Formation CNPD:
Introduction à la protection des données

Les obligations du responsable du traitement

Esch-sur-Alzette

4-6 juillet 2017

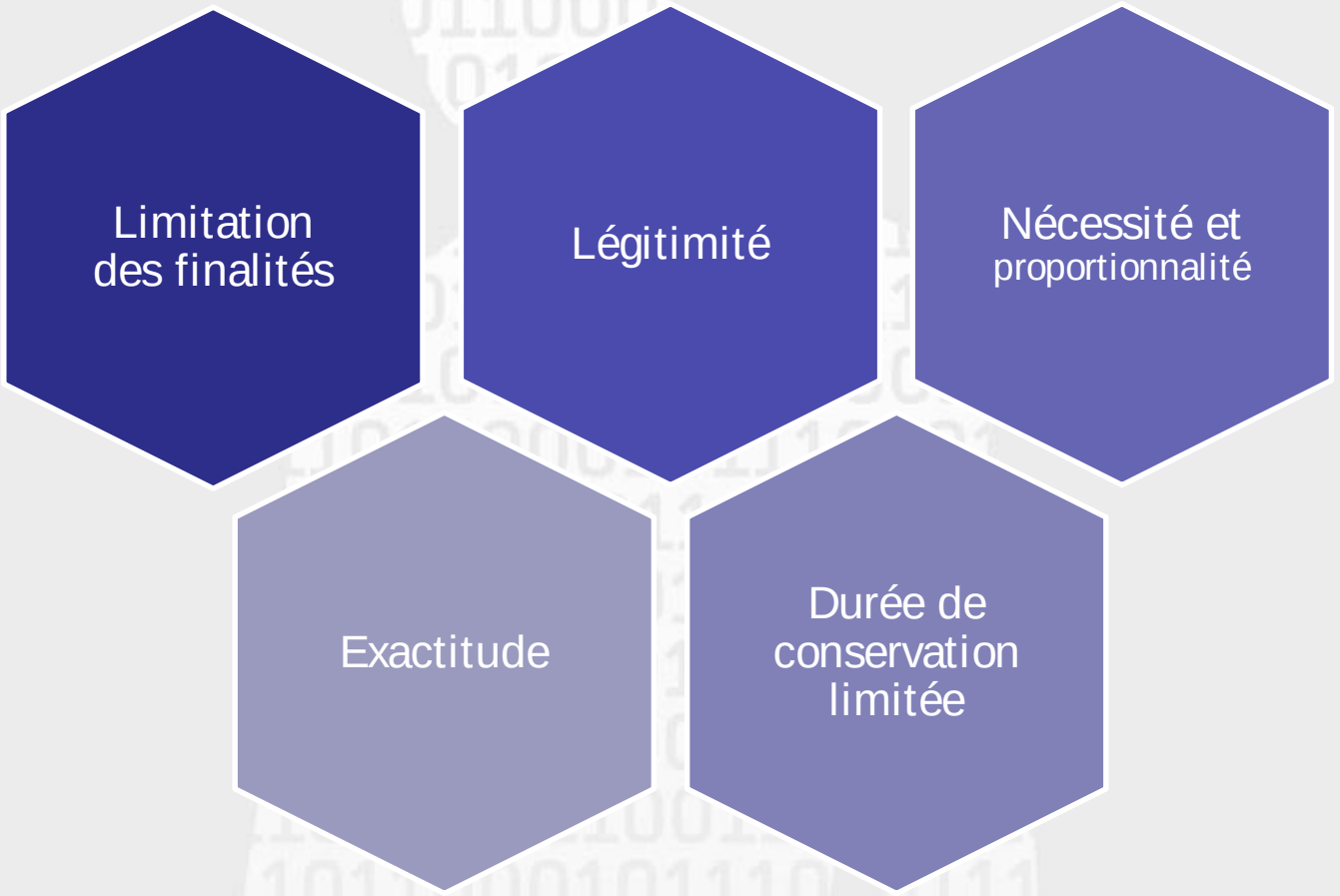
Arnaud Habran

Service juridique

Programme

1. Introduction
2. Les notions élémentaires
3. Les droits des personnes concernées
4. Le rôle de la CNPD
5. **Les obligations du responsable du traitement**
6. Nouveautés apportées par règlement européen sur la protection des données


