# L'INTÉGRATION D'INFRASTRUCTURES ET SERVICES CLOUD : RISQUES ET PRECAUTIONS

**8 novembre 2016**

## COMMISSION JURIDIQUE


**Thomas Beaugrand**

**Avocat**

STAUB & ASSOCIÉS

société d'avocats

89, bd Haussmann - 75008 Paris

+33 1 47 42 47 42

www.staub-associes.com

1) Diversité des modèles d'intégration cloud

2) Enjeux contractuels de l'intégration de services cloud

3) Protection des données personnelles

4) Sécurité des données et applicatifs dans le cloud

STAUB & ASSOCIÉS
société d'avocats

# SOMMAIRE

Design : WebhelpOffice, Paris

# Diversité des modèles d'intégration de services cloud

# CONTEXTE MARCHE – L'INTEGRATION DE SYSTEMES

## ❑ L'intégration classique de solutions informatiques

> Traditionnellement, les SSII proposent à leurs clients des prestations d'intégration de solution informatiques « **on premise** ». Les travaux se faisaient soit chez le client directement, soit dans les centres de Services des intégrateurs, et la solution était soumise à une procédure de recette avant d'être mise en production.

## ❑ L'avènement du Cloud

> L'avènement du Cloud computing a entrainé un **basculement du marché**, les entreprises plaçant désormais leurs ressources informatiques dans le « *nuage électronique* » :

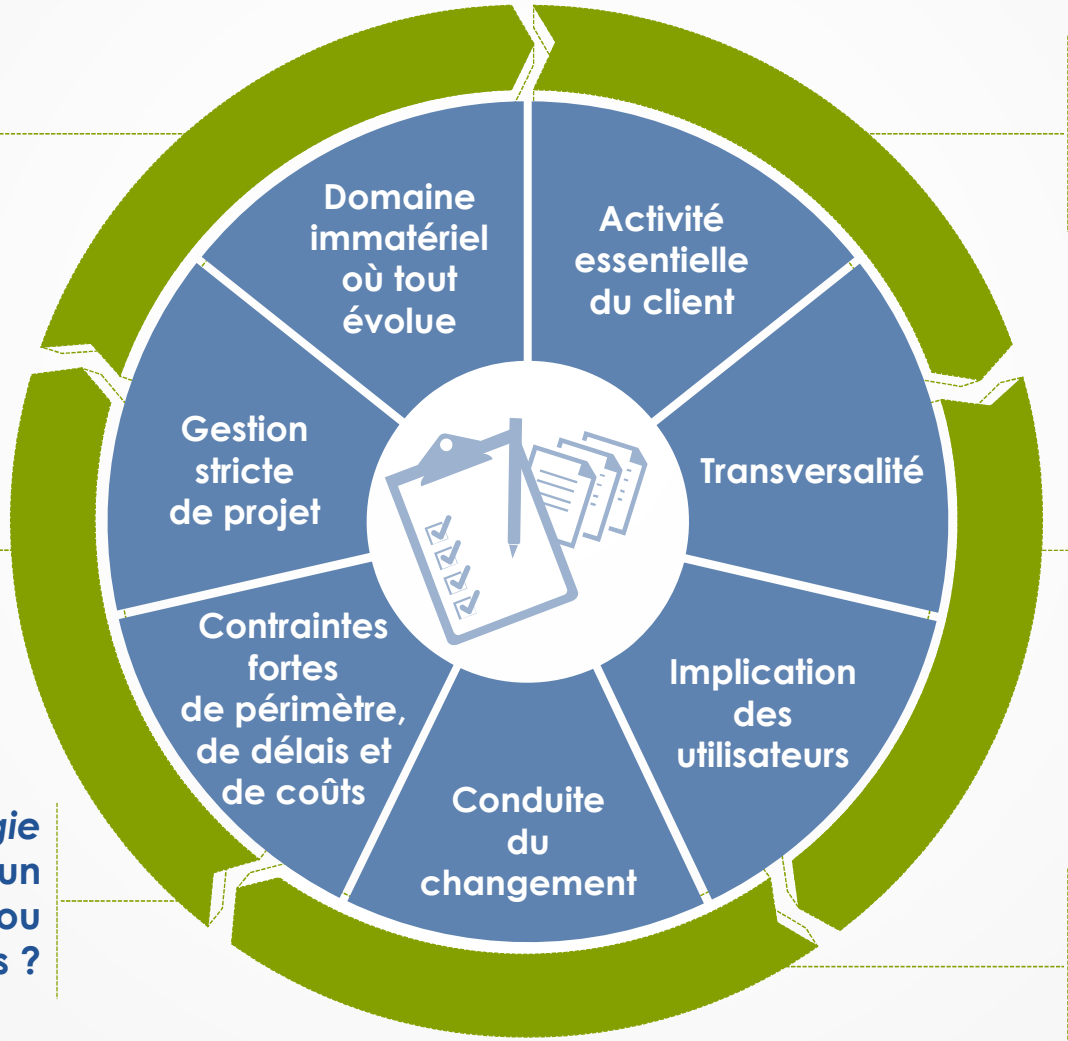
- Les éditeurs logiciels ont converti leurs produits logiciels en **services applicatifs**
- De nouveaux éditeurs sont apparus, proposant des **services cloud natifs**
- Les **intégrateurs** ont changé de rôle et leur profession évolue
- Les clients ont commandé des solutions désormais « **virtualisées** »
- Le modèle de la licence a fait place au modèle de la **souscription**
- Les **métriques de mesure** se sont complexifiées

