Séance d'information spécialisée sur: Le nouveau règlement européen relatif à la protection des données.

Le futur rôle de la CNPD et l'impact sur les divers acteurs.

Guillaume Byk
Juriste – Chargé de Mission

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

14-17 novembre 2016, Chambre de Commerce

1. Bref rappel historique

- La loi actuelle est basée sur une directive de 1995.
- La réglementation actuelle n'est plus adaptée aux évolutions technologiques actuelles (big data, smart phone, cloud computing…).
- Ce nouveau règlement **actualise et renforce** les droits des personnes concernées et les devoirs des responsables de traitement et leur sous-traitants.
- Le règlement étant applicable partout en Europe, il harmonise la législation au niveau européen et participe à l'émergence d'un marché numérique européen.
- Le règlement sera applicable à partir du **25 mai 2018.** Avant cette date, la loi actuelle demeure applicable.

Principaux acteurs affectés par le RGPD

Personnes Concernées (PC)

(Individus dont les données personnelles sont traitées)

Le RGPD fournit au PC un ensemble élargi de droits qu'ils peuvent imposer aux responsables du traitement et/ou sous-traitant

Responsable du Traitement (RT) & Sous-Traitant (ST)

(organismes privés ou publics qui traitent les données personnelles d'individus)

RT et ST sont assujettis à une série de nouvelles obligations des personnes concernées et/ou des autorités de contrôle

Autorités de Contrôle (ACs)

ACs assistent les PC pour protéger leurs droits et les RT & ST pour la mise en application de leurs obligations comme décrites dans le règlement. Le RGPD renforce les pouvoirs de supervision des ACs.

2a. La supervision après le RGPD

Aperçu

- Responsable du Traitement et/ou Sous-Traitant

  Responsabilité = mise en œuvre de la conformité & capacité de la démontrer à tout moment (Art. 5.2)

  – Tâches déclaratives auprès de l'AC réduites due à l'abolition des formalités préalables,

  – Augmentation des mesures internes de conformité pour le RT/ST,

  – Liberté dans la mise en œuvre de la conformité, mais aussi responsabilités accrues des RT et/ou ST.

- Autorité de Contrôle

  – **Contrôle a posteriori** au lieu de l'examen a priori.

  – Les formalités préalables (notification et demande d'autorisation) sont remplacées par des contrôles et investigations.

  – L'objectif est de s'assurer que les RT/ST se conforment à leurs nouvelles obligations et sont responsabilisés, avec une attention particulière pour les contrôles ex-post des responsables non-conformes.

2b. La supervision après le RGPD
Étoffage des missions (Art. 57)

- Conservation de certaines missions actuelles
  - Sensibilisation et guidance de l'ensemble des acteurs càd des RT/ST et du public
  - Avis et conseils au gouvernement, aux entreprises et aux citoyens
  - Suivi de l'évolution des nouvelles technologies de l'information
- Certaines missions sont précisées ou renforcées
  - Coopération obligatoire avec les autres ACs européennes
  - Instruction des plaintes et réclamations déposées auprès de la CNPD
  - Encourager l'élaboration de codes de conduite, adoption des clauses contractuelles et approbation des règles d'entreprise contraignantes
- Nouvelles missions
  - Consultation préalable dans certains cas
  - Encourager la mise en place de mécanismes de certification et de labels
  - Gestion d'un registre interne des violations liées au règlement et des mesures correctrices
  - Participer aux activités du Comité Européen de la Protection des Données

2c. La supervision après le RGPD
Renforcement des pouvoirs (Art.58)

- Certains pouvoirs actuels sont précisés ou renforcés
  - Pouvoir d'investigation et d'enquête auprès des RT / ST,
  - Pouvoir de sanction / d'adopter des mesures correctrices (sanctions financières),
  - Pouvoir d'autorisation et pouvoir consultatif.

- Nouveaux pouvoirs
  - Respect des nouveaux droits des PCs,
  - Retrait de certifications,
  - Ordonner au RT de communiquer aux PCs une violation de données,
  - Possibilité d'infliger une amende administrative (max. 10/20 millions d'euro ou 2/4% du chiffre d'affaire annuel mondial de l'exercice précédent) en fonction notamment de la nature, gravité et durée de la violation etc. . Cette sanction se doit d'être effective, proportionnée et dissuasive.

