Règlement UE 2016/679 du 26 avril 2016

Règlement général sur la protection des données (RGPD)

Problématiques liées au transfert de données personnelles : Atelier de travail

dcl avocats / Luxembourg

INTRODUCTION

Cadre Légal

- Règlement européen assure une harmonisation maximale des règles européennes en matière de protection de données personnelles
- RGPD ne vise expressément que la problématique du transfert vers un pays tiers
- Chapitre V du RGPD (article 44 à 50) et article 13

Plan de l'atelier

- Rappel des principes RGPD (définitions, champ d'application, conditions)
- Flux transfrontaliers
- Secret professionnel et transfert

DEFINITION

Transfert (aucune définition dans le règlement)

CNIL (Guide « Les transferts de données à caractère personnel hors union Européenne », ed. 2012)

Un transfert de données personnelles est caractérisé lorsque ces données sont transférées depuis le territoire européen vers un ou des pays non membres de l'U.E. ni de l'E.E.E. Le transfert peut s'effectuer par communication, copie, déplacement de données par l'intermédiaire d'un réseau (accès à distance à une base de données) ou d'un support à un autre, quel que soit le type de support (ex: d'un disque dur d'ordinateur à un serveur) qui sont destinées à faire l'objet d'un traitement

Exemples:

- centralisation intra-groupe dans un pays tiers de la base de données de gestion de commandes des clients et facturation des clients (ou gestion des données RH)
- sous-traitance d'un service support clients en Inde

CHAMP D'APPLICATION

Sont concernés par les restrictions au transfert (art. 44)

- Responsable de traitement situé dans l'U.E.
- Sous-traitant situé dans l'U.E.

Mais aussi

Sous-traitant (d'un responsable localisé en U.E.) localisé hors U.E. vers un autre sous-traitant localisé dans un autre pays tiers : sous-traitance en cascade

CONDITIONS

Conditions de licéité de tout transfert (art. 44 et s.)

- Transfert fondé sur une décision d'adéquation (art. 45)
- Transfert reposant sur la mise en place de garanties appropriées (art. 46) e.a. transfert effectué dans le cadre de règles d'entreprise contraignantes (art. 47)
- Transfert reposant sur des dérogations dues à des situations particulières (art. 49)

Transfert fondé sur une décision d'adéquation

Cas particulier du transfert vers les Etats Unis - Privacy Shield (12/7/2016) - mécanisme d'auto-certification

Les entreprises US ayant adhéré à ce mécanisme sont considérées comme offrant un niveau de protection adéquat

Attention

- Ce mécanisme ne concerne ni les banques, ni les compagnies d'assurance, ni les opérateurs téléphoniques
- Certification annuelle => prévoir une procédure interne pour vérifier si le destinataire est toujours titulaire de la certification
- Certification délivrée pour certaines données seulement
- Informer la personne concernée

CONDITIONS

Transfert reposant sur la mise en place de garanties appropriées

- Contrat organisant les relations entre deux responsables ou la sous-traitance stipulant expressément les clauses types prévues par la Commission
- Contrat organisant les relations entre deux responsables ou la sous-traitance stipulant des clauses *adhoc* sans reprendre les clauses types mais sous réserve de l'autorisation de la CNPD
- La mise en place de règles d'entreprise contraignantes
- L'adhésion et le respect d'un code de conduite ou d'une certification
- etc.