# CONTEXTE TECHNIQUE – DIVERSITE DES INTEGRATIONS

- **Diversité des projets informatiques commandés par les Clients**

**Projets en mode cascade ou en mode Agile ? Quelle méthode pour quel budget ?**

**Intégration de projets informatiques ERP, ECM, BI, CRM, SIRH, SOA, PABX, CU… et déploiements afférents ?**




**Développement de sites web (e-marketing, boutiques online) et d'applications**

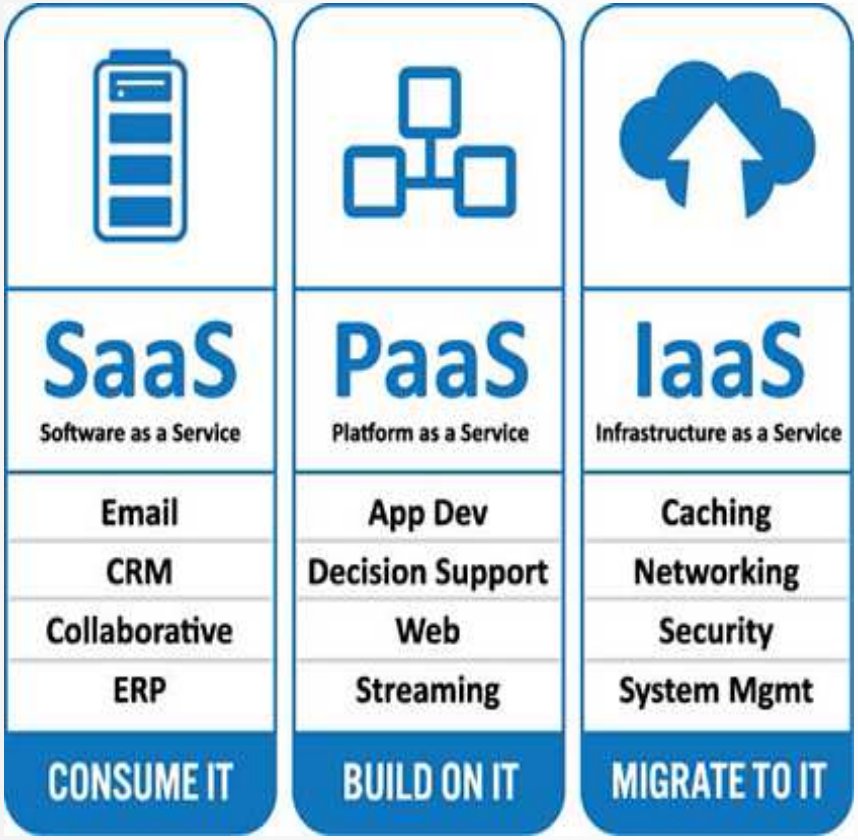
**Projets Cloud (prestations SaaS, IaaS, PaaS, etc.) et intégration de services applicatifs préexistants**

**Compte facturé en *régie* ou au *forfait* ? Selon un échéancier spécifique ou suivant les recettes ?**

**Projets de solutions métiers ou développements spécifiques (phase de conception cruciale)**

# CONTEXTE TECHNIQUE – DIVERSITE DES SOLUTIONS

## ❑ Les solutions fonctionnelles




### Infrastructure As A Service (IaaS)

Offre d'hébergement distant et de stockage, qui revient en dernière analyse à **louer une infrastructure de stockage** et réseau qui fonctionnent au sein d'une machine virtuelle chez le prestataire. Le client « consomme » de l'espace-disque et de la puissance machine à la demande, dans le cadre d'unités d'œuvres ou de métriques en lien avec la consommation des ressources allouées à ses besoins. **L'intégrateur qui fournit un IaaS acquiert véritablement un rôle d'hébergeur**

### Software As A Service (SaaS)

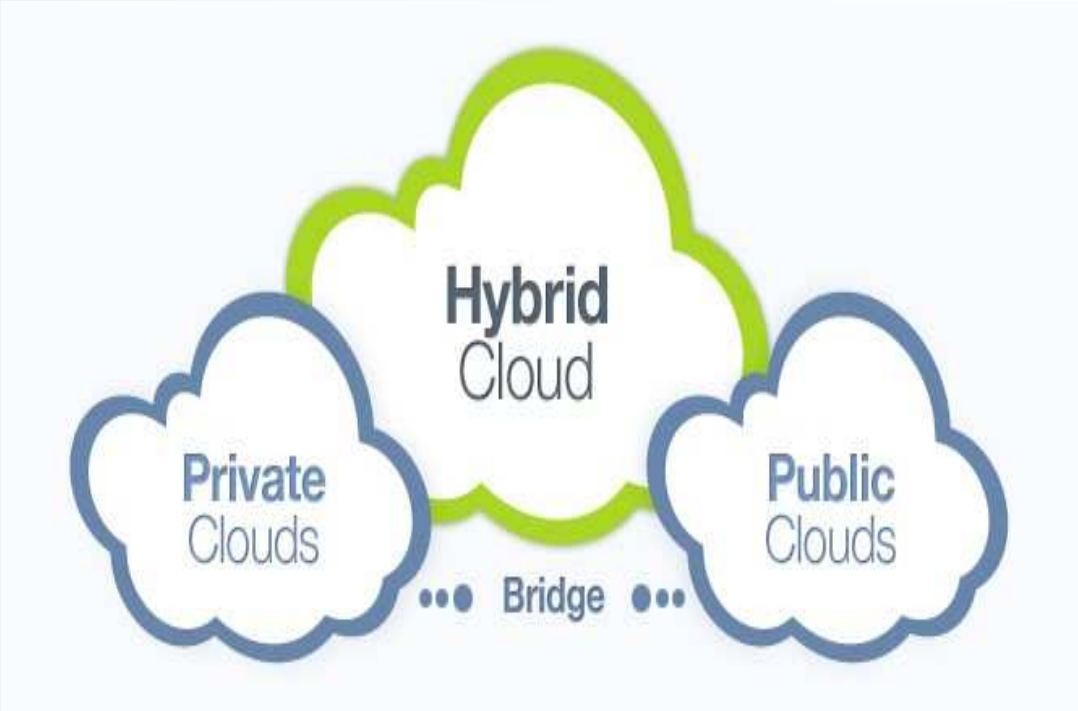
Offre permettant d'utiliser à distance un progiciel en ligne (ex : CRM SalesForce ou progiciel de gestion de paie), qui est l'héritier de l'ASP et se décline aujourd'hui sous de nombreuses formes et selon des modèles économiques qui sont proches de l'abonnement. Le client ne paie plus des « droits d'utilisation » dans le cadre d'une licence portant sur le logiciel, mais paie la consommation d'un Service. **L'intégrateur ne doit plus seulement indiquer le montant d'une licence, mais intégrer la dimension « abonnement » des solutions qu'il intègre**

