RÔLE ET OBLIGATIONS DES PARTIES AUX TRAITEMENTS

«La protection des données, j'en fais mon affaire» - Projet Boost – 9 mars 2021

Autorité de protection des données
Gegevensbeschermingsautoriteit

Lignes directrices du Comité Européen de la Protection des Données 07/2020

sur les notions de responsable de traitement et de sous-traitant dans le cadre du RGPD

Pourquoi ?

- La compréhension des concepts de responsable de traitement et sous-traitant est essentielle à la bonne application et au respect des règles du RGPD

Responsable de traitement

- Éléments à prendre en compte : légaux ou factuels

Une entité qui exerce une **influence sur les finalités et les moyens essentiels** est responsable de traitement

⇒ Détermine le pourquoi et le comment

⇒ l'accès ou non aux données à caractère personnel n'importe pas

⇒ les dispositions du contrat sont un indice important mais pas toujours déterminant

Responsable de traitement

- Maîtrise de sa relation avec le sous-traitant et les sous-traitants ultérieurs

  - choix d'un sous-traitant présentant les qualités et garanties requises pour le traitement, même si ce prestataire dispose de contrats-type sans négociation possible
  - Acte contraignant écrit (article 28 RGPD) + annexes concernant les procédures à suivre
  - Prévoir les modalités de transferts internationaux de données
  - Octroi ou non d'autorisation de sous-traitants ultérieurs
  - Garder la maitrise sur les sous-traitants et sous-sous traitants (audit)

- Veiller à la réutilisation conforme des données : engagement contractuel

Sous-traitants

- Éléments à prendre en compte : légaux ou factuels

Une entité qui traite les données **pour le compte** du responsable de traitement et qui est **distincte** de celui-ci

⇒Être prestataire ne signifie pas être sous-traitant : quel rôle dans le traitement de données à caractère personnel ?

⇒Ne détermine pas le pourquoi ni le comment, sauf sur les éléments non essentiels

⇒Les dispositions de votre contrat sont un indice important mais pas toujours déterminant

⇒Obligations propres au sous-traitant

Article 28.3 RGPD

- Écrit : instructions écrites
- Contraignant : contrat ou autre forme juridiquement contraignante
- Signé des parties
- précisions concernant la manière dont le sous-traitant est amené à assister le responsable de traitement dans le respect de ses obligations selon les articles 32 à 36 du RGPD
- Pour aider à la démonstration de la conformité => « *toutes les informations sur la manière dont l'activité de traitement sera conduite pour le compte du responsable de traitement* », par exemple les « *informations sur le fonctionnement des systèmes utilisés, les mesures de sécurité, la conservation de données, la localisation des données, les transferts de données, l'accès aux données et destinataires des données, le recours à des sous-traitants ultérieurs etc.* »
- Transferts internationaux
- Sous-traitance ultérieure : le premier ST est pleinement responsable vàv du RT
- Formulaires et procédures d'assistance => par exemple : violation de données, le contrat devrait contenir un délai (en heures) endéans lequel le ST prévient le RT
- Audit : coopération en toute bonne foi

Responsables conjoints de traitement

- **déterminent ensemble** les finalités et les moyens conjointement **ou** dont les **activités de traitements sont indissociablement liées ou complémentaires**
- décision commune prise par les acteurs impliqués ou plusieurs décisions convergentes de différents acteurs (le CEPD précise à ce sujet que le traitement de données personnelles ne serait pas possible sans la participation des deux parties concernant tant la détermination des moyens que des finalités)
- La mise en commun de moyens de traitement n'implique pas nécessairement la responsabilité conjointe
- Peu importe qu'ils aient ou non accès aux données
- pas besoin d'exercer un contrôle sur l'ensemble du traitement pour être qualifiée de responsable conjoint du traitement (une étape spécifique peut suffire)
- pas nécessairement le même niveau d'implication

Accord entre les responsables conjoints (Article 26 RGPD)

Le CEPD précise ce qu'implique l'accord entre les responsables conjoints :

Acte écrit contraignant qui couvre l'objet, la ou les finalités du traitement, les catégories de données personnelles, les catégories de personnes concernées, et qui détermine la responsabilité :

- des obligations déduites des articles 13 et 14 RGDP,
- du suivi des demandes formulées par les personnes concernées qui exercent leurs droits ;
- de la détermination des mesures de sécurité techniques et organisationnelles nécessaires,
- de la documentation de la base juridique du/des traitement(s),
- de la notification/communication des violations de données
- de l'AIPD
- de recruter et superviser les sous-traitants,
- de s'assurer de la légalité des transferts internationaux de données personnelles, et
- d' agir comme contact pour les personnes concernées et les autorités de contrôle.

Accountability

Responsable de traitement, seul ou conjoint

Savoir quel est son rôle et ses obligations

Documentation

Sous-traitant

Savoir quel est son rôle et ses obligations

Documentation

•la qualification des acteurs peut être complexe mais néanmoins obligatoire

•détermination au cas par cas tenant compte du degré d'influence effectif que chaque entité a dans la détermination des finalités et moyens du traitement

•activités et rôles effectivement assumés dans un cadre donné plutôt que désignation formelle des parties en tant que responsable ou sous-traitant.

•vous seuls êtes en mesure de savoir quel est votre rôle :vous avez la connaissance de vos traitements, des procédures de prise de décision y relatifs et des moyens de ces traitements

•l'APD n'est donc pas chargée de vous dire quel est votre rôle mais pourrait, le cas échéant, le requalifier (et éventuellement, sanctionner) !

• consigner votre activité et votre rôle dans le cadre de votre devoir d'accountability

•il n'est plus aujourd'hui optionel pour une partie de ne pas se poser la question des rôles au regard de la protection des données lors du lancement d'un traitement de données à caractère personnel, la conclusion d'un nouveau contrat, partenariat ou autre.

Vous devez établir votre rôle sur base de faits, le refléter dans vos contrats et veiller au respect de vos obligations mais également être attentif au respect de leurs obligations par vos partenaires.

- **Autorité de Protection des données de Hamburg :** Absence d'accord (Art. 26 RGPD) entre responsables de traitement conjoints = 13000 euros
- **Autorité de Protection des Données francaise (CNIL):** sanction de 150000 euros pour un responsable de traitement et 75000 pour son sous-traitant « *le responsable de traitement doit décider de la mise en place de mesures et donner des instructions documentées à son sous-traitant. Mais le sous-traitant doit aussi rechercher les solutions techniques et organisationnelles les plus appropriées pour assurer la sécurité des données personnelles, et les proposer au responsable de traitement* »