CONDITIONS

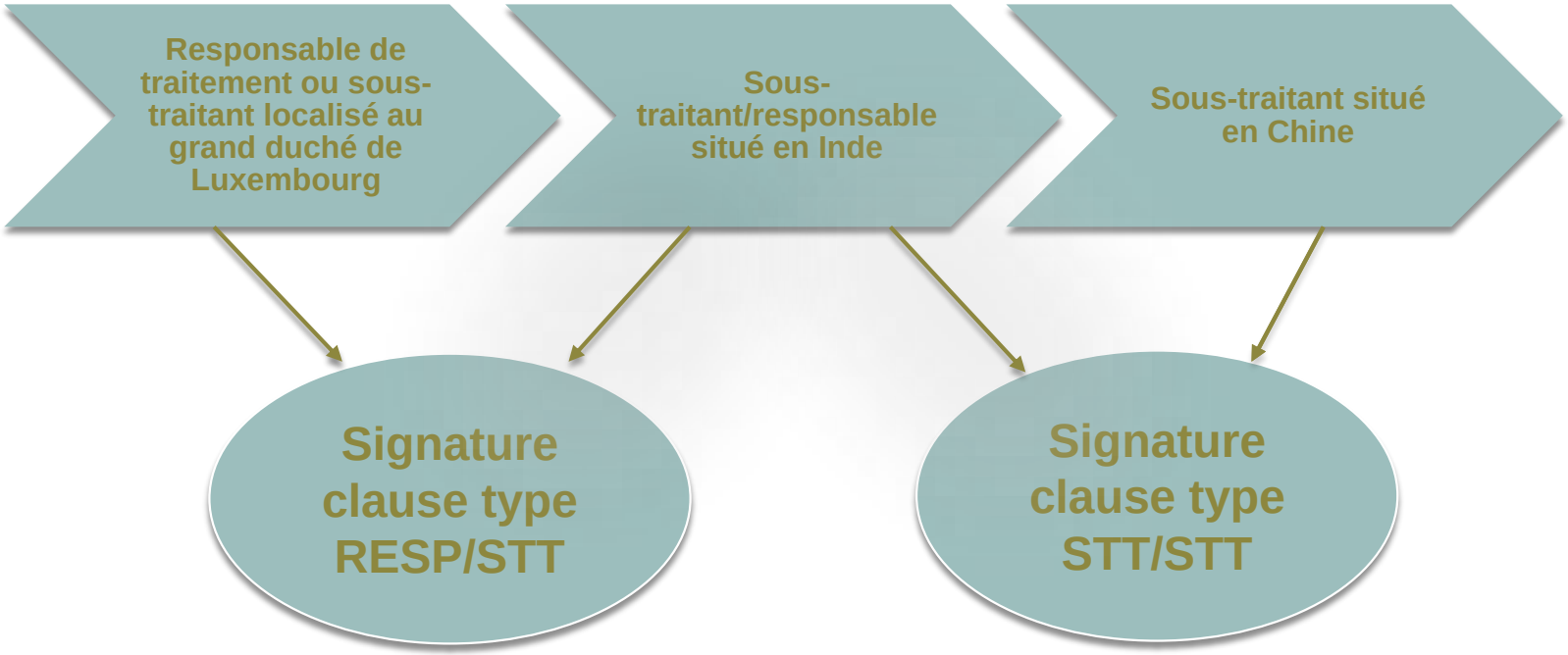
Contrat stipulant expressément les clauses types prévues par la Commission

1ère étape : identifier avec précision la relation contractuelle entre les 2 (ou 3) entités : responsable/responsable ou responsable/sous-traitant
Différences : régime de responsabilité, règlement des litiges, droit d'accès et coopération entre régulateurs

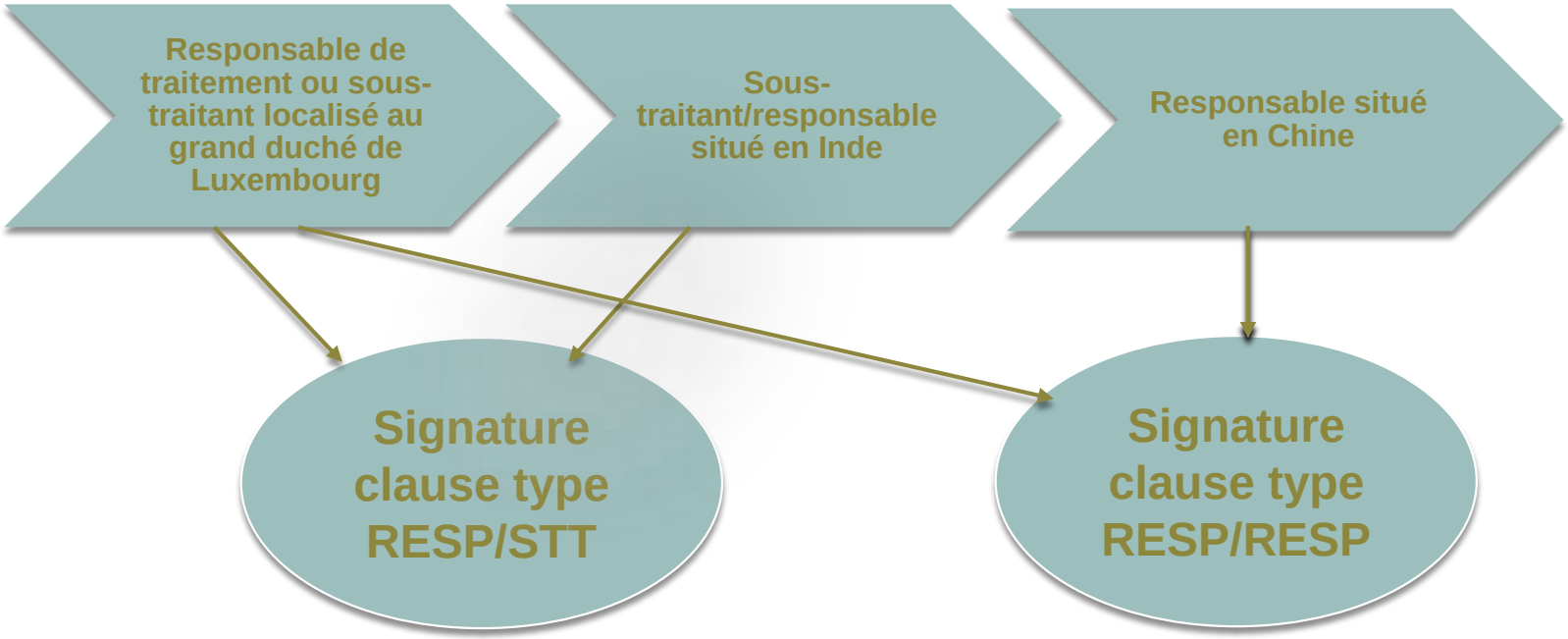
2ème étape : lire, comprendre et compléter les clauses avant de les insérer dans le contrat (conseil : les reprendre *in extenso*)

