ALLEN & OVERY

Quelles obligations pour les sous-traitants?

Cycle de conférences “Fit4*DataProtection*”
27 novembre 2017

Agenda

1	Qu’est-ce qu’un sous-traitant?
2	Les obligations des sous-traitants
3	Que faire en pratique?
4	Responsabilité et sanctions

1. Qu'est-ce qu'un sous-traitant?

Définitions (art.4 RGPD) /1

Le « **responsable du traitement** » est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

Le « **sous-traitant** » est la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

Etes-vous sous-traitant?

Quelques critères*:

- Niveau d'instruction donné par le client au prestataire
- Degré de contrôle de l'exécution de la prestation
- Valeur ajoutée fournie par le prestataire
- Degré de transparence sur le recours à un prestataire

* Avis 1/2010 du G29 du 16 février 2010

Exemples de sous-traitant

- Prestataires de services informatiques (hébergement, maintenance,..)
- Sociétés de sécurité informatique
- Agences de marketing ou de communication
- Certains organisme public ou une association

Plus généralement:

tout organisme offrant un service ou une prestation impliquant un traitement de données à caractère personnel pour le compte d'un autre organisme

Etes-vous soumis au RGPD?

Champ d'application territorial étendu ! Le RGPD s'applique aux sous-traitants:

- établis dans l'UE
- établis en dehors de l'UE si les activités de traitement sont liées à l'offre de biens ou de services à des personnes concernées dans l'UE au suivi du comportement de ces personnes (*profiling*), lorsqu'il a lieu au sein de l'UE

:

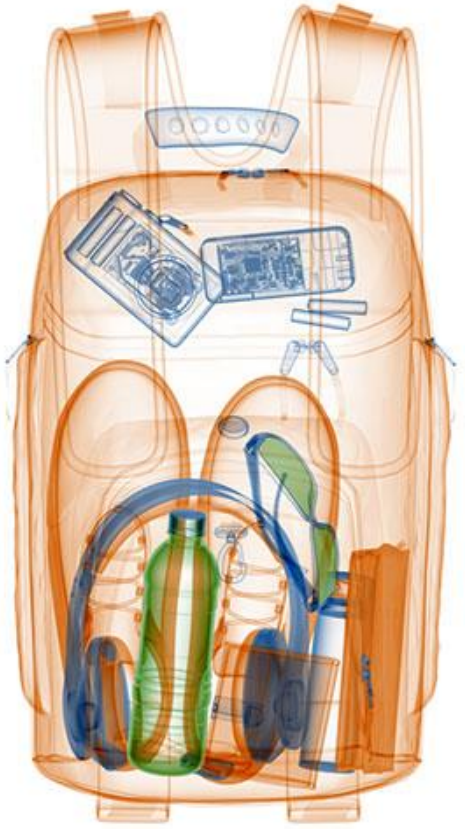
-

2. Les obligations des sous-traitants

Obligations du sous-traitant /1

Obligation de transparence et de traçabilité

- Contenu minimum prescrit pour les contrats de sous-traitance (art. 28)
- Demander l'autorisation écrite du client avant de faire appel à un sous-traitant
- Démontrer le respect de vos obligations
- Tenir un registre des traitements effectues pour compte.



Obligations du sous-traitant /2

Obligations contractuelles (art. 28)