Principes de qualité des données
Formalités administratives
Mesures de sécurité
Les obligations du responsable du traitement
Droits des personnes concernées
Sous-traitance
Transferts vers des pays tiers


Limitation des finalités
Légitimité
Nécessité et proportionnalité
Exactitude
Durée de conservation limitée

I. Principes de qualité des données

A. Limitation des finalités

- ***Finalité = objectif poursuivi par le traitement de données à caractère personnel***
  - La(les) finalité(s) doi(ven)t être définie(s) à l'avance
  - Les données doivent être seulement collectées pour des finalités spécifiques, explicites et légitimes
  - Les données ne peuvent pas être traitées ultérieurement de manière incompatible avec ces finalités
    - « compatibilité de finalités » pour le traitement de données compatible avec la finalité initiale pour laquelle les données ont été collectées (critère = attente raisonnable de la personne concernée)

I. Principes de qualité des données

B. Légitimité (1/2)

- ***= nécessité de légitimer le traitement sur base d'un des critères restrictifs prévus par la loi***
  - article 5 de la loi (« régime général »)
    - ex. consentement, obligation légale, nécessaire à l'exécution d'un contrat, mission d'intérêt public
  - article 6 de la loi (données sensibles)
    - → *Principe : le traitement de données sensibles est interdit*
    - Exceptions : ex. consentement exprès, motif d'intérêt public
  - article 7 de la loi (données traitées par les services de santé)
    - ex. raisons médicales, recherche en matière de santé ou scientifique + consentement explicite et écrit

I. Principes de qualité des données

B. Légitimité (2/2)

- article 8 de la loi (données judiciaires)
  - → *Principe : le traitement de données judiciaires est interdit*
  - Exception : si mis en œuvre en exécution d'une disposition légale
  - ex. casier judiciaire
- article 10 et 11 de la loi (traitement à des fins de surveillance)
  - ex. vidéosurveillance, surveillance des outils informatiques, enregistrement des conversations téléphoniques, utilisation de systèmes biométriques, géolocalisation, contrôle des accès et surveillance électronique des horaires de travail
  - → *Conditions restrictives + autorisation préalable auprès de la CNPD*
  - N.B. Surveillance sur le lieu de travail - l'article 11 de la loi et l'article L.261-1 Code du travail (cf. brochure)

I. Principes de qualité des données

C. Nécessité et proportionnalité

= traiter seulement les données nécessaires et en lien avec la finalité

- Traitement des seules données adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées

→ « *Need to have, not nice to have* »

→ Possibilité d'atteindre la même finalité sans traiter de donnée à caractère personnel ou en traitant moins de données?

→ Existence de moyens alternatifs moins intrusifs dans la vie privée des personnes concernées?

I. Principes de qualité des données

D. Exactitude

- **= *données exactes et, si nécessaire, mises à jour***
  - Des données incorrectes ou fausses peuvent porter préjudice à la personne concernée
  - Prendre toute mesure raisonnable pour effacer ou recitifier les données inexactes ou incomplètes
  - Si ce n'est pas le cas, les données personnelles doivent être corrigées ou effacées

I. Principes de qualité des données

E. Durée de conservation limitée

- ***= collecte des données pas plus longtemps que nécessaire pour la réalisation des finalités pour lesquelles elles sont collectées et traitées***
  - Si la finalité est totalement réalisée, les données doivent être (définitivement) supprimées ou (complètement) anonymisées
  - L'appréciation de la durée de conservation des données est relative et dépend de la détermination de la finalité (ex.: durée de prescription) → analyse au cas par cas
  - En tous cas : il n'est pas permis de conserver les données indéfiniment pour la simple raison qu'elles pourraient peut-être être « utiles » un jour

II. Mesures de sécurité

- Mesures techniques et organisationelles selon “l’état de l’art”
- Mesures doivent être adaptées au contexte et aux spécificités du domaine concerné
  - Analyse: nature des données, prescriptions légales, taille de la société ou de l‘organisation, complexité du système, risques encourus, etc.

