Règlement général sur la protection des données

(Banques & PSF)

Max SPIELMANN
Avocat
Schiltz & Schiltz

14 novembre 2016

uni.lu UNIVERSITÉ DU LUXEMBOURG

APDL Association pour la Protection des Données au Luxembourg

INTRODUCTION

- **RGPD** : Applicable à partir du <u>25 mai 2018</u>

- <u>Quels sujets seront traités ?</u>

  I. Qu'est-ce qu'une donnée personnelle?

  II. Quand est-ce qu'on peut traiter les données?

  III. Les principes de qualité des données

  IV. Responsabilité (*accountability*) & vos obligations

  V. Les droits de la personne concernée

  VI. Transferts internationaux de données

I. QU'EST-CE QU'UNE DONNÉE PERSONNELLE?

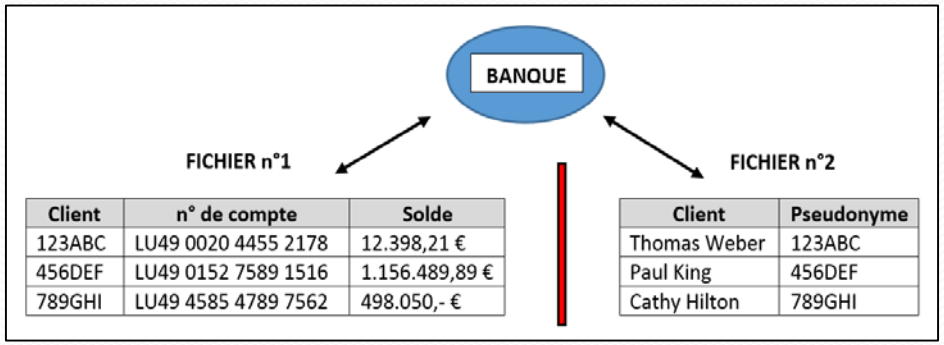
- **Définition**: « *toute information se rapportant à une personne physique identifiée ou identifiable* »

- **Données « anonymisées » c/ données « pseudonymisées »**
  - → Anonymisation = L'individu n'est plus identifiable (pas de données personnelles)
  - → Pseudonymisation = Les identifiants sont remplacés par un pseudonyme, mais la ré-identification reste possible (données personnelles)

I. QU'EST-CE QU'UNE DONNÉE PERSONNELLE? - illustrations

- **Services bancaires téléphoniques** : Conservation des enregistrements vocaux = <u>données personnelles</u>

- Données clients conservées sous forme de **pseudonymes** = <u>données personnelles</u>



Client	n° de compte	Solde
123ABC	LU49 0020 4455 2178	12.398,21 €
456DEF	LU49 0152 7589 1516	1.156.489,89 €
789GHI	LU49 4585 4789 7562	498.050,- €

Client	Pseudonyme
Thomas Weber	123ABC
Paul King	456DEF
Cathy Hilton	789GHI

- Plus délicat: Données clients **anonymisées** (fins statistiques) (<u>ex.</u> Ville de 12.000 habitants dont 8 médecins):
  - Commune de résidence, sexe, âge, profession (sans nom ou adresse) = <u>Données personnelles</u> ("ciblage")
  - Commune de résidence, sexe, âge, "diplôme universitaire?" = <u>Pas de données personnelles</u>

II. QUAND EST-CE QU'ON PEUT TRAITER LES DONNÉES? - Général

- **RGPD** = *A priori* identique à la Dir. 95/46/CE

- **Bases légales** :

Traitement de données

  - consentement
  - contrat (exécution ou mesures précontractuelles)
  - obligation légale
  - intérêts vitaux
  - intérêt public
  - intérêts légitimes (responsable du traitement ou tiers)

II. QUAND EST-CE QU'ON PEUT TRAITER LES DONNÉES? - Consentement

- **Consentement** = « *toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement* »

- **Conditions**:
  - preuve du consentement
  - forme compréhensible et aisément accessible, et formulée en des termes clairs et simples
  - doit être donné « librement »

- **Droit de retirer son consentement à tout moment**

- **Consentement obtenu sous la Dir. 95/46 reste valable** (si les conditions du RGDP sont remplies)