### Platform As A Service (PaaS)

Mise à disposition à distance d'un environnement informatique à vocation plus technique qu'applicative, et prêt à l'emploi (environnement de test ou de développement d'applications à personnaliser) (ex : Google AppEngine ou Windows Azure) **Le client s'appuie sur une plateforme distante pour effectuer ses propres travaux d'ingénierie et développement logiciel.**

# CONTEXTE TECHNIQUE – DIVERSITE DES SOLUTIONS

## Les solutions techniques




### Cloud Public

L'éditeur d'un Cloud public mutualise ses ressources (puissance de calcul, espace de stockage, connexions réseaux, maintenance technique et bande passante) et les propose à ses clients. L'éditeur est seul propriétaire des éléments logiciels et matériels du service

### Cloud Privé

Le client utilisateur est souvent le propriétaire du matériel, décide des applicatifs inclus dans la solution Cloud, et en confie l'intégration et/ou l'hébergement à un prestataire Cloud. Le Cloud privé permet souvent des paramétrages et mesures de sécurité renforcés, l'intégration du service au sein du système d'information du Client est facilitée

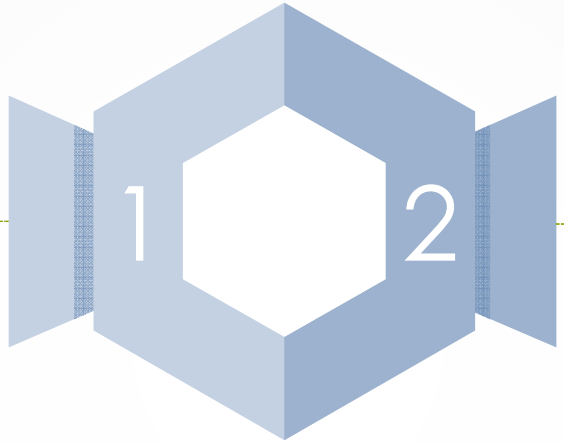
### Cloud Hybride

Il propose de cumuler les avantages des précédentes configurations en permettant via une plateforme virtualisée unique de passer d'un cloud privé à un cloud public, par exemple pour absorber une montée en charge significative, multiplier les possibilités fonctionnelles ou distinguer des traitements d'importance inégale

# CONTEXTE JURIDIQUE ET ECONOMIQUE

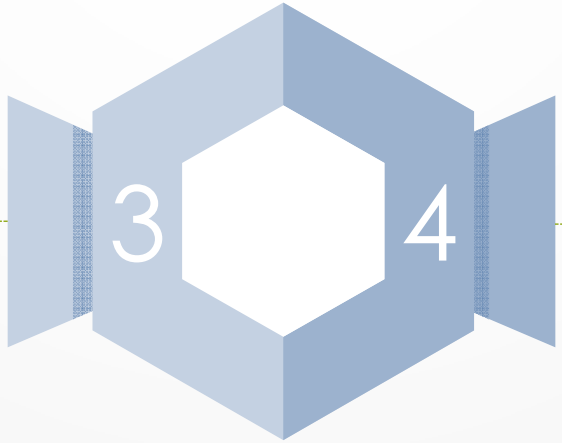
## Les 4 grands changements de paradigme qui caractérisent l'intégration cloud

- **Notion d'équipement > notion de service :**
- l'*objet de droit* qui est commandé par l'acheteur n'est plus le logiciel en tant que tel, mais un **service dématérialisé** qui mêle un objet incorporel (un progiciel, une architecture virtuelle) et des services associés (maintenance, hébergement, monitoring, exploitation)




**Notion de conformité > notion de disponibilité :**
la « *conformité* » de la solution par rapport à un référentiel (CdC, SFD) est remplacée par la « *disponibilité* » du service. **Bien sûr dans de nombreux cas (intégration) la conformité reste due**, mais une fois intégrée, la solution est fournie sans installation sur le système du client

- **Sécurité interne > sécurité déléguée :** la sécurité est aussi externalisée, ce n'est plus le client qui met en place des dispositifs de sécurité sur ses serveurs au sein de sa salle informatique, mais l'intégrateur qui déploie des **dispositifs de sécurité sur son datacenter** (ou le plus souvent son sous-traitant hébergeur)




**Coresponsabilité dans la dataprotection :**
Le RGDP organisant la nouvelle dataprotection a un impact décuplé sur les relations entre client acheteur et prestataire intégrateur. La dataprotection ne fait plus l'objet d'une « navette » contractuelle, mais d'une **coresponsabilité dynamique**, l'intégrateur étant tenu de fournir des services conformes à la Règlementation.

