

**ALLEN & OVERY**

*Cloud computing*  
*Des risques et des solutions*

**CONFÉRENCE EUROCLOUD, 26 FÉVRIER 2013**

**CYRIL PIERRE-BEAUSSE**

---



## INTRODUCTION

### L'INFORMATION DANS L'ENTREPRISE

## *Double mouvement paradoxal*

VIRTUALISATION ET DÉCENTRALISATION CROISSANTES  
DU PATRIMOINE INFORMATIONNEL DE L'ENTREPRISE

L'entreprise dépend de plus en plus de ses données, mais pression croissante  
à la réduction des coûts, d'où l'attrait pour le cloud

RÉGULATION ET EXIGENCES CROISSANTES EN MATIÈRE DE SÉCURITÉ  
ET DE CONTRÔLE DE L'INFORMATION

Pression croissante sur les entreprises, triomphe de  
l'approche-risque, sanctions de plus en plus élevées,  
régulation plus forte



**ALLEN&OVERY**

## INTRODUCTION

### CONTEXTE LUXEMBOURGEOIS

## *Luxembourg: sensibilité particulière*

#### SECTEUR FINANCIER

secret professionnel et règles de conduite

#### CIBLE D'ATTAQUES EXTERNES

intelligence économique, espionnage financier et industriel

#### HOSTILITÉ D'AUTRES ÉTATS

tentatives d'intimidation, de corruption par des autorités étrangères

#### UN OBJECTIF AMBITIEUX

devenir le coffre-fort numérique de l'Europe

#### POLITIQUE VOLONTARISTE

investissements en infrastructures (ex. LuxConnect)

législation audacieuse (ex. eArchivage, cloud computing)



## PROBLÉMATIQUE

RAPPEL, OBLIGATION DE SÉCURITÉ

### *Obligation de sécuriser l'information*

SECTEURS RÉGLEMENTÉS: DISPOSITIONS SPÉCIFIQUES

- secteur financier: secret professionnel, exigences opérationnelles
- communications électroniques: confidentialité des communications, sécurité et intégrité des réseaux
- régulateurs (CSSF, CaA, ILR) peuvent imposer des règles spécifiques

DONNÉES PERSONNELLES: DISPOSITIONS GÉNÉRALES

- champ d'application très large
- dispositions très précises quant aux mesures de sécurité
- sanctions pénales en cas de défaillance