II. QUAND EST-CE QU'ON PEUT TRAITER LES DONNÉES? – Intérêts légitimes

- **Permis si** le traitement est nécessaire aux fins des intérêts légitimes poursuivis

- **Limite:** intérêts (y compris libertés et droits) de la personne concernée prévalent

= **Approche *in concreto***

↓

attentes raisonnables de la personne concernée

- **Exemples**:
  - nécessaire pour prévenir des fraudes
  - fins de prospection
  - garantir la sécurité du réseau et des informations
  - transmission intra-groupe de données à des fins administratives

II. QUAND EST-CE QU'ON PEUT TRAITER LES DONNÉES? – Traitements ultérieurs

- **Principe**: <u>pas</u> être traitées ultérieurement d'une manière <u>incompatible</u>

➔ **Mais comment apprécier la compatibilité?**

- lien entre les finalités initiales (à la collecte) et les finalités envisagées
- contexte de la collecte et relation avec le responsable du traitement
- nature des données
- conséquences possibles du traitement
- garanties appropriées (chiffrement ou pseudonymisation)

➔ Finalités historiques, statistiques et scientifiques = **toujours compatible**

- **Exceptions** (nouvelles):
  - consentement
  - loi

} permettent d'effectuer des traitements incompatibles

III. LES PRINCIPES DE QUALITÉ DES DONNÉES

- Les principes de la qualité des données **s'appliquent à tout traitement de données**

- **Ils incluent** (parmi d'autres) la :
  - limitation des finalités
  - licéité, loyauté, transparence
  - minimisation des données

- Le responsable du traitement doit démontrer le respect de ces principes

  → Principe d'«*accountability* »

IV. *ACCOUNTABILITY* & OBLIGATIONS

- ***Accountability*** = Conséquence de la *risk-based approach*

  → Passage du contrôle e*x-ante* à un contrôle *ex-post*

- ***Accountability*** = <u>être responsable</u> du respect et <u>démontrer le respect</u>

  - <u>Démontrer le respect du RGPD</u>… Mais comment? (exemples)

    → mesures techniques et organisationnelles appropriées

    → tenir un registre des activités de traitement

  - <u>Être responsable</u> = risque des amendes administratives

    ➔ jusqu'à 20 millions € ou 4 % du chiffre d'affaires annuel mondial total

IV. *ACCOUNTABILITY* & OBLIGATIONS

- **Vos obligations** sont nombreux et diverses

➔ **Vous devez** (exemples):

- prévoir des mesures techniques et organisationnelles appropriées
- respecter les principes de la *privacy by design* et *by default*
- designer, le cas échéant, un représentant dans l'UE
- sous-traitants qui présentent des garanties suffisantes
- tenir un registre des activités de traitement
- …

Obligations

- Le RGPD encourage aussi l'adoption de Codes de conduite et le recours à des certifications

IV. *ACCOUNTABILITY* & OBLIGATIONS

A. Choisir un sous-traitant (1)

Obligations

- **Pour les responsables du traitement:** vos sous-traitants doivent présenter des garanties suffisantes

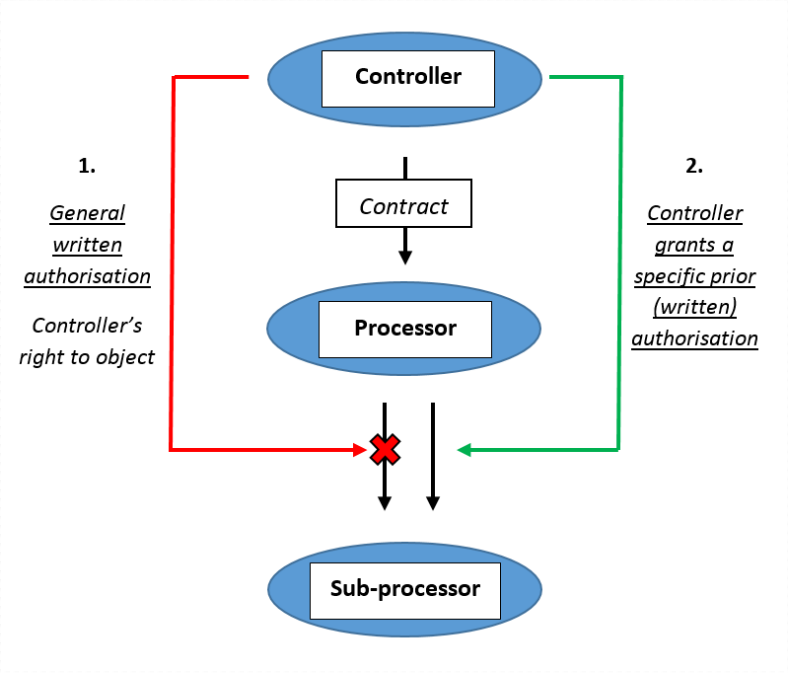
➔ Obligation de conclure un contrat ou un autre acte juridique qui traite:

- objet et la durée du traitement
- type des données personnelles
- nature et la finalité du traitement
- obligations à respecter par le sous-traitant
- …

IV. *ACCOUNTABILITY* & OBLIGATIONS

A. Choisir un sous-traitant (2)

- **Cas spécifique**: Le sous-traitant recrute un autre sous-traitant



Obligations

➔ Le sous-traitant initial demeure pleinement responsable devant le responsable du traitement

IV. *ACCOUNTABILITY* & OBLIGATIONS – B. Registre des activités

- **Principe:** tenir un registre des activités de traitement

Obligations

- **Limite**: moins de 250 employés + aucun risque pour les personnes concernées, traitement est occasionnel et pas de données sensibles

Pour les responsables du traitement	Pour les sous-traitants
• coordonnées du responsable du traitement • description des catégories de données • catégories de destinataires des données • description des transferts internationaux de données • description générale des mesures de sécurité techniques et organisationnelles	• coordonnées du ou des sous-traitants et de chaque responsable du traitement pour le compte duquel le sous-traitant agit • catégories de traitements effectués • transferts internationaux de données • description générale des mesures de sécurité techniques et organisationnelles

IV. *ACCOUNTABILITY* & OBLIGATIONS – C. Codes de conduite

- **Principe:** Associations (et autres organismes) représentant des catégories de responsables du traitement ou de sous-traitants peuvent élaborer des codes de conduite

Obligations

→ <u>Codes peuvent spécifier:</u>

  - intérêts légitimes poursuivis dans des contextes spécifiques
  - mesures de sécurité techniques et organisationnelles à mettre en place
  - l'exercice des droits des personnes concernées
  - …

- Codes de conduite = principalement **3 avantages majeurs**:
  - optique *marketing*
  - élément démontrant le respect du RGPD (sanctions)
  - transferts internationaux de données

→ une fois approuvé (autorité nationale + Commission) les acteurs de pays tiers peuvent adhérer au Code (condition = engagement contraignant et doté de force obligatoire)

IV. *ACCOUNTABILITY* & OBLIGATIONS – D. Certifications

- **Généralement** = mêmes avantages que les Codes de conduite

Obligations

- **Principes:**
  - Autorités posent les conditions selon lesquelles une certification peut être délivrée
  - Autorités ou les organismes de certification (secteur privé) sont ensuite en droit de délivrer des certifications
- Validité maximale de **trois ans** (renouvelable)
- Certification **ne diminue pas la responsabilité** de l'acteur

V. DROITS DE LA PERSONNE CONCERNÉE – Information du client (1)

- **Distinction** : données sont collectées auprès de la personne concernée, ou pas (même structure que Dir. 95/46/CE)

- **Plus d'informations sont à fournir sous le RGPD** (dans les deux cas), notamment sur :
  - → la période de conservation
  - → les intérêts légitimes poursuivis
  - → les droits des personnes concernées
  - → le droit de réclamation auprès d'une autorité de contrôle

- **Précision**: Si les données ne sont pas collectées auprès de l'individu, il faut l'informer sur la source des données

V. DROITS DE LA PERSONNE CONCERNÉE – Information du client (2)

- **Limite:** droit d'être informé n'est pas absolu…

→ *Mais quelles sont les exceptions*?

données sont collectées auprès de la personne concernée	**données ne sont pas collectées auprès de la personne concernée**
• personne concernée dispose déjà de ces informations	• personne concernée dispose déjà de ces informations • fourniture = impossible ou exigerait des efforts disproportionnés • Fourniture risque de rendre impossible ou de compromettre gravement la réalisation des objectifs dudit traitement" • données à caractère personnel doivent rester confidentielles