02

# Enjeux contractuels de l'intégration de services cloud

# CONTEXTE JURIDIQUE

## 1) L'éditeur-intégrateur : la virtualisation de ses propres solutions éditoriales

### Adopter une logique d'hébergeur

- **Disponibilité** et **accessibilité** du Service
- **Chargement** et traitement des données (qui en assure la responsabilité, le client ou le prestataire ?)
- **Sécurisation** réseau et accès (cf. infra)
- **SLA, KPI :** quels engagements, quelle mesure, quelles sanctions ?
- Responsabilisation du client sur les **connexions et traitements** de ses utilisateurs

### Sécuriser les accès

- Puisque le traitement et les actifs sont à distance, la sécurité d'accès est un point essentiel > confidentialité des codes / **PSSI** du client ou **PAS** contractuel. Le PAS standardisé est très recommandé, il permet de définir une « règle du jeu » et le référentiel auquel doit se conformer l'éditeur

### Mesurer la consommation

- Contractualiser les **métriques** de facturation
- **Monitoring** et contrôle de consommation

### Conserver aussi la logique d'intégrateur

- Phase d'initialisation (**« build », « set-up »,** personnalisation, adaptation…)
- **Conformité** du service aux spécifications issues de la phase de conception (attention aux demandes évolutives) >> clarté et univocité du **Référentiel de conformité**
- Phase de recette (parfois VABF + VSR)
- Mise en production et assistance du prestataire au client (attention aux recettes tacites)

### Stipuler les engagements

- Une **matrice RACI** reste pertinente
- Si le Client demande des **interfaçages**, ils sont à spécifier et dimensionner dans l'offre, et le prestataire doit conditionner sa prestation en fonction de ce qu'il sait des produits tiers et de l'éventuelle collaboration de leurs utilisateurs

### Industrialiser la maintenance

- Cloud = **mutualisation** des ressources + standardisation des solutions
- Cloud = **standardisation** de leur maintenance

# CONTEXTE JURIDIQUE

## 2) L'intégration de solutions cloud tierces (SaaS + SaaS, IaaS + SaaS, etc.)

- **Ne pas vendre plus qu'on n'obtient**
  - **Contrôler** les conditions de POC (à partir de quels contrats fournisseurs est-il développé ? Pourra-t-on l'industrialiser et le commercialiser sur cette base contractuelle ?)
  - **Valider** les droits et garanties à acquérir auprès des éditeurs de solutions cloud (SLA, garantie d'éviction et de conformité, métriques de mesure, etc.)
- **Définir qui va opérer les services**
  - En contexte cloud, ce sont les utilisateurs du client, mais le périmètre de ces users doit être soigneusement contrôlé (préposés, clients finaux, etc.)
- **Construire l'offre contractuelle**
  - A contributeurs distincts, **responsabilités différenciées** : l'intégrateur doit donc procéder à un **lissage global** de la responsabilité et des SLA (*si l'offre est construite et rationalisée en amont, sinon il risque de supporter les delta*)… ou proposer des **Livrets contractuels** (*contrat d'intégration + CGV des éditeurs cloud*) afin de faire une **application différenciée** des SLA et pénalités. La solution à adopter dépend de la typologie et des exigences des clients
- **Ne pas s'engager au-delà de ce qu'on fait**
  - **Distinguer** le périmètre d'intégration (build ou set-up) de la phase de *run* (SLA)
  - **Contrôler** les limitations de responsabilité des fournisseurs tiers, et prévoir un **plafond d'indemnisation** calé sur **le + petit dénominateur commun**, ou proposer des **plafonds différenciés** dans le cadre d'un Livret contractuel
  - **Assurer le schéma contractuel** de fourniture en conformité avec le projet de vente
- **Prévoir les escalades techniques**
  - Si l'intégrateur assure le guichet unique, il doit assurer le relais dont il a besoin chez les éditeurs
- **Prévoir les appels en garantie**
  - La notion de **périmètre de responsabilité** est cruciale
  - **Bien connaître les contrats fournisseurs** (« ***back-to-back*** » et garanties autonomes)
  - Couvrir l'ensemble des sources de responsabilité en déterminant vers qui escalader les anomalies et à qui demander réparation le cas échéant

# CONTEXTE JURIDIQUE

## 3) L'intégration de solutions composites : intégrer puis héberger

- **Variante de la solution précédente :**
  - **Conception** et développement d'une solution (logique « *on premise* ») par intégration de briques logicielles tierces
  - Interconnexion puis **placement dans le cloud** par hébergement distant
  - **Organisation des spécificités cloud** (sécurité des données, des connexions, monitoring, charge de la preuve, etc.)
  - Responsabilisation du client sur ses **connexions**
  - Application d'une **responsabilité contractuelle lissée** ou d'une **responsabilité contractuelle différenciée** selon les produits inclus
- **Assurer l'interopérabilité**
  - Attention aux interfaçages et à la **compatibilité ascendante**
- **Mesurer la consommation**
  - Contractualiser les **métriques** de facturation
  - **Monitoring** et contrôle de consommation

03

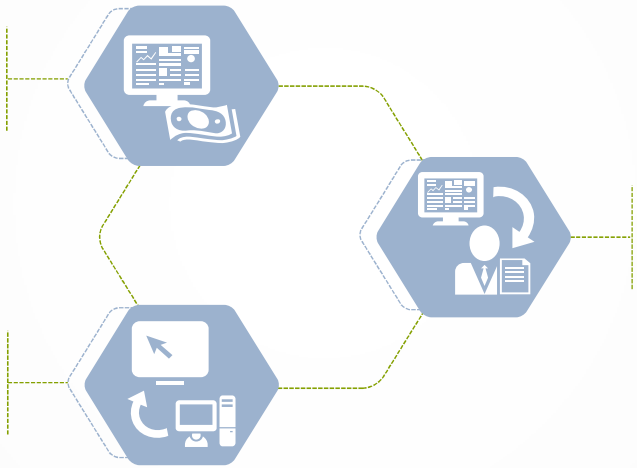
# Protection des données dans les services cloud et rôle de l'intégrateur