**ALLEN&OVERY**

## PROBLÉMATIQUE

### RAPPEL, OBLIGATION DE SÉCURITÉ

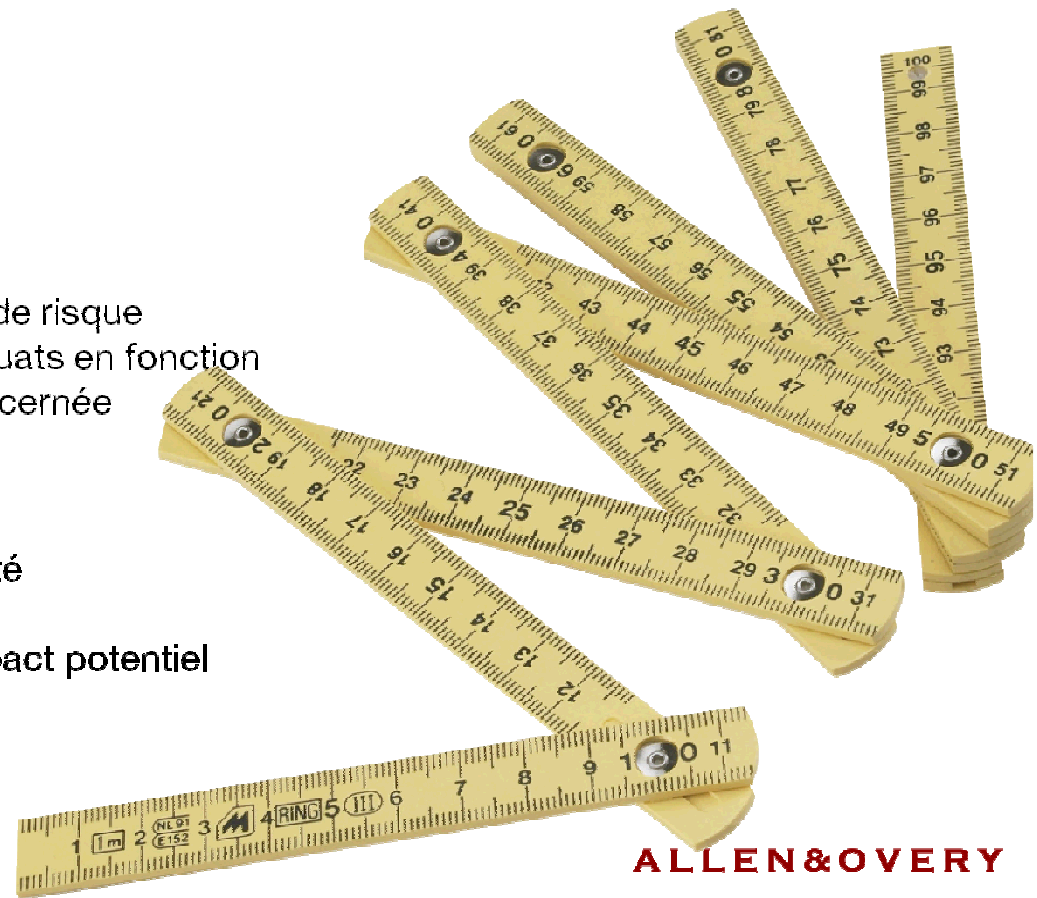
## *Deux règles d'or*

#### CONTRÔLER SON INFORMATION

- Maîtriser sa chaîne de l'information
- Traiter toute externalisation comme source de risque
- Mettre en place les outils contractuels adéquats en fonction de la sensibilité/criticité de l'information concernée

#### CONNAÎTRE SON RISQUE

- Identifier et documenter les risques
- Réduire son risque via la politique de sécurité
- Déterminer son risque résiduel
- Documenter probabilité d'occurrence et impact potentiel
- Valider le risque résiduel



**ALLEN&OVERY**

*Conflit apparent  
entre respect de ces principes et recours au cloud...*

*Quelles solutions?  
Bien choisir son prestataire  
et soigner le cadre contractuel*



# DONNÉES PERSONNELLES

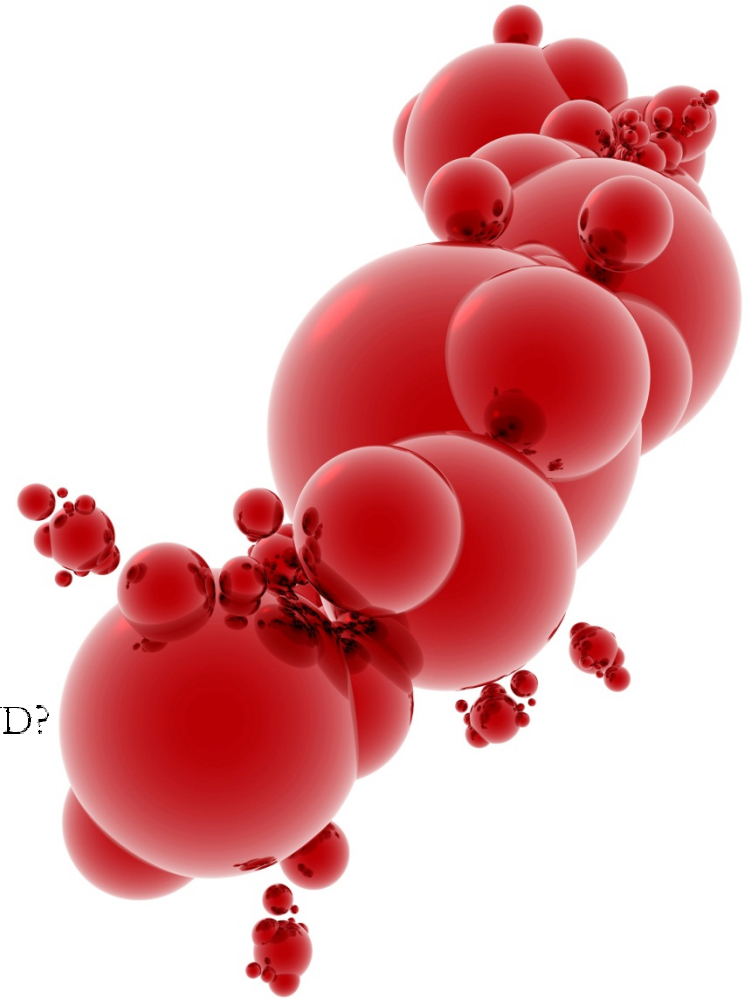
A photograph of a chessboard with several pieces. In the foreground, a black king and a black knight are standing. Behind them, a white king and a white pawn are also standing. In the center, a white king and a white pawn are lying on their sides, suggesting a game in progress or a checkmate. The background is a plain white surface.

