Le RGPD est arrivé: Quelles sont vos nouvelles obligations?

11 octobre 2018

mnks
A DIFFERENT LAW FIRM

Agenda

1. Définitions des notions clés
2. Les sanctions
3. Principe de responsabilité (“accountability”)
4. Mécanisme du consentement
5. Responsabilité des sous-traitants
6. Droits des personnes concernées
7. Transferts de données hors EEE
8. Notification d’une violation de données

1. Définitions des notions clés

- **Données personnelles**

Nom, prénom, adresse email (professionnelle et personnelle), photo, vidéo, copie de passeport, données de localisation, coordonnées bancaires, signature, fiche d'évaluation, salaire, personne de contact, données de déclaration fiscales, etc.
Certaines données sont considérées comme sensibles.

⇒ Ne vise que les personnes physiques

⇒ Données relatives (i) aux employés, (ii) à vos clients personnes physiques, (iii) aux personnes de contact, directeurs, bénéficiaires économiques, etc. liés à vos clients personnes morales et à vos sous-traitants, (iv) à toute personne qui est dans vos contacts

- **Traitement de données personnelles**

Toute opération faite sur les données : collecte, conservation, transfert, copie, etc

- **Responsable du traitement**

Entité qui décide quelles données doivent être collectées, pour quels buts, pendant combien de temps, etc

- **Sous-traitant**

Entité qui traite des données personnelles au nom et pour le compte du responsable du traitement (ex. prestataire de services de secrétariat social)

=> Une entité peut être à la fois responsable et sous-traitant

2. Les sanctions

- **Amendes administratives**

Augmentation des sanctions - amendes administratives allant jusqu'à 20.000.000 EUR, soit 4% du chiffre d'affaires mondial annuel.

Approche de la CNPD :

- Focus sur les sociétés considérées comme étant “à risque”;
- Réalisation d’un audit en cas de plainte reçue;
- Accompagner la société de bonne foi et ne pas sanctionner d’office.

➢ Source de risque: 1. les employés
2. les clients

3. Principe de responsabilité - « accountability » (1/2)

Plus de notifications préalables

Mais ...

Responsabilité

- Registres détaillés de traitement des données en interne
- Protection des données dès la conception (« privacy by design »)
- Protection des données par défaut (« privacy by default »)
- Désignation d'un DPO ?
- Mise en place de mesures techniques et organisationnelles

3. Principe de responsabilité - « accountability » (2/2)

- Exemples de mesures de sécurité à suivre:
  - Clean desk policy tous les soirs (risques femmes de ménage)
  - Fermer les armoires à clés et ne pas laisser la clé à la vue de tous
  - Utiliser le moins de papier possible – garder une version papier uniquement lorsque vous avez une obligation légale de le faire
  - Faire attention avant d'envoyer un email hors de l'entreprise et contenant des données personnelles
  - Utiliser une GED / sharepoint: encadrer la conservation des documents électroniques
  - Classer au mieux vos emails
  - Ne garder que les documents et données nécessaires
  - Ne pas créer de dossiers partagés à tout va / Gérer les accès

4. Mécanisme du consentement

- Principe: le consentement n'est en général pas nécessaire pour collecter et conserver des données personnelles (information préalable)
- Le consentement préalable des personnes concernées peut être nécessaire:

➢ Lorsque vous traitez des données sensibles

➢ Lorsque vous transférez des données hors EEE et qu'aucune autre base légale n'est possible

➢ Lorsque vous envoyez des communications commerciales à des contacts qui ne sont pas vos clients (opt-in)

- Le consentement doit être éclairé et explicite et pouvoir être retiré à tout moment

5. Responsabilité des sous-traitants

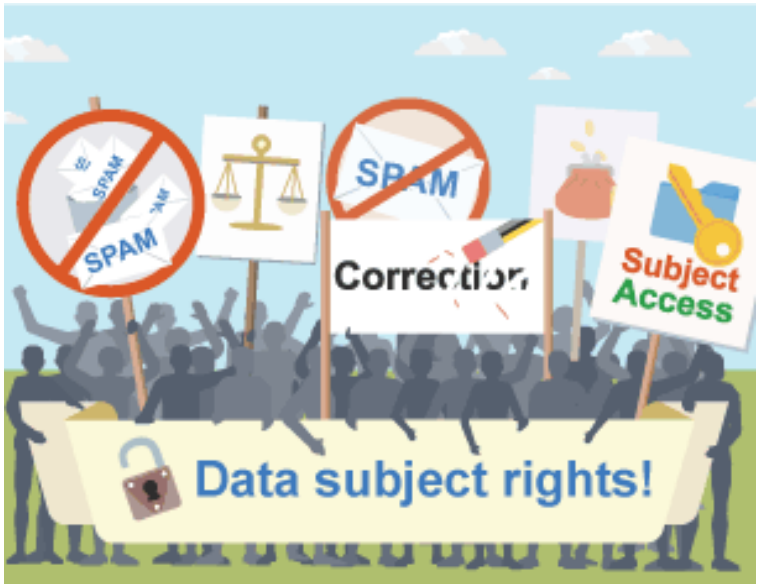
Directive 95/46/EC

- Aucune obligation directe imposée aux sous-traitants

Règlement

- Application aux sous-traitants
- Nouvelles obligations des sous-traitants
  - clauses obligatoires dans le contrat entre responsable du traitement et sous-traitant
  - tenue d'un registre de données
  - mise en place de mesures de sécurité techniques et organisationnelles
  - notification des violations de données
  - nomination d'un DPO
- De nouvelles responsabilités
  - responsabilité contractuelle envers le responsable du traitement
  - responsabilité envers les personnes concernées
  - Sanctions

6. Renforcement des droits des personnes concernées



- Droit à l'information
- Droit d'accès aux données
- Droit de rectification des informations inexactes ou incomplètes
- Droit d'opposition et de limitation au traitement

- Droit d'obtenir l'effacement des données (droit à l'oubli)
- Droit à la portabilité
- Droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé (profilage)

7. Les transferts internationaux de données

- **Les transferts de données hors EEE sont en principe interdits**

- **Exceptions :**

- transferts vers les pays assurant un niveau de protection adéquat;
- transferts basés sur des clauses contractuelles types de la CE;
- Transferts basés sur des Règles d'Entreprise Contraignantes (sous réserve d'une autorisation préalable de la CNPD);
- transferts basés sur le consentement préalable;
- code de conduite approuvé;
- mécanisme de certification approuvé.

8. Notification des violations de données

Violation des données personnelles : Une violation de la sécurité entraînant la destruction accidentelle ou illégale, la perte, la modification, la divulgation non autorisée ou l'accès à des données personnelles transmises, stockées ou traitées d'une autre manière.

Notification au responsable du traitement (Art 31)

- Dans les meilleurs délais
- Après en avoir pris connaissance

Notification à l'autorité de contrôle
(Art 33)

- Dans les meilleurs délais – si possible dans les 72 heures
- Délai autorisé si « justification motivée »
- Exempté si pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques

Communication à la personne concernée
(Art 34)

- Dans les meilleurs délais
- Si susceptible d'engendrer un risque pour les droits et libertés des personnes physiques
- 3 cas d'exemptions :

a. Données cryptées
b. Pas de risque élevé
c. Communication exigerait des efforts disproportionnés

Merci!

Contact

Audrey Rustichelli

Head of *Technologies & IP*
T: +352 26 48 42 35 98
rustichelli@mnks.com