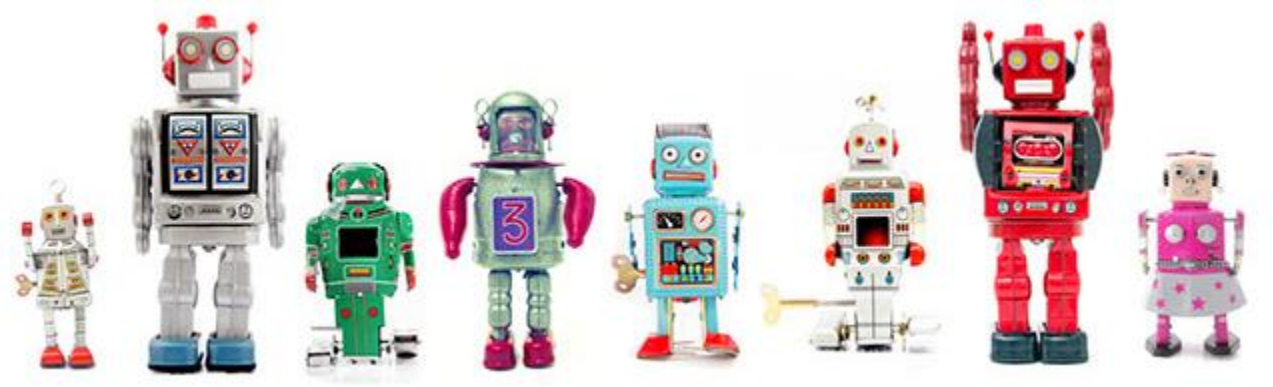
- Agir uniquement **sur instruction documentée** du responsable;
- Imposer une obligation de **confidentialité** au personnel impliqué;
- Mettre en œuvre les **mesures de sécurité** nécessaires;
- **Sous-traiter** des activités de traitement uniquement avec l'accord préalable du responsable;
- Dans la mesure du possible, prendre les **mesures techniques et organisationnelles** appropriées pour permettre au responsable de respecter les droits des personnes concernées;
- **Assister le responsable** pour remplir ses obligations relatives à la sécurité des données et la consultation avec les autorités de contrôle;
- **Effacer ou renvoyer** au responsable toutes les données personnelles après la fin de fourniture des services visés par le traitement;
- Mettre à la disposition du responsable toutes les **informations** nécessaires relatives aux activités de traitement du sous-traitant.

Obligations du sous-traitant /3

Prise en compte des principes de protection des données dès la conception et de protection des données par défaut

- **Dès leur conception**, vos outils, produits, applications ou services que vous offrez à vos clients, intègrent de façon effective les principes relatifs à la protection des données et

- **Par défaut**, vos outils, produits, applications ou services garantissent que seules sont traitées les données nécessaires à la finalité du traitement au regard de la quantité de données collectées, de l'étendue de leur traitement, de la durée de conservation et du nombre de personnes qui y a accès



Obligations du sous-traitant /4

Garantir la sécurité des données traitées

- Mise en œuvre des mesures de sécurité
- Obligation de confidentialité à charge des employés
- Notification d'une violation de données à caractère personnel au responsable du traitement dans les meilleurs délais
- Gestion des données en fin de contrat

Obligations du sous-traitant /5

Assistance, alerte et conseil

- Notification d'une violation de données à caractère personnel au responsable du traitement dans les meilleurs délais
- Exercice des droits des personnes concernées
- Coopération avec l'autorité de contrôle (la CNPD)

4. Que faire en pratique?

Obligations légales directes

- Analysez les nouvelles obligations à respecter
- Vérifiez si vous devez désigner un DPO
- Mettez en place ou adaptez les procédures internes
- Tenez un registre des activités de traitement
- Vérifiez si la documentation contractuelle existante est adaptée
- Formez votre personnel

Désignation d'un DPO

Un délégué à la protection des données doit être désigné si:

1. Vous êtes une autorité ou un organisme public

ou

2. vos activités de base vous amènent à réaliser, pour le compte de vos clients, un suivi régulier et systématique des personnes à grande échelle

ou

3. vos activités de base vous amènent, pour le compte de vos clients, à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et infractions.

Un délégué peut aussi être désigné sur base volontaire

Un délégué peut être suffisant pour un groupe de sociétés

Revoyez votre documentation contractuelle

Assurez-vous que le contrat comporte les prescriptions listées à l'art. 28 ainsi que les autres obligations

Établissez un modèle de contrats pour les nouveaux clients

Revoyez les contrats existants

Armez-vous pour les négociations

Modifiez les contrats existant par avenant

Qui supportera les coûts des changements législatifs?

Elaborez un registre des traitements

Registre **écrit**

Couvrant toutes les activités de traitement de données effectuées pour le compte d'un responsable de traitement: le Règlement énumère une liste détaillée des informations qui doivent être inclues dans ces registres

Mis à disposition des autorités de contrôle sur demande

Exceptions

Société employant moins de 250 personnes

sauf si (i) le traitement présente des risques pour les droits et libertés des personnes concernées, (ii) il n'est pas occasionnel, (iii) il porte notamment sur des données sensibles (y compris des condamnations pénales).