# LE CONSEIL DE L'INTEGRATEUR AU CLIENT

> L'intégrateur qui assembler une solution cloud, qu'elle soit native ou composite, ne peut pas ignorer les objectifs et traitements qui seront effectués par le Client. Sans s'y substituer, le Prestataire doit se distinguer en apportant un **conseil circonstancié** au Client sur l'ensemble de ses obligations générales relatives aux données personnelles :

**Un très grand nombre de solutions traitent des données personnelles, à titre principal ou incident**

> un SIRH traite des données des salariés



> un CRM gère les contacts des clients, etc.

> un site web enregistre les adresses IP des visiteurs…

> l'introduction dans l'entreprise d'une technologie qui permet la collecte et le traitement de données personnelles doit impérativement faire l'objet d'une **information précise du personnel au préalable** (droit social)

> toute technologie qui traite de données personnelles (de la vidéosurveillance à la messagerie d'entreprise, du badge d'accès au journal de logs), devait faire l'objet d'une **déclaration auprès de la CNIL** (loi de 1978 modifiée par la LCEN de 2004) et désormais d'une **analyse de risque** et d'un système **d'accountability** (cf. infra).

  > Le prestataire ne doit jamais se substituer au client pour les obligations qui incombent à ce dernier, mais…

  > **Le prestataire doit tenir à la disposition du client un exposé clair et complet des mesures de protection logiques et physiques dont il entoure son datacenter (cf. infra)**

# LE CONSEIL DE L'INTEGRATEUR AU CLIENT

## Une solution Cloud peut le plus souvent traiter de données personnelles :

- À titre principal : messageries professionnelles, plateformes de travail collaboratif, CRM digital, gestion de la paie, service marketing, etc.
- A titre incident : contacts opérationnels, intervention de maintenance, offshoring, etc.
- Dans tous les cas, tant la structure technique que l'organisation de l'entreprise doivent correspondre aux exigences de protection des données personnelles

## En cas de flux transfrontalier de données, le client pose la question :

- de la **localisation des données** (de préférence en Europe)
- de la **divulgation aux tiers** possibles
- du rôle des autorités locales (ex : Patriot Act ou PRISM, et Loi Renseignement Fr)
- du respect par le prestataire du **niveau de protection standard** d'Europe

L'intégrateur doit apporter (i) son conseil sur les obligations du « *data controller* », car il ne joue qu'un rôle de « *data processeur* ». L'intégrateur, s'il recourt à des sous-traitants situés à l'étranger, doit certifier qu'ils se conforment aux obligations européennes (« ***clauses contractuelles type*** »). **Mais c'est par construction aux éditeurs de services cloud, qu'ils les hébergent eux-mêmes ou s'appuient sur un sous-traitant hébergeur, de prouver leur conformité aux exigences légales.**

> **Les entreprises, en particulier les intégrateurs, doivent désormais concevoir les solutions en prenant en compte l'impératif de protection des DP de manière native et structurelle.**

# LES PRINCIPES DE PROTECTION DES DONNEES PERSONNELLES

- **Les 4 points cardinaux de la protection légale**
  - *Quelles données* collectées ?
  - Pour *quelle(s) finalité(s)* ?
  - Pour *quel(s) destinataire(s)* ?
  - Pendant *combien de temps* ?
- **Le principe de proportionnalité**
  - La collecte doit être « ***loyale*** » (transparente) et également « ***légitime*** »
  - Les données doivent être ***pertinentes*** pour les ***finalités*** poursuivies
  - Pas de conservation indéfinie
- **Le principe d'information de la personne**
  - Complexité des systèmes de recueil du consentement (*opt-in, opt-out, exceptions*)
  - Confusions entre traitements et finalités (*plusieurs applications pour une même finalité, ou inversement*)

**Le sujet est devenu tellement central, sur le plan juridique et contractuel, que l'intégrateur de services cloud doit maîtriser cette législation pour répondre efficacement à ses clients.**

# LES PRINCIPES DE PROTECTION DES DONNEES PERSONNELLES

> **Bien que n'étant pas le responsable du traitement commandé, le Prestataire est tenu :**

- De fournir des prestations conformes à la législation applicable (il est donc capital de définir cette législation dans le contrat);
- De ne traiter les données personnelles du Client (et le plus souvent de ses clients finaux) de manière sécurisée et confidentielle, uniquement sur instruction du Client
- D'apporter au Client le conseil nécessaire pour assurer la protection des données personnelles (obligation de conseil et de mise en garde)

> **En revanche, c'est bel et bien le Client qui est tenu de :**

- Obtenir le **consentement préalable** de la personne dont les données sont collectées
- **Informer la personne** des droits dont elle dispose et de la finalité poursuivie
- Collecter des données **pertinentes et proportionnées** par rapport à la **finalité** poursuivie
- **Déclarer le traitement** à la CNIL ou obtenir son autorisation
- **Sécuriser le traitement** et la conservation des données

CNIL
Commission Nationale de l'Informatique et des Libertés

**Toutefois attention, l'obligation de conseil du prestataire s'intensifie en ce moment, notamment via les nouveaux concepts édictés par le Règlement Européen de protection des données personnelles (RGDP), dans lequel les sous-traitants assument un rôle de plus en plus important et détaillé.**