ALLEN&OVERY

**DONNÉES PERSONNELLES**  
**HYPOTHÈSE**

*Un utilisateur place  
des données personnelles  
sur le cloud*

QUI EST RESPONSABLE DEVANT LA LOI?  
QUID DES TRANSFERTS DE DONNÉES VIA LE CLOUD?  
QUE DIT LA LOI?



**ALLEN&OVERY**



## DONNÉES PERSONNELLES CLOUD & CONFORMITÉ

### *Le cloud est-il compatible avec la loi?*

PAS D'INTERDICTION OU DE RESTRICTION  
A PRIORI MAIS ATTENTION...

À LA RESPONSABILITÉ DU TRAITEMENT  
Qui est responsable au regard de la loi?  
Quels sont les rôles des différents intervenant?

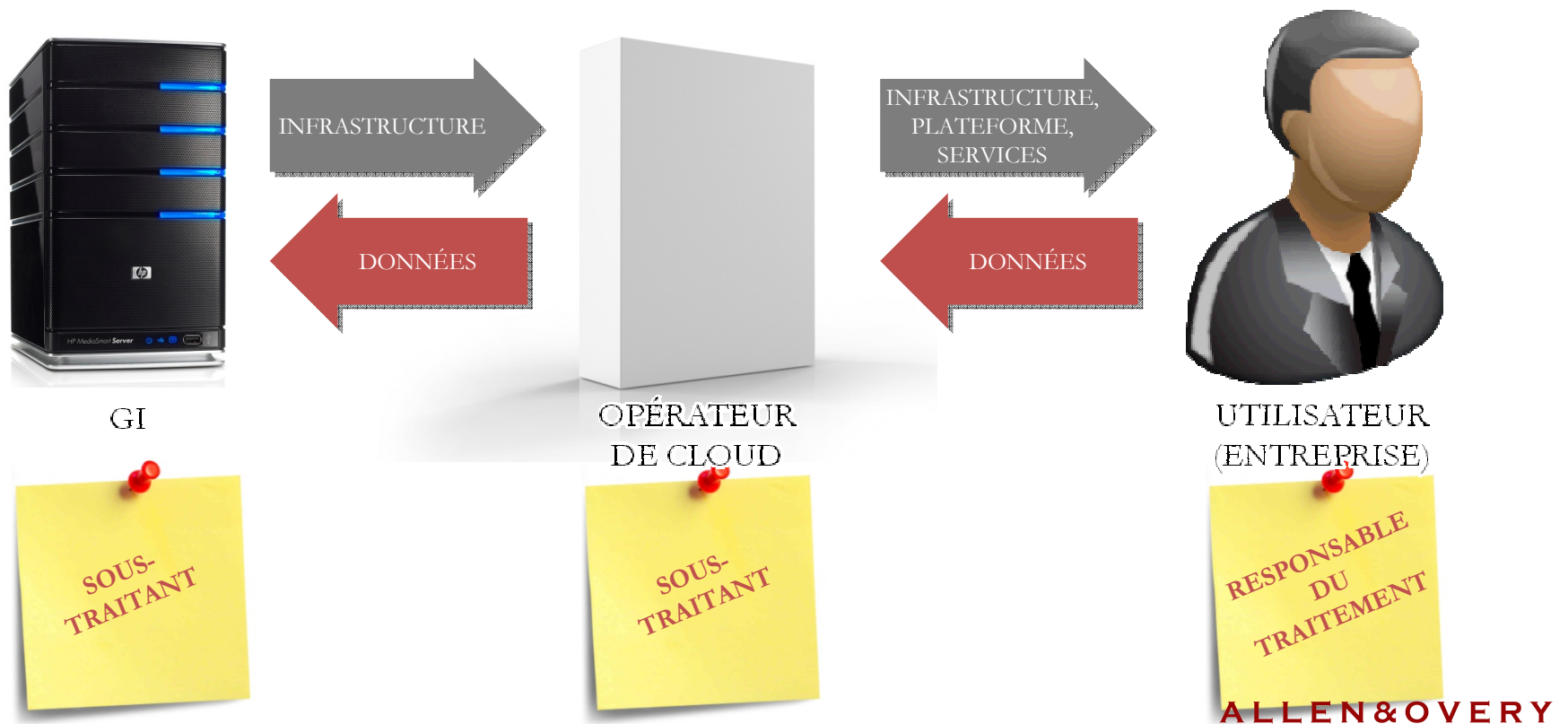
AU TRANSFERT DE DONNÉES PERSONNELLES  
Au sein de l'UE et en dehors...