Notification de violations des données

Le sous-traitant doit informer dans les meilleurs délais le responsable du traitement de toute violation

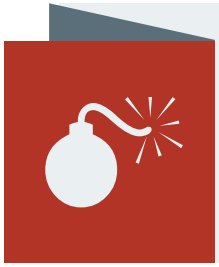
Le sous-traitant doit reporter et documenter toutes les violations au responsable du traitement

Aspects pratiques

- Toutes les sociétés (responsables de traitement et sous-traitants) devront adopter des procédures internes pour gérer les violation de données

➔ **Action**: développer ou mettre à jour les procédures internes de notification de violations

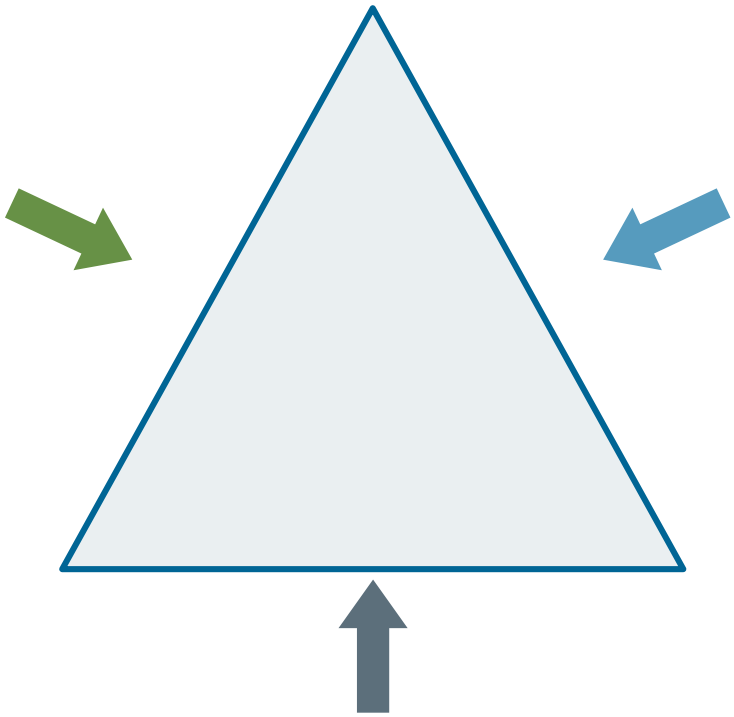
- Ces procédures doivent être testées régulièrement



Assurez-vous que les systèmes et processus existants permettront la détection et la notification de violations des données en temps utile

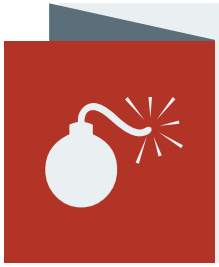
Pluralité de sous-traitants

Accord écrit préalable (spécifique ou général) du responsable du traitement



Si autorisation spécifique: information du responsable en cas de changement de sous-traitant secondaire

Le contenu du contrat doit respecter les obligations prescrites à l'art. 28



Le sous-traitant direct est responsable devant le responsable du traitement de la mauvaise exécution des obligations contractuelles de ses propres sous-traitants

4. Responsabilité et sanctions

Responsabilité des sous-traitants

- **Responsabilité directe des sous-traitants**: les personnes concernées peuvent porter plainte directement contre les sous-traitants

- **Droit à réparation**: le sous-traitant peut être tenu responsable des dommages résultant d'une non-conformité et peut être condamné à effectivement indemniser les personnes concernées

Conditions :

- Le sous-traitant n'a pas respecté les obligations directes applicables aux sous-traitants en vertu du GDPR

ou

- Le sous-traitant a agi en dehors des instructions du responsable ou contrairement à celles-ci

Pensez à souscrire une assurance pour couvrir les risques (violation de données)

Renforcement des sanctions (art.21)

Augmentation des sanctions

Violation des droits dont bénéficient les personnes concernées (article 12 à 22):

- amendes administratives jusqu'à **20 millions d'euros**
- pour les entreprises, jusqu'à **4% du chiffre d'affaires mondial annuel** de l'exercice précédent

On retient le montant le plus élevé

Charles-Henri Laevens
Juriste
Tel: +352 444455 282
charles-henri.laevens@allenovery.com