# LES FLUX TRANSFRONTALIERS DE DONNEES

> **Sanctions en cas de transfert non autorisé :**

> sanction pénale: jusqu'à 5 ans d'emprisonnement et 300 000 € pour les personnes physiques (article 226-16 CP) et jusqu'à 1.5 M€ pour les personnes morales (article 226-24 CP)

>

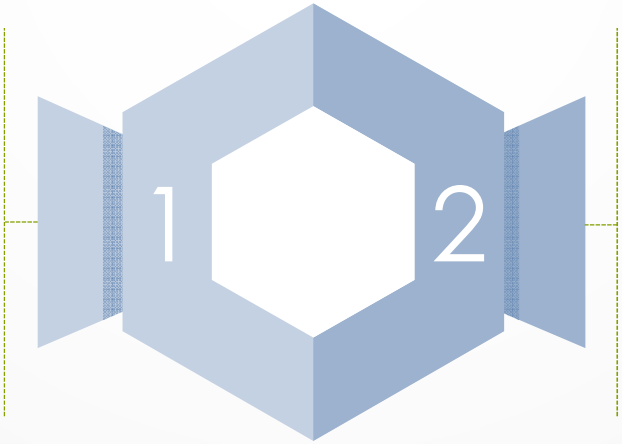
> sanction administrative, la CNIL disposant d'un pouvoir de sanction propre. Les avertissements et/ou les mises en demeures prononcées à l'encontre des entreprises par la CNIL peuvent notamment être accompagnés de sanctions pécuniaires allant de 150,000 euros pour le premier manquement à 300,000 euros en cas de récidive, et **vont être alourdies par le Règlement européen (*infra*)**

## Deux solutions juridiques sont admises :

### « Binding Corporate Rules »

- Ensemble de règles internes relatives aux transferts de hors de l'UE (ou des pays de protection « adéquate ») au sein d'un même groupe de sociétés.
- Adoptées de manière volontaire, les BCR créent un cadre normatif unique avec « *des garanties au regard de la protection de la vie privée et des droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants* »

>




### Clauses Contractuelles Types

Contrats-types publiés par la Commission Européenne pour conférer des droits aux personnes physiques, opposables aux responsables de traitements et sous-traitants hors UE :

- CCT entre deux responsables de traitement
- CCT entre un responsable et un sous-traitant
- Cas du offshoring (sous-traitance secondaire) et possibilités de signature directe avec le maître d'ouvrage

# DE L'INVALIDATION DU SAFE HARBOR…

**C'est très important pour les éditeurs cloud, mais également pour les intégrateurs qui (i) sous-traitent une partie de leurs travaux à l'étranger, ou (ii) assemblent des services SaaS fournis ensuite au Client**

## > Safe Harbor

> *Le « Safe Harbor » était un label de confiance, créé par la Commission européenne (décision n°520/2000/CE du 26 juillet 2000), autorisant les entreprises américaines à « **auto-certifier** » auprès des autorités américaines, qu'elles se conformaient au niveau de protection exigé en Europe, et qu'elles appliquaient les règles listées au sein du label.*

## > CJUE 6 octobre 2015

*La CJUE a décidé que les conditions dans lesquelles Facebook envoyait les données européennes vers les USA ne répondaient pas aux exigences de la législation européenne, que **les autorités nationales n'étaient pas liées par la décision de la Commission** qui ne pouvait en aucun cas de substituer aux investigations des CNIL européennes, et que l'une d'elles pouvait parfaitement considérer que le niveau « adéquat » de protection n'était pas assuré, nonobstant le « Safe Harbor ».*

## > Effet de la décision

*De facto, tous les contrats qui avaient fait de l'adhésion Safe Harbor une condition sont potentiellement menacés, puisque partiellement illicites, ou en tous cas non-conformes aux règles européennes qui s'imposent aux entreprises européennes. En cas de flux transfrontalier de données non autorisé, ou comme ici vers un pays n'offrant pas le « niveau adéquat » de protection, ces entreprises françaises risquent **5 ans d'emprisonnement et 300.000 € d'amende**…*

# … A L'ADOPTION DU PRIVACY SHIELD

- Le 29 février 2016, la Commission européenne a rendu publics les documents juridiques qui instaureront le *« bouclier de protection des données UE-Etats-Unis »* (Privacy Shield), censé offrir des *« garanties solides pour restaurer la confiance dans les transferts transatlantiques des données »*

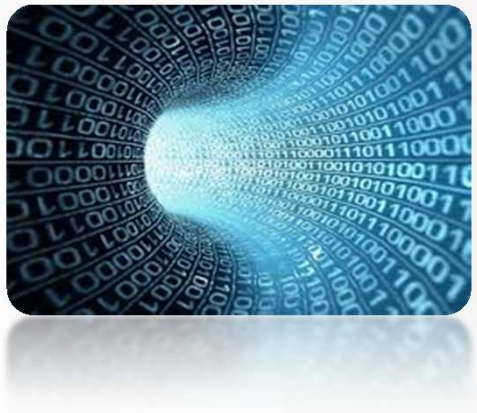
- Le G29 a admis un « *pas en avant* » mais déplore un **manque de clarté**, du texte, les principes et garanties apportés par le *Privacy Shield* se retrouvant à la fois dans la décision d'adéquation et dans ses annexes censées les expliciter et les préciser

- Les modalités d'application du **principe de finalité limitée** ne sont pas claires (alors qu'il s'agit bien de « fermer » un périmètre d'utilisations autorisées) ;
- L'absence de mention expresse du **principe de durée de conservation limitée** des données(ce qui ruine en pratique la notion de durée maximale de conservation si celle-ci est sujette à interprétation…) ;
- L'absence de dispositions dédiées à la **protection** qui devrait être offerte lorsque les **décisions individuelles automatisées** sont prises sur le seul fondement d'un traitement automatisé de données ;
- Le caractère complexe du mécanisme de **recours offert aux individus,** difficile à mettre en pratique, notamment parce qu'il ne pourrait s'exercer qu'en anglais ;
- Les autorités américaines n'ont pas apporté d'éléments suffisamment précis pour écarter la possibilité d'une **surveillance massive et indiscriminée des données des citoyens européens**.