- Pouvoirs additionnels peuvent être conférés à la CNPD par la loi nationale

3a. Le guichet unique et le contrôle de la cohérence

Aperçu

- Dans les cas transfrontaliers, le RT/ST a un point de contact unique dénommé AC chef de file lié à l'établissement principal (Art. 4.16) ou l'établissement unique du RT/ST (Art. 56.1).
- Coopération entre l'AC chef de file et les AC concernées grâce au mécanisme du guichet unique dans le but de parvenir à un consensus (Art. 60).
- Avec l'implication du Comité Européen de la Protection des Données (doté de la personnalité juridique) grâce au mécanisme de contrôle de la cohérence (Art. 63).
- Recours contre les décisions de l'EDPB dans un délai de 2 mois directement devant la CJUE en application de l'art. 263 TFUE.

3b. Le guichet unique (One-stop-shop)
Aperçu

- Nouveau système de régulation pour les traitements transfrontaliers:

  - Traitement de données dans le cadre des activités d'établissements dans plusieurs États membres d'un RT/ST ,

  ou

  - Traitement de données d'un établissement unique d'un RT/ST dans l'Union, mais qui affecte sensiblement ou est susceptible d'affecter sensiblement des PC dans plusieurs États membres.

- Avantages:
  - Pour les PC: meilleur défense de leurs droits car elles peuvent s'adresser directement à l'AC dans leur pays (proximité, point de contact unique).

  - Pour les RT/ST: simplicité/moins de contraintes administratives (point de contact unique) et meilleure sécurité juridique.

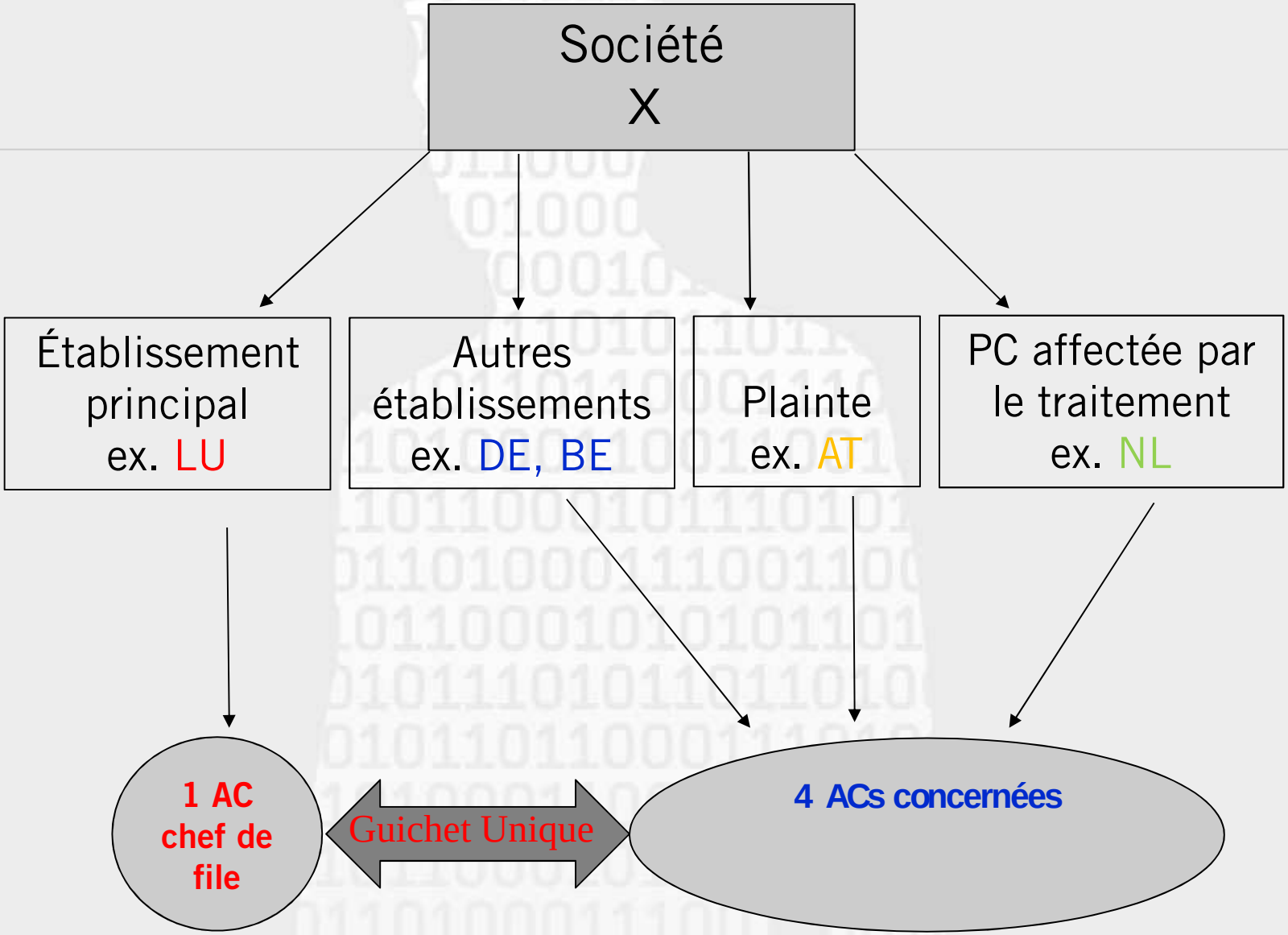
3c. Le mécanisme de contrôle de la cohérence