À LA SÉCURITÉ DES DONNÉES  
Quelles obligations en matière de sécurité?



ALLEN&OVERY

## DONNÉES PERSONNELLES SCENARIO GÉNÉRAL



\* L'opérateur ne prend aucune décision/initiative sur les données

# *Attention à la prise de décision par l'opérateur de cloud!*

DÉPLACEMENT DES DONNÉES (ex. d'un GI à un autre)

RÉTENTION DES DONNÉES (ex. refus de procéder à la destruction ou restitution demandée par le client)

DESTRUCTION DES DONNÉES (contre la volonté du client)

TOUT AUTRE ACTE DE TRAITEMENT NON DEMANDÉ PAR LE CLIENT

(ex. consultation, utilisation, extraction, transmission, divulgation)



RISQUE DE REQUALIFICATION DE L'OPÉRATEUR EN RESPONSABLE DE TRAITEMENT






MISE EN CONFORMITÉ À LA LOI DIFFICILE (IMPOSSIBLE?)

**ALLEN&OVERY**

## DONNÉES PERSONNELLES

### APPLICATION TERRITORIALE DE LA LOI

*La loi luxembourgeoise s'applique si...*

				
GI		OPÉRATEUR DE CLOUD		UTILISATEUR (ENTREPRISE)
N'importe où dans le monde		N'importe où dans le monde		Luxembourg
N'importe où dans le monde		Moyens de traitement à Luxembourg (hors transit)		N'importe où dans le monde
Luxembourg		N'importe où dans le monde		N'importe où dans le monde

ALLEN&OVERY

## DONNÉES PERSONNELLES DROITS DES PERSONNES

### *Transparence et assistance*

L'OPÉRATEUR DE CLOUD EST UN SOUS-TRAITANT  
ET NE PEUT PRENDRE DE DÉCISION AUTONOME  
QUANT AUX DONNÉES (ex. transfert, modification, destruction)

L'UTILISATEUR EST RESPONSABLE  
DEVANT LES PERSONNES CONCERNÉES  
ET DOIT LEUR PERMETTRE D'EXERCER LEURS DROITS:

- droit d'accès
- droit de rectification
- droit d'opposition (le cas échéant)

L'OPÉRATEUR DE CLOUD DOIT (DEVRAIT) ASSISTER L'UTILISATEUR



ALLEN&OVERY



A close-up photograph of a red and black pencil lying diagonally across the frame. The pencil's lead tip is broken and jagged. To the left of the pencil's tip, there is a small, dark, conical pile of lead shavings. The background is a plain, light-colored surface.

