Les midis de l’entreprise

Règlement général sur la protection des données
Quel impact concret sur mon entreprise ?

Mardi 16 janvier 2018

- Le Règlement général sur la protection des données (le « **Règlement** »)
  - 4 ans de discussions
  - Application directe
  - Mais uniformité relative
    - Projet de loi n°7184

Source: internet - gunruinabottle.com

- Entrée en vigueur **25 mai 2018**

Suis-je concerné(e) par le Règlement ? A quel titre ?

- Mon entreprise est établie dans l'UE, et dans certains cas en dehors de l'UE

- Et elle
  (i) traite des données personnelles
  (ii) contenues dans un fichier
  (iii) concernant une personne identifiée ou identifiable

- Responsable du traitement ou sous-traitant ?

Qu’est-ce qui change pour mon entreprise ?

- Sanctions renforcées
- Nouveau paradigme: concept d’*accountability*
- Renforcement des droits des personnes concernées
- Transferts vers des pays hors UE

Quelles sont les sanctions que je risque d'encourir ?

- Nouveau pouvoir de sanctions financières pour les autorités de contrôle en cas de violation du Règlement:
  - 4% C.A. mondial ou EUR 20 MIO, resp.
  - 2% C.A. mondial ou EUR 10 MIO
- Maintien des sanctions administratives existantes
- Sanctions pénales nationales maintenues ?

Qu'est-ce que le principe d'*accountability* ?

Privacy by design and by default

- Démontrer que toutes les mesures appropriées ont été mises en œuvre pour se conformer au Règlement et les documenter

- Analyse d'impact
- Registres, *policies*, codes de conduite, certifications
- Contrats sous-traitants et « *accountability* » du sous-traitant : nouvelles obligations
- Désignation d'un Délégué à la protection des données (DPO)
- Notification des violations de données

Comment démontrer ma conformité ?

- Analyses d'impact préalables requises si le traitement de données présente un risque élevé :
  - liste non exhaustive de cas prévue par le Règlement
  - nature des mesures à adopter: en fonction du risque

- Obligation de tenir un registre des traitements de données
  - ǂ notifications

- Politiques de traitement des données (*policies*) et procédures internes

- Possibilité d'adhérer à des codes de conduite et des certifications / labels

A quoi ressemble un registre des traitements de données ?

#	Catégorie de finalité	Finalités spécifiques du traitement	Personnes concernées	Catégories de données traitées	Origine des données	Transfert interne de données	Transfert externe de données
Traitt. 1							
Traitt. 2							
Traitt. 3							
Traitt. 4							
Traitt. 5							

Comment gérer la sous-traitance ?

- Importance du choix du sous-traitant
- Plus de précisions dans les contrats de sous-traitance :

Obligations contractuelles beaucoup plus détaillées

Instructions documentées !

Obligation de coopération

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

Suppression / renvoi des données au terme du contrat

- Nouvelles obligations légales et responsabilité accrue du sous-traitant :
  - Tenue d'un registre
  - Désignation d'un DPO
  - Assiste le RT à respecter ses obligations en matière d'analyse d'impact et de violation de données personnelles
  - Recours juridictionnel contre le sous-traitant et droit à réparation

Dois-je nommer un délégué à la protection des données ?

- Désignation obligatoire:
  - activités de base:
    - suivi régulier et systématique à grande échelle des personnes concernées
    - traitement à grande échelle des catégories particulières de données sensibles
  - autorités ou organismes publics
  - autres cas pourront être définis à l'avenir
- Un seul délégué pour un groupe d'entreprise (pas forcément local)
- **MAIS** désignation d'un DPO sur base volontaire est recommandée dans de nombreux cas
- Importance du bon choix

Comment dois-je réagir en cas de violation de données ?

- Notification à la CNPD dans les 72 heures
- Notification aux personnes concernées sans délai

Comment permettre aux individus d'exercer leurs droits ?

Précisés :

- Droit à l'information
- Droit d'accès et de rectification
- Droit d'opposition

Nouveaux :

- Droit à l'effacement
  déjà consacré en 2014 par l'arrêt de la CJUE Google Spain, C131/12
- Droit à la portabilité des données

➢ **Mise en place de procédures internes**

Illustration: Martin Vidberg – Communication du groupe de travail « Article 29 »

Quelles informations dois-je fournir ?

