GDPR & LCBFT: Comment les concilier?

Elisabeth GUISSART
Avocat à la Cour

Chambre de commerce – 8 décembre 2020

DEUX REGLEMENTATIONS INCONCILIABLES?

Des logiques opposées

- GDPR: volonté de limiter les traitements à ce qui est nécessaire. Respect de la vie privée.
- LCBFT: volonté de connaitre le client et de documenter

Mais des réglementations conciliables

- GDPR n'empêche pas de collecter et traiter des données à des fins LCBFT
- GDPR donne un cadre
- Loi 2004 tient compte de GDPR

LCBFT

PLAN

1 GDPR: CONTEXTE
2 GDPR: GRANDS PRINCIPES
3 CARTOGRAPHIER
4 INFORMER
5 DROIT D'ACCÈS
6 PRESTATAIRES EXTERNES

1

GDPR: CONTEXTE

PROTECTION DES DONNÉES
CONTEXTE HISTORIQUE

20 ans de règles européennes sur les données personnelles

- directive 95/46 en 1995
- directive = lois nationales = variations locales
- Luxembourg a transposé en 2002
  en essayant d'être premier de la classe (surveillance)

GDPR

- règlement UE = harmonisation
- objectif: faire de la protection des données
  un élément de la gouvernance des organisations
- règles plus complexes, sévérité accrue

PROTECTION DES DONNÉES
POURQUOI?

Pourquoi GDPR? Les raisons officielles

- Le précédent cadre légal UE date de 1995
- Pas de prise en compte d'internet, des *smartphones*
- Modernisation du cadre légal
- Adaptation aux traitements nouveaux
  (ex. géolocalisation, profilage)

PROTECTION DES DONNÉES
POURQUOI?

Pourquoi GDPR? Les autres raisons…

- TOUTES les organisations sont vulnérables à l'information, peu le reconnaissent et traitent leurs données en conséquence
- Illustrations régulières avec les *data breaches*:
  - risque pour la vie privée des personnes
  - risque réputationnel & économique pour l'organisation
- En cascade, un risque pour l'économie UE
- GDPR force les entreprises à:
  - connaître et maîtriser leurs données
  - les sécuriser et garantir leur protection
  - respecter les personnes concernées

2

GDPR: GRANDS PRINCIPES

GRANDS PRINCIPES

4 PRINCIPES CLES

1 Finalité

- traitement uniquement pour finalités déterminées, explicites, légitimes
- pas de traitement incompatible avec ces finalités

2 Pertinence

- données adéquates, pertinentes, non excessives / finalités
- données exactes et (si nécessaire) mises à jour

3 Rétention limitée

- données identifiant les personnes concernées conservées uniquement tant que nécessaires pour les finalités

4 Légitimité

GRANDS PRINCIPES
CLE DE VOUTE

PROPORTIONNALITE

- les moyens du traitement doivent être proportionnés à la finalité recherchée
- les actes de traitement doivent être nécessaires à atteindre la finalité recherchée

MINIMISATION

- ne collecter que ce qui est strictement nécessaire
- LCBFT: principe à garder aussi à l'esprit

GRANDS PRINCIPES

FINALITÉ

La finalité est le but recherché par le responsable du traitement et qui justifie le traitement

- les finalités doivent être déterminées à l'avance
- les finalités doivent être légitimes
- toutes les finalités doivent être divulguées (transparence)
- les données ne doivent pas être traitées ultérieurement pour des **finalités incompatibles**

«compatible»: ce à quoi la personne concernée peut raisonnablement s'attendre

PAS DE TRAITEMENT SECONDAIRE

LOI 2004

Art.3, (6bis), al.2 : « […] *Le traitement des données […] sur base de la présente loi pour toute autre finalité est interdit* »

GRANDS PRINCIPES
LÉGITIMITÉ: EN GENERAL

Un traitement «standard» est légitime si...

TRAITEMENT «STANDARD»
DONNÉES SENSIBLES
SECTEUR DE LA SANTÉ
DONNÉES JUDICIAIRES

- obligation légale
- intérêt public important
- contrat/mesures pré-contractuelles avec la personne concernée
- intérêt légitime du responsable /droits et libertés de la personne
- intérêt vital
- consentement de la personne concernée

GRANDS PRINCIPES
LÉGITIMITÉ: LCBFT

Un traitement «standard» est légitime si...