**Dans le doute, on doit donc plutôt considérer qu'en l'état, et malgré l'affaire *« Facebook / Max Schrems »* ayant conduit à l'invalidation du *Safe Harbor*, le grief demeure entier.**

# ADOPTION DU RÈGLEMENT EUROPÉEN DE DATAPROTECTION

- Règlement uniforme d'**applicabilité directe** partout en Europe (adopté le 27 avril 2016, pleinement applicable en 2018)
- Création d'un « ***Data Protection Officer*** » dans l'entreprise (remplace le CIL)
- Simplification des formalités (plus de déclaration préalable) mais responsabilité accrue des entreprises et de leurs prestataires dans le déploiement d'une dataprotection structurelle et permanente, documentée



**La complexité va s'accroître, et la responsabilité des entreprises également :**

## *De nouveaux droits au profit des personnes physiques :*

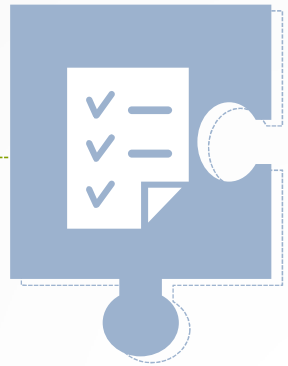
- Droit opposable à la **portabilité des données** (d'un prestataire à l'autre)
- Droit à la **limitation** (suspension du traitement à la demande de la personne)
- Droit à l'**oubli numérique** (sauf motifs d'intérêt général)

## *De nouveaux concepts à mettre en œuvre par les prestataires :*

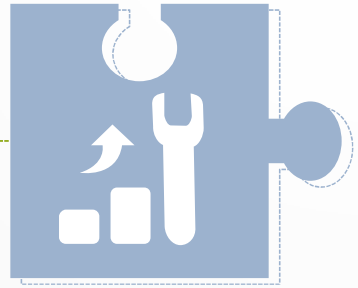
- Exigence de **l'analyse d'impact** à la charge du responsable du fichier, mais qui s'étend au prestataire pour les produits qu'il développe et commercialise
- Développement « **Privacy By Design** » : protection structurelle des DP dans les règles de gestion du produit logiciel
- Principe du « **Security By Default** » : minimalisation des DP utilisées dans le produit logiciel
- Obligation des règles d' « **accountability** »

# ADOPTION DU RÈGLEMENT EUROPÉEN DE DATAPROTECTION

- Le recours aux prestataires numériques (le responsable du traitement fait appel à un « *sous-traitant* ») change : non seulement le **contrat** doit comporter tous les engagements nécessaires…



- … Mais cette démarche devient **dynamique**, le sous-traitant devant justifier de l'entretien des mesures de dataprotection auprès de son donneur d'ordre le responsable du traitement, qui lui-même doit pouvoir faire état des mesures à tout moment. Le rôle du DPO est donc constant dans le maintien de la conformité.



- **Champ d'application :**
- La loi française protégeait les données des français, mais ne s'appliquait qu'aux entreprises de droit français.
- Le Règlement simplifie les choses : dès qu'un prestataire *propose* des biens ou services à des **personnes se trouvant sur le territoire de l'UE**, ou s'il se contente « *d'observer* » le comportement de ces personnes (allusion au profilage marketing notamment), ce responsable est soumis au Règlement, et ce **quand bien même il n'est pas établi sur le territoire de l'UE ou n'est pas de nationalité européenne** (il doit alors y désigner un représentant).

**Pour les entreprises, il n'est plus seulement question d'assurer l'exploitabilité juridique de la donnée personnelle, mais de mettre en œuvre tout un <u>écosystème du traitement de la donnée</u>, qui assure son équilibre et sa confidentialité de bout en bout, par des entreprises soumises à des obligations renforcées et constantes**

# LA RESPONSABILITE ACCRUE DES SOUS-TRAITANTS

> Le Règlement conserve la même définition du sous-traitant, qui reste soumis à la même forme de **propagation de la législation européenne** en même temps que les données sont transférées vers lui, quelle que soit la localisation de ses serveurs. Mais les termes des contrats qui lient les responsables de traitements avec leurs sous-traitants vont considérablement s'enrichir, à mesure que les deux cocontractants deviennent **coresponsables** de la protection des données personnelles manipulées. Le contrat va devoir :

- Définir dans le détail la ou les **finalités du traitement** (qui précédemment s'inférait uniquement de la nature des prestations confiées par le client au prestataire) ;
- Indiquer **l'objet et la durée de conservation** des données personnelles concernées ;
- La **typologie des données collectées** et traitées par le sous-traitant pour le compte du responsable du traitement ;
- La **typologie des personnes concernées** par la collecte et le ou les traitements ;
- Les droits du sous-traitant et les obligations du responsable de traitement (et plus seulement l'inverse) ;
- Les **engagements du sous-traitant** en matière (i) de reproduction des mentions d'information ou de collecte du consentement au sein de la solution qu'il fournit ou qu'il administre ;
- La mise en œuvre et l'entretien d'une **documentation précise** exposant les mesures de protection et de confidentialité entourant les données ainsi que leurs accès ;
- L'exigence de **coopération entre les parties** pour donner effet aux droits des personnes, mais aussi entre les parties et les autorités de contrôle ;
- L'assistance entre les parties dans la **gestion des demandes** des personnes physiques dont les données sont traitées ;
- Les modalités de **notification des failles** de sécurité ;
- L'entretien des dispositifs et procédures internes du prestataire permettant d'attester en tout temps du **respect du principe constitutif de « *privacy by* design »** (infra) ;
- Les **mesures d'urgence** en cas (i) de fuite de données et/ou (ii) de non-conformité du dispositif aux niveaux convenus.