Informations existantes	Informations additionnelles / nouvelles
Identité du responsable du traitement et de son représentant le cas échéant	Coordonnées du responsable / représentant / DPO
Finalités du traitement	Base juridique du traitement
	Si traitement basé sur l'intérêt légitime→ intérêt à préciser
Destinataire(s) / catégorie(s) de destinataires	Si transfert vers un pays tiers → le caractère adéquat de la protection / référence aux garanties appropriées et les moyens d'en obtenir une copie
Réponses aux questions obligatoires / facultatives / conséquences défaut de réponse	Caractère règlementaire ou contractuel de la fourniture de données
	Durée de conservation (ou les critères pour la déterminer)
Droit d'accès / droit de rectification / droit d'opposition en cas de marketing	Droit à l'effacement / à la portabilité des données / droit de retirer son consentement / droit d'introduire une réclamation auprès de l'autorité de contrôle
	Existence d'une prise de décision automatisée comprenant un profilage

Comment dois-je fournir l'information ?

- Information concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples

- Option : information sous forme d'icônes normalisées (à définir par la Commission européenne)

Exemples:

Aucune donnée à caractère personnel n'est **divulguée** à des tiers commerciaux

Aucune donnée à caractère personnel n'est conservée de manière **non cryptée**

Comment puis-je valablement recueillir un consentement ?

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

- Sans information conforme, pas de consentement valable !
- Consentement explicite requis
  - ☑ *Je souhaite recevoir des informations sur les nouveautés et opérations spéciales de la société X* (case pré-cochée)
- Validité du consentement limitée :
  - véritable liberté de choix et possibilité de refuser consentement sans préjudice
- Il doit être aussi simple de retirer son consentement que de le donner

Comment puis-je transférer des données hors UE ?

Permis si

- Niveau adéquat de protection ou
- Garanties adéquates
- Exceptions possibles
- Sinon mêmes principes/exceptions qu'auparavant pour les transferts hors UE

Comment transférer aux Etats-Unis ?

Quelles sont les principales conséquences du Règlement sur mon entreprise?

- Enjeux considérables compte tenu de la complexité de la matière et des sanctions encourues
- Implication du conseil d'administration et des actionnaires nécessaire
- Importance du rôle du DPO
- Formation du personnel indispensable

Quelles sont mes prochaines étapes ?

Etat des lieux:

- ✓ Recensement des traitements, définition précise des finalités des traitements de données
- ✓ Audit : évaluation du niveau de conformité actuel et identification des lacunes
- ✓ Vérification de la base de légitimité au vu du Règlement
- ✓ *Mapping* de tous les transferts de données :

  catégories de données, destinataires, raisons du transfert, bases de légitimité en cas de transferts hors UE, etc.

Documentation:

- ✓ Etudes d'impact
- ✓ Tableau sur les durées de conservation des données :

  prise en compte de la finalité de chaque traitement et mise en œuvre d'une procédure d'effacement

- ✓ Mise en place et/ou adaptation de la documentation :

  registres, *policies*, procédures, documents d'information de la personne concernée, contrats de sous-traitance, etc.

Les services d'Arendt Regulatory and Consulting

- Création du Registre
  - ✓ Analyse des flux de données en fonction de la structure de l'entreprise ou du groupe
  - ✓ Méthodologie et organisation: sensibilisation, workshops, initialisation et maintenance, etc.
  - ✓ Mise en place éventuelle d'un logiciel de support pour le suivi et la planification des mesures de remédiation (e.g. Data Privacy Manager)
  - ✓ Identification des mesures correctives et planification

- DPO externalisé (délégué à la protection des données)
  - ✓ Condition préalable d'avoir participé à la création du Registre
  - ✓ Objectif: assurer la surveillance de l'application des dispositions légales et réglementaires sur base du périmètre couvert lors de la création du Registre et son évolution pendant la durée du service
  - ✓ Bénéfices: indépendance, expertise, gestion du risque, maîtrise des coûts

www.arendt-arc.com

Les défis de l'entreprise

Mardi 6 février 2018 à 17h30

Arendt House

Thème : L'entreprise et le temps

Avec la participation de Thomas Coville (navigateur français) et Elie Canivenc (responsable technique Team Sodebo).

Intervenants:

- Marc Giorgetti
- René Grosbusch
- Jean-Pierre Lutgen
- Claude Wagner

Plus d'informations ici

Veuillez cliquer ici pour vous inscrire

Nous contacter

- Sophie Wagner-Chartier, Partner
  - Tél : (352) 40 78 78 253
  - Email : sophie.wagner-chartier@arendt.com

- David Alexandre, Senior Associate
  - Tél : (352) 40 78 78 3806
  - Email : david.alexandre@arendt.com

- Astrid Wagner, Senior Associate
  - Tél : (352) 40 78 78 698
  - Email : astrid.wagner@arendt.com