "as a Service" ou de services de stockage ou archivage dans le Cloud.

Repasser en revue tous les contrats est nécessaire

Comme le précise le guide du sous-traitant édité en septembre 2017 par la CNIL, le spectre des prestataires dont la responsabilité sera engagée en cas de fuite de données personnelles va être très large. Seront ainsi concernés les prestataires de services qui assurent l'hébergement et la maintenance des



plateformes, mais aussi les intégrateurs de logiciels, les sociétés de service impliquées dans la sécurisation de la plateforme et tout pres-

tataire qui a accès aux données personnelles. Dans ce contexte, le contrat va jouer un rôle clé dans les obligations des deux parties. Le DSI et son service juridique vont devoir passer en revue tous les contrats liant l'entreprise avec ses prestataires informatiques, afin que ces contrats soient actualisés et intègrent les dispositions mentionnées dans l'article 28 du règlement européen. La CNIL précise que le prestataire va devoir recenser par écrit toutes les instructions de son client concernant les traitements de ses données, de manière à pouvoir présenter une preuve que les actions engagées sont réalisées "sur instruction documentée du responsable de traitement". Enfin, le prestataire doit prouver à ses clients qu'il respecte ses obligations en termes de protection des données, y compris les rapports d'audit.

Partage d'expérience

FLORENT GASTAUD, DPO d'OVH

La conformité au RGPD implique une maîtrise de la chaîne de sous-traitance

"La conformité des clients en

leur qualité de responsables de traitement est directement conditionnée par la bonne conformité d'OVH en sa qualité de sous-traitant, et de ses éventuels sous-traitants ultérieurs. Cela implique de maîtriser la chaîne de sous-traitance d'OVH, ce qui nous pousse à renforcer les critères de sélection des sous-traitants, à procéder à des audits,

réviser les engagements contractuels, ... Fort heureusement, l'un des atouts d'OVH est justement la maîtrise de sa chaîne de valeur (conception des serveurs, maintenance, etc. qui sont gérés en interne). " Nous avons révisé les documents contractuels types afin qu'ils répondent aux exigences du RGPD, reflètent les engagements d'OVH à l'égard de ses clients et leur fournissent une protection optimale " ■



THIÉBAUT DEVERGRANNE, Docteur en droit, expert RGPD,
fondateur de donneespersonnelles.fr et Legiscope

« Le RGPD est un progrès majeur qui va dans le sens d'une clarification des responsabilités. »

"L'apport fondamental du RGPD est de donner aux juristes des outils qui vont nous permettre de clarifier le partage de responsabilité entre le responsable de traitements et ses sous-traitants vis-à-vis des données personnelles. Nous avons énormément de situations dans lesquelles on s'interrogeait : par exemple qui est responsable de traitement quand vous créez une page Facebook et collectez des données personnelles ? C'est sujet à beaucoup de débats... Le RGPD a la vertu de nous donner des outils pratiques et efficaces pour résoudre ce type de problématique ou la plateforme

se place entre le responsable de traitements et les sous-traitants. Ainsi, par exemple, la notion de responsable conjoint dans l'article 26 va nous permettre de fabriquer des solutions dans l'article 26 va nous permettre de fabriquer des solutions qui vont répondre aux situations les plus diverses. Le prestataire ou Cloud va pouvoir se positionner en tant que sous-traitant ou responsable conjoint selon ses services, et les juristes disposeront d'outils bien plus flexibles que ce qu'il était possible de faire jusqu'à aujourd'hui. Cela ne veut pas dire qu'il n'y aura plus de débats ni difficultés, mais au moins nous aurons des outils opérationnels pour résoudre ces questions." ■

De nouvelles clauses doivent être rédigées

Face à l'ensemble des nouvelles contraintes et obligations, les prestataires Cloud doivent mettre à jour leurs contrats et les conditions générales qui s'appliquent à leurs services souscrits. C'est ce qu'à déjà réalisé OVH en révisant ses CGS

(Conditions Générales de Services) afin de prendre en compte les exigences du RGPD. Néanmoins, Florent Gastaud, DPO d'OVH veut aller plus loin avec la mise en place de DPA (Data Processing Agreement), notamment pour les grands comptes. "Les DPA sont signés en complément du contrat classique

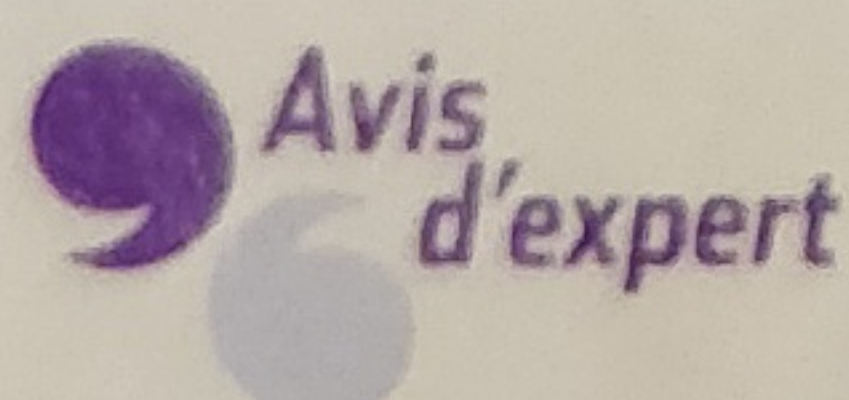
et sont spécifiquement conçus pour intégrer les exigences et obligations de chacune des parties en matière de traitement des données personnelles."

Pour l'instant DSI et prestataires cherchent à pousser le curseur au

maximum vers l'autre partie, mais il faudra savoir trouver le bon équilibre d'ici au 25 mai 2018.

Les obligations du RGPD concernent tous les organismes qui traitent des données personnelles pour le compte d'un autre organisme, dans le cadre d'un service ou d'une prestation. Sont notamment concernés : les prestataires de services informatiques (hébergement, maintenance, ...), les intégrateurs de logiciels, les sociétés de sécurité informatique, les entreprises de service du numérique qui ont accès aux données, les agences de marketing ou de communication qui traitent des données personnelles pour le compte de leurs clients. ■

> Les obligations du RGPD concerne les organismes qui traitent des données personnelles pour le compte d'un autre organisme, dans le cadre d'un service ou d'une prestation, comme les prestataires de services informatiques (hébergement, maintenance, etc.).



EMILIE DUMERAIN, Déléguée juridique, Syntec Numérique

Un travail de collaboration entre le client et son prestataire pour les contrats

"Le règlement impose la mention responsable de traitement et prestataires qui traitent des données personnelles pour le compte du client. L'article 28 impose qu'il faut décrire la nature, la finalité du traitement et sa durée, la nature des données. Référencer tous les cas de figure dans des clauses type est impossible et c'est un travail de collaboration entre le client et son prestataire pour obtenir les bons termes du contrat, sachant que c'est au client, qui connaît la finalité des traitements à qui revient l'initiative de cette négociation. Certaines mentions de

cet article 28 sont relativement floues, notamment lorsque le texte évoque la notion d'aide que doit le sous-traitant au responsable de traitement pour remplir ses obligations. Jusqu'où doit aller le sous-traitant dans cette aide ? Il faut respecter un équilibre entre ces deux rôles sachant que les clients ne peuvent se déresponsabiliser, et que le responsable de traitement reste le maître du fichier. Il convient donc de respecter l'équilibre entre les deux rôles dans les contrats." ■