# L'OUTIL CONTRACTUEL

ALLEN&OVERY



## SOLUTIONS

### L'OUTIL CONTRACTUEL

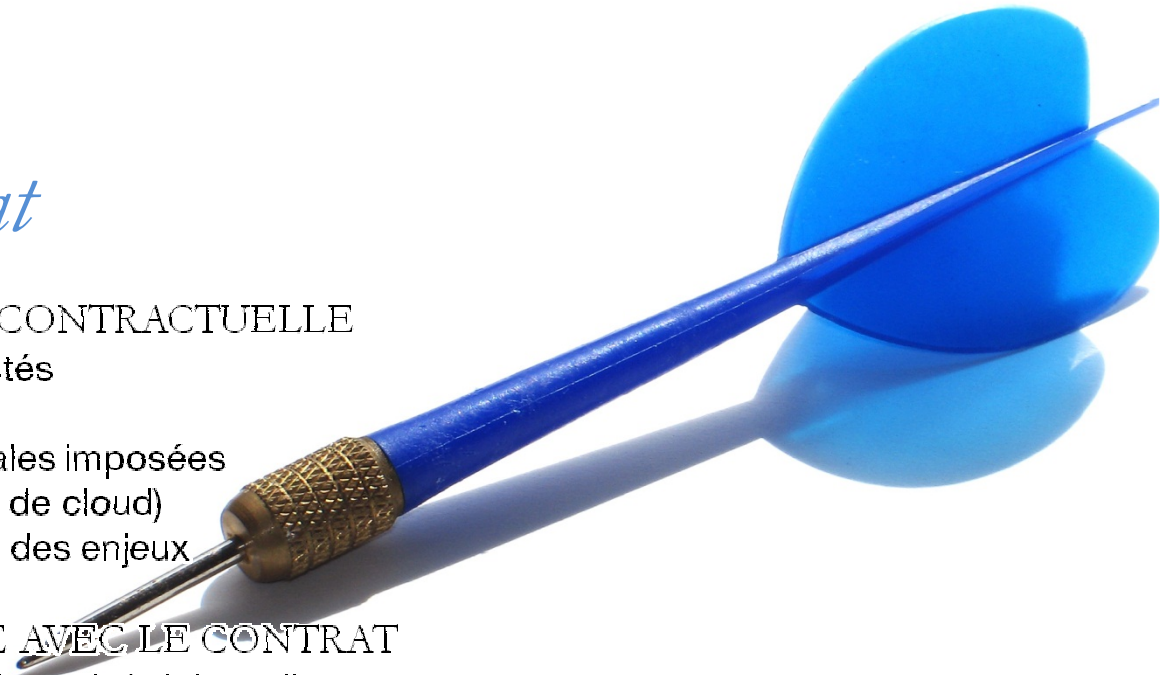
## *Un projet, un contrat*

#### ATTENTION À LA MÉDIOCRITÉ CONTRACTUELLE

- Chaque projet présente des spécificités et porte des risques différents
- Prudence avec les conditions générales imposées par le prestataire (la règle en matière de cloud)
- Soupeser chaque clause en fonction des enjeux

#### APRÈS L'ACCORD, IL FAUT VIVRE AVEC LE CONTRAT

- Les personnes concernées (ex. chef de projet) doivent lire et comprendre le contrat (ex. modes de communication)
- L'input de toutes les parties concernées est précieux (legal, compliance, IT, RSSI, chargé de la protection des données)
- Au moins une personne doit lire et comprendre l'intégralité du contrat (rare en pratique)



**ALLEN&OVERY**

## SOLUTIONS

### CHOISIR SON PRESTATAIRE

## *Contrôle du prestataire*

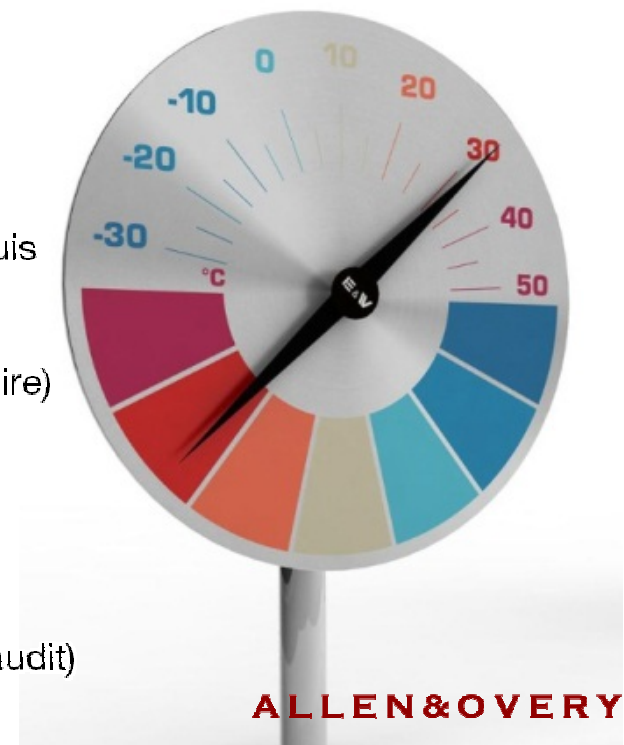
### QUALITÉS PROPRES AU PRESTATAIRE

Engagements sur:

- la compétence du prestataire (induit), ses capacités en termes de ressources humaines, infrastructure et patrimoine intellectuel
- le cas échéant, obtention/détention et maintien des agréments requis
- caractère intuitu personae, «change of control»
- sa coopération (avec le régulateur, ex. CSSF, maintien d'un accès effectif aux données et aux locaux du prestataire)

### EVALUATION DU PRESTATAIRE

- Mise en place de méthodes d'évaluation appropriées:  
SLO (Service Level Objectives), KPI (Key Performance Indicators),  
SLO (Service Level Reporting)
- Surveillance de l'exécution des fonctions externalisées (reporting, audit)



## SOLUTIONS

### L'OUTIL CONTRACTUEL, PRINCIPES IMPORTANTS

#### *Sous-traitance en cascade*

##### ENCADREMENT DE LA SOUS-TRAITANCE

- **Transparence:** toute sous-traitance doit être connue
- **Contrôle:** tout sous-traitant doit être soit mentionné dans le contrat, soit agréé ultérieurement au moyen d'un mécanisme précis
- **Due diligence** sur le sous-traitant doit pouvoir être réalisé au préalable, implique un délai raisonnable
- **Données personnelles:** la CNPD impose:
  - mécanisme d'approbation par le responsable du traitement
  - délai raisonnable pour due diligence (ex. 10/15 jours)
- **Réplication de toutes les obligations contractuelles** sur le sous-traitant (ex. confidentialité, audit)  
+ maintien de la responsabilité du prestataire



**ALLEN&OVERY**

## SOLUTIONS

### L'OUTIL CONTRACTUEL, PRINCIPES IMPORTANTS

#### *Continuité et réversibilité*

##### GÉRER LA CONTINUITÉ PENDANT LA RELATION

- Vérifier les mesures (BCP, DRP) du prestataire
- Contrôler la compatibilité avec la politique de sécurité, les besoins de l'entreprise, les obligations réglementaires
- Effectuer des tests de mise en œuvre

##### GÉRER LA SORTIE DE RELATION

- Evaluer l'impact d'une résiliation sur la continuité des opérations
- Vérifier les options de réversibilité
- Prévoir une «exit procedure» et une clause d'assistance du prestataire



**ALLEN&OVERY**

**CLOUD & CONFORMITÉ**  
TRANSFERTS OFFSHORE

*Confidentialité et risque d'interception*

HORS DU LUXEMBOURG, POINT DE CERTITUDE!

Application de législations étrangères régaliennes (ex. Patriot Act)

Pre-trial discovery, eDiscovery

Interceptions de communications

Perquisitions chez les GI ou sous-traitants

PRÉCÉDENTS EN MATIÈRE DE TÉLÉCOM

Perquisitions ou interceptions de communications

permettent de contourner la procédure normale

par voie de commission rogatoire internationale



**ALLEN&OVERY**

## CLOUD & CONTRAT PEUT-ON NÉGOCIER?

### *Flexibilité zéro?*

UN BUSINESS MODEL QUI LAISSE  
THÉORIQUEMENT PEU DE PLACE À LA FLEXIBILITÉ  
Coûts bas permis par des économies d'échelle, donc standardisation  
L'offre jumelée de services provoque souvent une distorsion  
entre l'offre de l'opérateur et les attentes de l'utilisateur

#### TAKE IT OR LEAVE IT

Position standard de la plupart des opérateurs  
Il n'y a aucune raison d'accepter un diktat au prétexte qu'il s'agit de cloud...



ALLEN&OVERY



**ALLEN & OVERY**

*Questions?*



**CONFÉRENCE EUROCLOUD, 26 FÉVRIER 2013**

**CYRIL PIERRE-BEAUSSE**

---