Contrat-type publié par l'ICO (UK), disponible sur le site de la CNPD

Exemples pratiques d'hypothèse de transfert



Exemples pratiques d'hypothèse de transfert



CONDITIONS

Règles d'entreprise contraignantes (BCR) (art. 4.20 (définition) & art. 47 (contenu))

Règles internes suivies par un responsable de traitement ou un sous-traitant établi dans l'U.E. pour tout transfert ou ensemble de transferts **vers une entité du groupe** (ou **d'un groupe d'entreprises engagées dans une activité économique conjointe**, ex : 2 groupes actifs dans le secteur des transports, telecoms) située dans un **pays tiers**

Attention

Les BCR doivent être validées par la CNPD pour pouvoir justifier un transfert « *libre* » vers une entité localisée dans un pays tiers

CONDITIONS

Transfert fondé sur une ou plusieurs dérogations pour des situations particulières (art. 49) (interprétation stricte)

- Consentement explicite au transfert envisagé reposant sur une information préalable des risques liés au transfert vers un pays tiers

- Nécessaire à l'exécution d'un contrat ou à la mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée (ex : agence de voyage, réservation de nuitées d'hôtels en Inde)

- Nécessaire à la conclusion ou exécution d'un contrat conclu dans l'intérêt de la personne concernée (ex : organisation d'un rapatriement), etc.

Cette dérogation ne peut être utilisée pour des transferts massifs, répétitifs ou structurels (Groupe de travail de « Article 29 », ci-après Groupe 29). Cette dérogation ne pourrait donc pas être utilisée pour justifier des transferts réalisés dans le cadre d'une sous-traitance

Consentement explicite

Consentement défini à l'article 4.11: manifestation de volonté **libre**, **spécifique**, **éclairée** et **univoque** par laquelle une personne accepte, par une déclaration ou par un acte positif clair (consentement exprès), que ses données personnelles soient traitées

Dans l'hypothèse d'un transfert vers un pays tiers, l'information doit contenir e.a. les risques accrus du fait de l'absence de décision d'adéquation et de garanties appropriées ainsi que les circonstances particulières du transfert

Consentement explicite implique une **exigence supplémentaire** quant à l'expression du consentement exprès : une absence de doute totale sur l'expression du consentement, justifiée par une nécessité impérieuse de protection renforcée du fait des données concernées ou de l'utilisation de ses données ou de leur destination

Selon les explications du Groupe 29, la personne concernée doit donner son consentement exprès de telle manière qu'aucun doute ne subsiste sur l'expression de volonté libre, éclairée, univoque et spécifique de la personne

La preuve de l'existence du consentement explicite repose sur le responsable du traitement

Expression du consentement explicite

- Mention manuscrite (à la manière de celle demandée pour le cautionnement)
- Un formulaire électronique disponible sur un site internet ou envoyé par email par le responsable rempli par la personne concernée, signé (**manuscritement et électroniquement**) et renvoyé par elle (*réserve sur la véracité*)
- Une expression claire faite oralement et enregistrée (si toute les conditions exigées pour l'expression du consentement sont clairement établies)
- Confirmation en pressant un bouton lors d'une conversation téléphonique (réserve)

Exemples

- Site internet : l'utilisation de cases à cocher oui/non suivant immédiatement l'expression « ***j'accepte expressément*** *le traitement de mes données personnelles dans les conditions décrites précédemment* » serait suffisante à la condition que les informations reprises sur la même page détaillent clairement et de manière exhaustive l'ensemble des informations nécessaire à l'octroi ou au refus du consentement (scrolling obligatoire de la page ajoute une sécurité)