V. DROITS DE LA PERSONNE CONCERNÉE – Décisions individuelles automatisées (1)

- Toute personne = **droit de ne pas faire l'objet** d'une décision :

  (1) fondée exclusivement sur un traitement automatisé, y compris le profilage,

  et

  (2) produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire

- **Mais**: Droit n'est pas absolu → Exceptions

V. DROITS DE LA PERSONNE CONCERNÉE – Décisions individuelles automatisées (2)

➔ **Permis si** pareille décision:

- est autorisée par le droit européen ou national

  → Loi doit prévoir des mesures appropriées pour la sauvegarde des droits et libertés des individus

- est nécessaire pour un contrat (exécution ou conclusion)
- personne a donné son consentement explicite (nouveau)

Ici, c'est au responsable du traitement de prévoir des mesures appropriées

V. DROITS DE LA PERSONNE CONCERNÉE – Décisions individuelles automatisées (Exemples)

- **Banque permet de demander des crédits en ligne**
  - → Base légale autorisant la décision = ✓ (contrat + consentement)
  - → Mais quelles mesures appropriées? (2 possibilités)

(1) Demande = accueillie	(2) Demande = rejetée
✓ (Pas d'autres obligations)	<u>Client doit avoir le droit:</u> • d'exprimer son point de vue (intervention humaine) • de se faire expliquer la décision • de contester la décision

- **Procédure de recrutement de personnel en ligne** = Même garanties

VI. TRANSFERTS INTERNATIONAUX DE DONNÉES – Général

- **Principe:** Les transferts internationaux de données, sauf si les règles du RGPD sont respectées

- Cas d'ouverture = en grandes lignes les mêmes que sous la Dir. 95/46/CE
  - → décisions d'adéquation
  - → garanties appropriées
  - → Règles d'entreprise contraignantes (codifiées)
  - → dérogations

VI. TRANSFERTS INTERNATIONAUX DE DONNÉES – transfers *non-répétitif* (1)

*« **Lorsqu'un transfert ne peut pas être fondé** sur une disposition de l'article 45 ou 46, y compris les dispositions relatives aux règles d'entreprise contraignantes, et qu'aucune des dérogations pour des situations particulières visées au premier alinéa du présent paragraphe n'est applicable, un transfert vers un pays tiers ou à une organisation internationale ne peut avoir lieu que si ce transfert ne revêt **pas de caractère répétitif**, ne touche qu'un **nombre limité de personnes concernées**, est nécessaire aux fins des intérêts légitimes impérieux poursuivis par le responsable du traitement sur lesquels ne prévalent pas les intérêts ou les droits et libertés de la personne concernée, et si le responsable du traitement a évalué toutes les circonstances entourant le transfert de données et a offert, sur la base de cette évaluation, des garanties appropriées en ce qui concerne la protection des données à caractère personnel. Le responsable du traitement informe l'autorité de contrôle du transfert. Outre qu'il fournit les informations visées aux articles 13 et 14, le responsable du traitement informe la personne concernée du transfert et des intérêts légitimes impérieux qu'il poursuit. »*

(Article 49(1) RGPD)

VI. TRANSFERTS INTERNATIONAUX DE DONNÉES – transfers *non-répétitif* (2)

- ***Aucune autre base légale existe*** = Interprétation avec du recul

  → formulation = résultat d'un compromis politique (*trilogue*)

- "***Non-répétitif***" (texte Conseil = "not frequent" et "occasional")

  → ne devrait pas permettre des transferts similaires d'avoir lieu à titre régulier

  → Caractère résiduel = important

- "***Nombre limité de personnes concernées***" = Pas de clarifications

  → Nombre global des clients c/. clients concernés (%)

  - nature des données
  - finalité et la durée du traitement envisagé
  - situation dans le pays tiers

CONCLUSION

Le RGPD

(1) est complexe et comporte des risques pour les responsables du traitement et des sous-traitants

mais

(2) il offre aussi des opportunités pour ceux qui savent s'adapter

➡ et ceci est la raison pourquoi il est important **d'être prêt** le 25 mai 2018

Thank you - Merci - Danke

Max SPIELMANN
Avocat
Schiltz & Schiltz

UNIVERSITÉ DU LUXEMBOURG

APDL