Aperçu

- **Rôle central de l'EDPB** dans le cadre du mécanisme de contrôle de la cohérence qui contribue à l'application cohérente du RGPD par:
  - Avis obligatoire quand une AC souhaite adopter certaines mesures (Art. 64.1) (ex.: liste de traitement lié à un DPIA)
  - Décision contraignante quand l'EDPB joue son rôle de résolution des conflits (Art. 65.1)
  - Procédure d'urgence (Art. 66), procédure dérogatoire au mécanisme du guichet unique et de contrôle de la cohérence

- Avantages:
  - Pour les PC: interprétation commune dans l'ensemble de l'UE des droits conférés par le RGPD
  - Pour les RT/ST: interprétation commune dans l'ensemble de l'UE des obligations imposées par le RGPD

Exemple avec 5 ACs impliquées



4a. Evolution de la loi nationale
Dispositions nationales

- Le règlement confère une certaine latitude dans la mise en œuvre de mesures nationales pour certains secteurs ou aspects (recherche, droit du travail…).

- Il y aura une évolution de la loi nationale pour la rendre conforme aux dispositions du règlement.

- De l'information sur les aspects purement nationaux sera diffusée en fonction de l'avancement des travaux relatifs à la modification de la législation nationale.

4b. Evolution de la loi nationale

Mesures transitoires

- Dépôt au mois d'août un projet de loi pour simplifier les démarches administratives actuelles (Projet de loi n°7049).

- Le projet de loi supprime l'obligation d'une autorisation pour les traitement de données liées à:
  - La surveillance,
  - Le crédit et la solvabilité,
  - L'interconnexion de données,
  - Le transfert de données vers des pays tiers.

- Une notification demeure nécessaire.

5a. Travaux du groupe de l'article 29

- En février 2016, le groupe de travail de l'article 29 a publié ses priorités dans le cadre de la mise en œuvre du nouveau règlement.

- 3 actions principales ont été définies:
  - Mise en place d'une task force pour la création de l'EDPB,
  - Préparation du mécanisme du guichet unique et du mécanisme de cohérence,
  - Publication de guidance à l'attention des RT et ST.

5b. Travaux du groupe de l'article 29

- Pour la guidance, 4 thèmes de travail ont été retenus:
  - Le nouveau droit à la portabilité,
  - Notion de risque élevé et l'analyse d'impact relative à la protection des données (DPIA),
  - La certification,
  - Le Délégué à la Protection des Données (DPO).

- Le travail coopératif entre les différentes autorités de contrôle sur ces guidances a beaucoup progressé, mais elles sont toujours en cours d'élaboration. Elles seront probablement diffusées fin de cette année ou début de l'année prochaine.

Pour plus d'information

- Les présentations de la conférence du 11 octobre 2016 sont disponibles à l'adresse suivante:

- http://www.cnpd.public.lu/fr/actualites/national/2016/10/conference-CNPD-SMC-1110/index.html

- Notre dossier thématique sur ce sujet:

- http://www.cnpd.public.lu/fr/dossiers-thematiques/Reglement-general-sur-la-protection-des-donnees/Reglement-general-sur-la-protection-des-donnees/index.html

Commission nationale pour la protection des données

1, avenue du Rock'n'Roll
L-4361 Esch-sur-Alzette (Belval)
261060-1
www.cnpd.lu
info@cnpd.lu