# 04

# Sécurité des données et des actifs dans le cloud

# DERRIERE LA CONFIDENTIALITE, LA SECURITE

- Les réglementations comme les expériences du marché sont vaines si elles ne sont pas corrélées à la **sécurité logicielle et physique** qui doit entourer les données, contre les risques de fuite, détournement ou divulgation

- La sécurité logicielle n'est que rarement l'objet de textes réglementaires, car elle évolue sans cesse. Il existe des **normes**, qui peuvent servir de référence, ou d'exigence contractuelle.

- Certaines réformes passées imposent toutefois de la sécurité logicielle : notion d'**OIV**, **devoir d'alerte en cas de fuite de données pour les FAI**, etc.

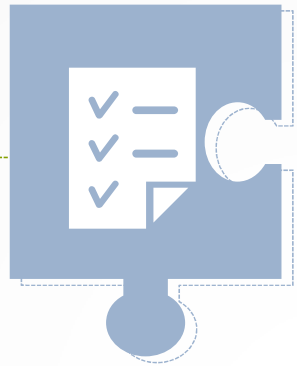
- La localisation des datacenters est importante, mais tout autant que (i) le déploiement d'une sécurité effective et (ii) la mise en œuvre de procédures conformes aux exigences réglementaires européennes.

- **Le risque zéro n'existe pas.**

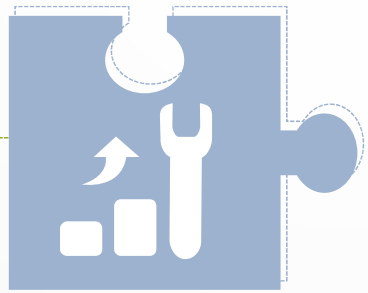
- **La sécurité procède moins d'exigences légales que de normes préconisées par l'état de l'art. La confidentialité des données est une question juridique, mais également technique et dans l'attente de futurs systèmes innovants (*Privacy by Design, Vendor Customer Relationship, etc.*) administrations et entreprises en restent responsables.**

# MAIS QUELLE SECURITE, POUR QUELLES DONNEES ?

- **La nécessité de connaître ses données**
  - **Analyse de risques** (préconisée par les normes ISO par exemple)
  - **Classification** des données de l'entreprise selon leur criticité
  - Définir une **Politique de Sécurité des Données**



- **Savoir évoluer dans la jungle des normes techniques**
- Convenir par contrat la conformité aux **normes pertinentes** (ISO 27001, SSAE, RGS, etc.)
- Prévoir les facultés d'**audit**
- Contrôler la **localisation des données**
- **Contractualiser** le respect de la législation européenne



- **Faire des choix de confidentialité, et donc de sécurité PERTINENTS, en recourant aux services d'un professionnel :**
- **Chiffrer** les données ? **Chiffrer** ou pas les communications (VPN) ?
- Recourir aux dispositifs de sécurité innovants (*UTM, cloud hybride, etc.*)
- Encapsuler les données personnelles dans un **« hub contractuel »** assurant le traitement conforme de bout en bout (*CCT, BCR, etc.*)
- Assurer que le **niveau « adéquat » de protection** est déployé sur toute la **chaine des intervenants**
- **Anonymiser** les données personnelles (*chaque fois que leur identification est dispensable, principe de « **Security By Default** »)*
- Concevoir des produits et services qui prennent techniquement en compte l'impératif de confidentialité des données (« ***Privacy By Design*** »)
- Prévoir des **procédures de signalement** et de sanctions internes en cas de non-respect

# LA SECURITE DES DONNEES

## Le Plan d'Assurance Sécurité

1. Elément parfois demandé par le Client si la prestation touche à un point névralgique de son SI ou de ses données, et systématiquement débattu s'il s'agit d'intégrer des services applicatifs en Cloud
2. Le Prestataire a grand intérêt à définir un **PAS standard** pour y stipuler notamment, en fonction de la nature du chantier, les éléments suivants, et éviter ainsi que le Client lui impose lui-même le respect de sa propre PSSI par exemple :

1. Les rôles assumés par chacun (RACI)
2. La localisation et la sécurisation des **datacenters** concernés
3. La gestion des **habilitations** et la **traçabilité** des accès
4. Les **référentiels techniques** de sécurité (souvent par application des normes ISO2700X, SOC I & II…)
5. Les indications sur le **chiffrement** de certaines données sensibles
6. La possibilité **d'audits de sécurité** et de contrôle de conformité aux normes techniques et/ou exigences légales.
7. Les outils de **sécurité** mis en œuvre
   *(sauf SaaS tiers complet)*
8. Les modalités **d'hébergement** distant et/ou **dédié**
9. La sécurisation des sessions, les **logs de connexion**
10. Les procédures de prévention des accès, de **monitoring**, de crash recovery, de redondance et de **sauvegardes**, de rétablissement de service (**SLA**), de reconstitution des données
11. La politique de **protection des données personnelles** si elles sont concernées

**Thomas Beaugrand**
Avocat **Staub & Associés**
89, bd Haussmann - 75008 Paris
+33 1 47 42 47 42
www.staub-associes.com

STAUB & ASSOCIÉS
société d'avocats

Design : WebhelpOffice, Paris