Exemples

- Une société envoie un email à son client l'informant que pour des raisons de centralisation de la gestion du fichier client, ses données vont être transférées en Inde. La société donne dans cet email l'ensemble des informations nécessaire au consentement éclairé, libre, explicite et univoque du client et lui demande d'accepter le traitement de ses données personnelles par retour d'email en reprenant expressément la mention suivante « ***j'accepte expressément*** *le traitement de mes données personnelles dans les conditions décrites dans votre email repris ci-dessous ».* Dès réception de cet email d'acceptation, la société génère un email automatique contenant un lien sur lequel le client doit cliquer pour vérifier le consentement explicite et le démontrer

- Une société de télécommunication informe ses salariés que le traitement des données RH se fera désormais depuis la maison-mère située en Californie. Une lettre-avenant (au contrat de travail) reprenant toutes les informations nécessaires au consentement est remise en main propre ou envoyée à chaque employé leur demandant de parapher chaque page, de signer l'avenant et d'apposer la mention manuscrite « ***j'accepte expressément*** *le traitement de mes données personnelles dans les conditions décrites dans cet avenant) »* suivie de leur signature (acceptation expresse), et de renvoyer/remettre l'original et une copie scannée au département RH

LES FLUX TRANSFRONTALIERS INTRA-GROUPE

Définition de la notion de groupe (article 4.19)

Le groupe d'entreprises est constitué de l'entreprise qui exerce le contrôle (influence dominante) et les entreprises qu'elle contrôle

Prise en compte de la spécificité des groupes d'entreprises ?

Dans le cadre des transferts vers des pays tiers, le RGPD n'a pris en considération l'existence d'un groupe de sociétés que pour l'exception à l'interdiction des transferts vers les pays tiers relative à la mise en place de BCP (c.f. supra)

Cette volonté de ne pas créer d'exception pour les transferts de données intra-groupe (considérant 48 RGPD) a été partagée par le législateur au sujet de la loi du 27 février 2018 portant mise en œuvre du règlement (UE) 2015/751 du Parlement européen et du Conseil du 29 avril 2015 relatif aux commissions d'interchange pour les opérations de paiement liées à une carte

SECRET PROFESSIONNEL ET TRANSFERT

Problématiques liées au secret professionnel et à l'application des règles édictées par RGPD

Problématiques générales

- Contrôle de la CNPD
- Droit à l'information
- Droit d'accès
- Assurance santé
- Sous-traitance pour les entreprises des secteurs règlementés (secteur des assurances, secteur financier, secteur des services de paiement)

ZOOM SUR LA SOUS-TRAITANCE

Pour les entreprises non régulées : renvoi aux développements précédents

Pour les entreprises régulées : Application cumulative des textes spécifiques encadrant la sous-traitance et de l'article 49 RGPD

- Secteur des assurances (article 300 de la loi sur le secteur des assurances)
- Secteur financier (article 41 de la loi sur le secteur financier)
- Secteur des services de paiements (article 30 de la loi sur les services de paiements)

SECRET PROFESSIONNEL ET TRANSFERT

Nouvelle exception à l'obligation au secret professionnel (art. 300 FSA, art. 41 LSF et art. 30 LSP)

L'obligation au secret n'existe pas à l'égard des **entités qui sont en charge de la prestation de services sous-traités** (…), **dans la mesure où le preneur d'assurance a accepté, conformément à la loi ou selon les modalités d'information convenues entre parties**, la sous-traitance des services sous-traités, le type de renseignements transmis dans le cadre de la sous-traitance et le pays d'établissement des entités prestataires des services sous-traités. Les personnes ayant ainsi accès aux renseignements visés au paragraphe (1) doivent être soumises **par la loi à une obligation de secret professionnel ou être liées par un accord de confidentialité**

Remarque

L'exception ne distingue pas selon que le sous-traitant soit localisé dans l'U.E. ou non. Aussi en cas de sous-traitance vers une entité européenne, les exigences sont-elles plus strictes que celles de RGPD alors qu'elles se superposent pour une sous-traitance vers un sous-traitant situé hors U.E.

SECRET PROFESSIONNEL ET TRANSFERT

Questions

- Signification concrète de « *selon les modalités d'information convenues entre parties* » ?
- Consentement tacite pour les transfert intra-U.E. possible ?
- Définition de l'accord de confidentialité : BCR ou définition civiliste ? Une simple clause de confidentialité stipulée dans un contrat de services (réglementant la sous-traitance) suffit-elle ?
- Droit applicable (clause de juridiction) à ces contrats de services

Questions concrètes secteur des assurances

- Nouveau preneur : modalité du consentement à la souscription et après
- Preneurs existants : quid si refus

POUR TOUTE QUESTION

Dorothée CIOLINO
Avocat aux Barreaux de Paris et de Luxembourg
ciolino@dclavocats.com

DCL Avocats S.à r.l.
9, Avenue Jean-Pierre Pescatore
L-2324 Luxembourg
Tél. + 352 26 00 11 1
Fax +352 27 12 51 81
www.dclavocats.com