TRAITEMENT «STANDARD»
DONNÉES SENSIBLES
SECTEUR DE LA SANTÉ
DONNÉES JUDICIAIRES

- obligation légale
- intérêt public important
- contrat/mesures pré-contractuelles avec la personne concernée
- intérêt légitime du responsable /droits et libertés de la personne
- intérêt vital
- consentement de la personne concernée

Art. 43 4ème Directive LCBFT: « *Le traitement de données à caractère personnel sur la base de la présente directive aux fins de la prévention du blanchiment de capitaux et du financement du terrorisme visés à l'article 1er est considéré comme une question d'intérêt public au titre de la directive 95/46/CE* »

/c

GRANDS PRINCIPES
RETENTION LIMITEE

Les données personnelles ne doivent pas être conservées de manière indéfinie

- Cas où la loi fixe une durée maximum (rare)
- Cas où la loi fixe une durée minimum
- Cas où la loi ne dit rien (principe)

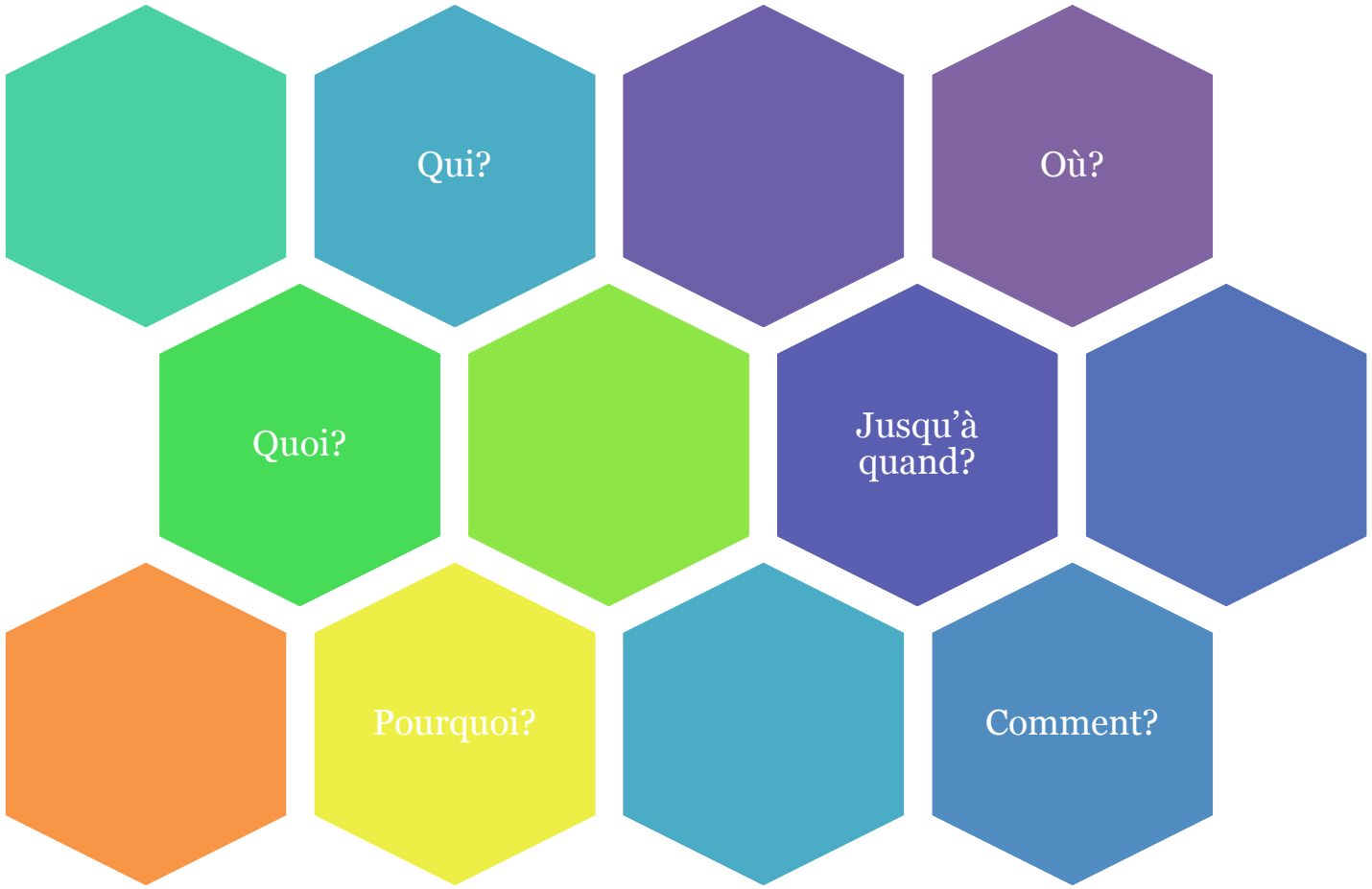
Art.3, (6), al.2 : 5 ans + 5 ans

Appréciation en fonction de la finalité

Penser en termes de cycle de vie !!

