RESPONSABLES DE TRAITEMENT ET SOUS-TRAITANTS

Mise en conformité et responsabilités accrues

Héloïse Bock

11 octobre 2016

IDENTIFICATION DES RÔLES

- Responsable du traitement (RT) / Sous-traitant

  → Définitions inchangées dans le Règlement (GDPR)

- Responsables conjoints : contrat écrit

- Désignation d'un représentant si le RT / sous-traitant est situé hors UE

ACCOUNTABILITY

- Obligation de <u>démontrer</u> conformité au GDPR et de <u>documenter</u> les mesures mises en œuvre

- GDPR: exemples de nouveaux moyens pour prouver la mise en conformité
  - Codes de conduite approuvés (article 40 GDPR)
  - Certifications (article 42 GDPR)
  - Labels (article 42 GDPR)

CONCEPT DE PROTECTION DES DONNÉES « INTÉGRÉE »

Protection dès la conception et par défaut *(privacy by design / by default*):

- Mesures techniques et organisationnelles appropriées en vue de:
  - Minimiser les données
  - Limiter le traitement aux données nécessaires

- Principes à appliquer dès le choix des moyens de traitement !

DOCUMENTATION ET ANALYSES D'IMPACT

≠ obligation de notification généralisée

Nouveau:

- Obligation de tenir un registre

  Exception très limitée pour les PME de moins de 250 personnes (seulement traitements occasionnels!)

- Analyses d'impact préalables si risque élevé, en particulier:
  - Évaluation systématique et approfondie d'aspects personnels
  - Traitement à grande échelle de catégories particulières de données
  - Surveillance systématique à grande échelle d'une zone publique

→ Nature des mesures à adopter: en fonction du risque / consultation des autorités compétentes

VIOLATIONS DE DONNÉES

Obligation générale de notification:

- A l'autorité de contrôle: dans les 72h
  Exception: si pas de risque pour les droits de la personne concernée

- Aux personnes concernées: dans les meilleurs délais
  Si risque élevé pour les droits et libertés individuelles

- Le sous-traitant doit notifier les violations au RT

- RT supporte le coût de la notification!

SÉLECTION DU SOUS-TRAITANT ET CONTRAT

➔ Sélection importante (garanties suffisantes en termes de connaissances spécialisées, fiabilité, ressources)

➔ Contrat de sous-traitance: plus de précisions

Instructions documentées!

Autorisation écrite préalable du RT pour la désignation d'un autre sous-traitant + contrat identique

Obligation de coopération

Suppression / renvoi des données au terme du contrat

Obligation de sécurité et de confidentialité

➔ « Sous-sous traitance » : obligations pour le sous-traitant d'imposer contractuellement les mêmes obligations à ses sous-traitants

AUTRES NOUVELLES OBLIGATIONS DU SOUS-TRAITANT

- Tenue d'un registre (article 30 §2)
- Assiste le RT pour les analyses d'impact et notifications des violations de données (article 33 §2)
- Obligation directe du sous-traitant de conformité en relation avec les transferts de données hors UE (article 46 GDPR)
- Recours juridictionnel contre le sous-traitant et droit à réparation (articles 79 et 82 GDPR)
- Contact et coopération avec l'autorité (article 31 GDPR)
- Désignation d'un DPO (article 37 GDPR)

DÉLÉGUÉ À LA PROTECTION DES DONNÉES (DPO)

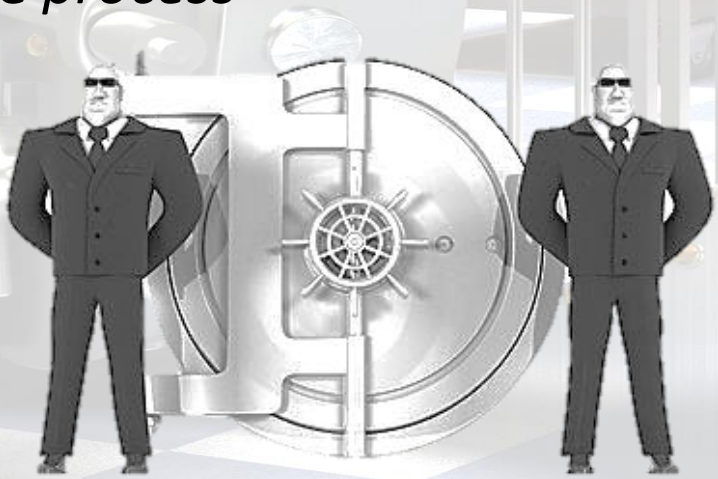
- Missions principales:
  - Veille à la conformité, conseille le RT / le sous-traitant
  - Point de contact pour l'autorité / personne concernée
- Désignation obligatoire :
  - activité de base concerne suivi régulier et systématique à grande échelle des personnes concernées
  - activité de base concerne traitement à grande échelle de catégories particulières de données
  - autorités ou organismes publics
- Désignation recommandée dans d'autres cas: garantie accrue de conformité
- DPO unique pour groupe d'entreprises ou associations
- Sélection importante: connaissances spécialisées en droit et contrat de services possible

ENJEUX

- Complexité de la matière
- Nombre de mesures à mettre en place
- Nouvelles sanctions financières :
  - de 2 à 4% C.A. mondial ou de 10 à 20 MIO€ pour violation et maintien des sanctions administratives existantes (ex. interdiction du traitement, ordre d'effacement des données etc).

To do

- Bonne gouvernance / *Privacy management*
- Désignation d'une personne en charge (cas échéant DPO) et formation du personnel
- Vérification conformité et suivi régulier !
- Mise en place de *process*



« *Rien ne sert de courir ; il faut partir à point.* »

Merci pour votre attention

Questions?

Héloïse Bock
Avocat à la Cour
Conseiller d'Etat
+352 40 78 78 321
heloise.bock@arendt.com