3 CARTOGRAPHIER

REGISTRE
OBJECTIFS



REGISTRE
FICHE: LCBFT

« photographie de la situation »

Données traitées

- Nom, prénom, telephone, adresse prof. + privée , date de naissance, données bancaires, ID, salaire, etc.

Personnes concernées

- Clients / prospects

Finalité

- LCBFT: obligation vigilance clientele, déclaration de soupçon, mise sous surveillance comptes ou clients, gel des avoirs

Support/Localisation

- Logiciels utilisés / pays

Transfert

- Personnes ayant accès aux données (interne et externe), destinataires (autorités), sous-traitants

4 INFORMER

DROITS DES PERSONNES CONCERNÉES
DROIT GÉNÉRAL À L'INFORMATION

Informations à communiquer

- identité du responsable
- finalités du traitement
- destinataires/catégories de destinataires
- caractère obligatoire/facultatif des questions, conséquences éventuelles défaut de réponse
- existence d'un droit d'accès/rectification

PREUVE

FORMER STAFF

ART. 13

+coordonnées DPO
+base juridique du traitement
+intérêt légitime poursuivi
+transfert vers pays tiers (niveau de protection local, mesures de sauvegarde)
+durée ou critères de rétention
+droit opposition
+droit effacement
+droit limitation
+droit retrait consentement
+droit réclamation/CNPD
+données requises par la loi
+contrat conditionné aux données
+info sur décisions automatisées
+info sur profilage
+info logique sous-jacente & conséquences

DROITS DES PERSONNES CONCERNÉES
DROIT GÉNÉRAL À L'INFORMATION: art. 14

Données reçue d'un tiers?

- catégories données concernées
- source de provenance des données
- max. 1 mois après obtention MAIS
  - au plus tard lors de la 1ère commun communication commerciale)
  - au plus tard lors du 1er transfert (si données à un autre destinataire)

DROITS DES PERSONNES CONCERNÉES
DROIT GÉNÉRAL À L'INFORMATION: LCBFT

LOI 2004

Art.3, (6bis), al.3 :

- avant de nouer une relation ou exécuter une transaction

- avertissement général concernant obligations LCBFT

5 DROIT D'ACCÈS

DROITS DES PERSONNES CONCERNÉES

DROIT D'ACCÈS

La personne concernée a normalement accès à toutes les informations la concernant

- accès illimité en théorie + copie
- exceptions (limitées) existent
- prudence recommandée avant tout refus de communiquer les données ou en cas de dissimulation de données
- communication logique qui sous-tend tout traitement avec décisions automatisées (y compris profilage)

GRATUIT

DROITS DES PERSONNES CONCERNÉES

DROIT D'ACCÈS: LIMITATION LCBFT

LOI 2004

Art.3, (6bis), al.4 : LIMITATION

Le RT limite ou diffère le droit d'accès

- Eviter de compromettre mesures prévues par LCBFT
- Pas d'accès à déclaration soupçon (consid. 46 4ème Directive LCBFT)
- Doit indiquer motif de refus de donner accès (art. 12 §4 GDPR)
- Recours possible devant CNPD

6

UTILISATION PRESTATAIRES EXTERNES

LES DIFFÉRENTS INTERVENANTS DANS GDPR

PROTECTION DES DONNÉES
INTERVENANTS

Responsable du traitement

Personne physique ou morale, autorité publique, service ou tout autre organisme qui, seul ou conjointement avec d'autres, **détermine les finalités et moyens** du traitement.

Il est crucial de bien identifier le responsable

Pluralité de responsables du traitement possible

/c

PROTECTION DES DONNÉES
INTERVENANTS

Sous-traitant

- personne physique ou morale, autorité publique, service ou tout autre organisme qui traite des données **pour le compte du responsable du traitement**

Ne pas confondre avec le responsable!

- obligations différentes dans GDPR
- obligation d'avoir un contrat de sous-traitance écrit contenant des clauses imposées par GDPR

Exple.: prestataire IT hébergeant données

GDPR & SOUS-TRAITANCE

OBLIGATIONS PORTANT SUR LE RESPONSABLE DU TRAITEMENT

Le choix du responsable

- uniquement des sous-traitants qui présentent des garanties suffisantes:
  - mise en œuvre de mesures de sécurité techniques et organisationnelles appropriées
  - traitement doit répondre aux exigences légales
  - garantir la protection des droits de la personne concernée
- CNPD doit pouvoir vérifier la conformité

PRESTATAIRES EXTERNES LCBFT

PRESTATAIRES LCBFT
DIFFICULTES DE QUALIFICATION

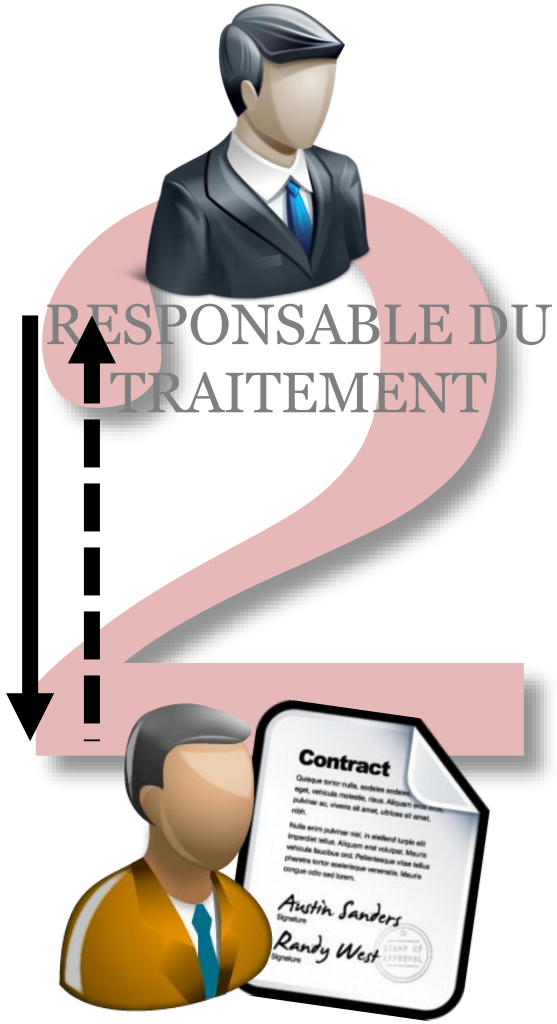
Appréciation au cas par cas

Outil en local

RESPONSABLE DU TRAITEMENT

FOURNISSEUR

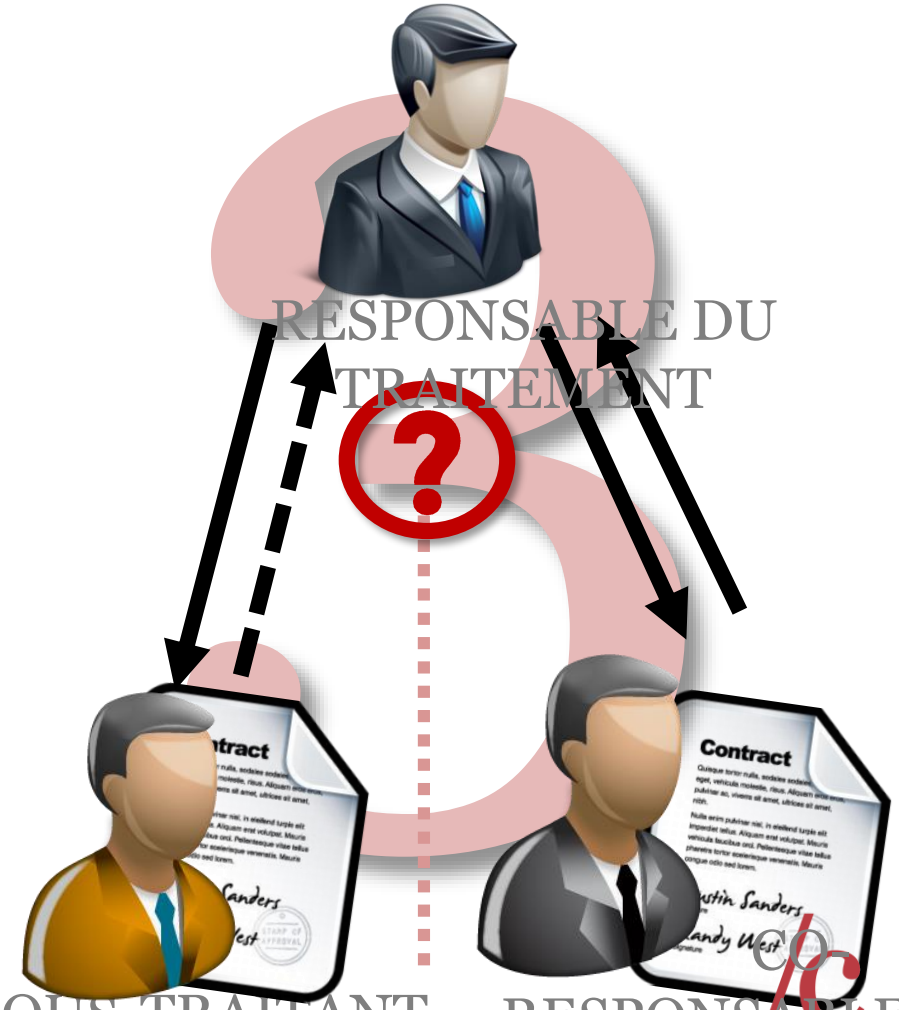
Saas



RESPONSABLE DU TRAITEMENT

SOUS-TRAITANT

Enquête



RESPONSABLE DU TRAITEMENT

SOUS-TRAITANT

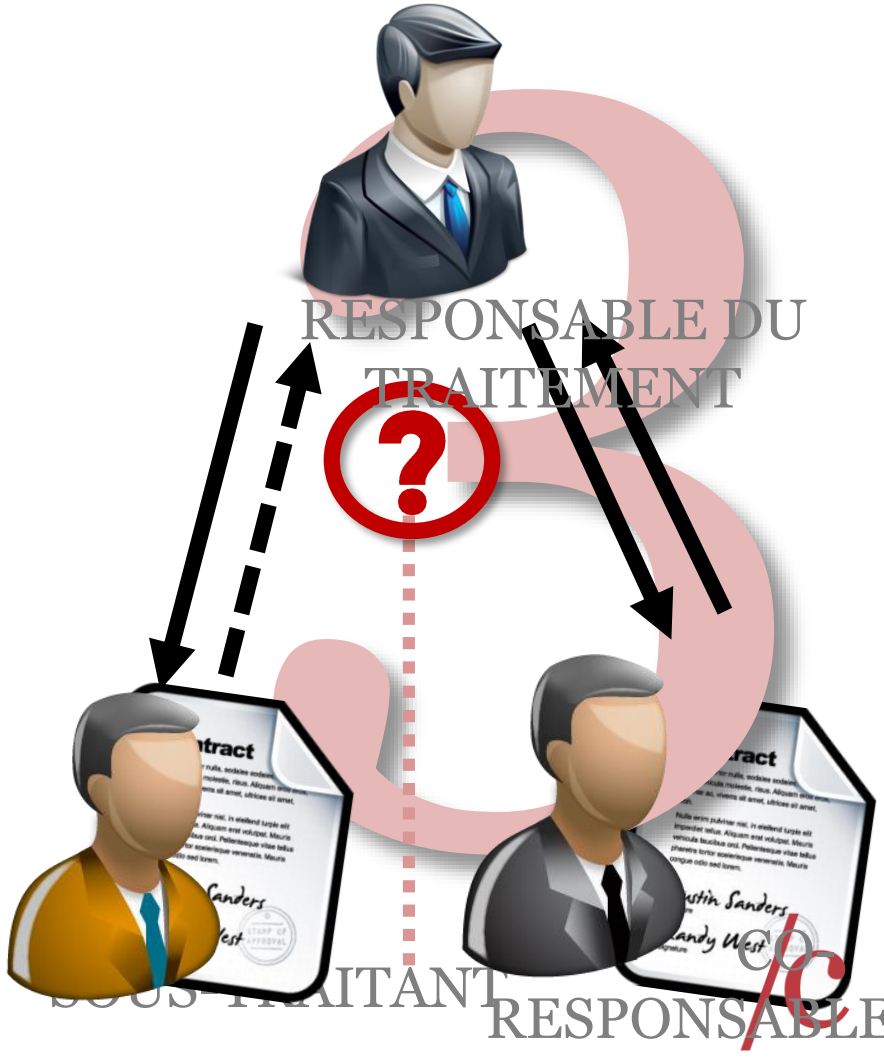
RESPONSABLE

PRESTATAIRES LCBFT
DIFFICULTES DE QUALIFICATION

Enquêtes?

- Si fournisseur = ST => est responsable de ses actes (catégories de données collectées, moyens mis en œuvre, etc.)
- Si fournisseur définit par ex. moyens pour faire les enquêtes, type de données /informations que contient le rapport: fournisseur = probablement RT (=> contrat de coresponsabilité, information de PC)

Prudence dans choix



/c law

THE LUXEMBOURG
IP&IT FIRM.

Questions?

Elisabeth GUISSART
Avocat à la Cour
(+352) 28 80 90 10
elisabeth.guissart@claw.lu
24,rue Jean l'Aveugle L-1148 Luxembourg