III. Sous-traitance

- Contrat écrit obligatoire (responsable du traitement – sous-traitant) prévoyant que:
  - le sous-traitant n'agit que sur la seule instruction du responsable du traitement
  - les obligations du responsable du traitement (en matière de mesures de sécurité) incombent également au sous-traitant

IV. Transferts vers des pays tiers

- Libre circulation des données au sein de l'UE/EEE permise
- Transferts de données vers des pays tiers (= en dehors de l'UE) interdits, sauf :
  - Décision d'adéquation pour un pays (ou pour un secteur spécifique dans un pays déterminé)
  - Garanties appropriées (au Luxembourg: BCR ou clauses contractuelles types, avec autorisation préalable de la CNPD)
  - Dérogations pour transferts occasionels, spécifiques (ex. consentement, contrat, etc.)

V. Respect des droits des personnes concernées

- ***= les personnes concernées doivent :***
  - être **informées** sur les traitements les concernant (avant que les informations les concernant fassent l'objet du traitement),
  - avoir **accès** à leurs données faisant l'objet d'un traitement (sur leur demande),
  - pouvoir **s'opposer** au traitement de leurs données pour des raisons prépondérantes et légitimes tenant à leur situation particulière,
  - pouvoir demander la **rectification** des données inexactes ou fausses les concernant.
  - N.B. communications non sollicitées et marketing – droits et obligations spécifiques → loi du 30/05/2005

VI. Formalités administratives (1/4)

1. Autorisation préalable

– Quand?

- Surveillance et surveillance sur le lieu de travail (notamment vidéosurveillance)
- Traitement de données génétiques
- Traitement de données biométriques
- Traitement concernant le crédit et solvabilité (excepté pour les PSF et sociétés d'assurance → notification)
- Interconnexion de données
- Traitement ultérieur/utilisation secondaire de données à des fins historiques, statistiques ou scientifiques (≠ collecte directe des données des personnes concernées)
- Cas spécifique : transfert de données vers des pays tiers (= en dehors de l'Union européenne)

VI. Formalités administratives (2/4)

1. Autorisation préalable

– Comment?

- vidéosurveillance, transfert de données vers des pays tiers → formulaires sur le site de la CNPD
- contrôle des accès et surveillance électronique des horaires de travail → engagement formel de conformité (décisions uniques)
- autres traitements : courrier libre comprenant les informations reprises à l'article 14 (2) (pas de formulaire prédéfini)

– Quoi?

- Analyse juridique du traitement par la CNPD
- Attendre l'autorisation de la CNPD avant de commencer les opérations de traitement

VI. Formalités administratives (3/4)

2. Notification préalable

- **Quand?**
  - Pour tout traitement non soumis à l'autorisation et non sujet à dérogation
- **Comment?**
  - Formulaire de notification sur le site de la CNPD
- **Quoi?**
  - Formalité administrative (pas d'analyse juridique)

VI. Formalités administratives (4/4)

- Pas de formalité administrative requise si:
  - Pas de donnée à caractère personnel
  - Données à caractère personnel complètement anonymisées (définition stricte)
  - Exemption de notification pour des traitements "journaliers" et non sensibles
    - ex.:administration du personnel et gestion des candidatures (recrutements), administration des salaires, comptabilité, gestion de la clientèle et des fournisseurs, …
  - Nomination d'un chargé de la protection des données (DPO) → registre
    - sauf pour les traitements soumis à autorisation → autorisation reste nécessaire

VII. Dans le futur (RGPD):

- Maintien des obligations existantes (par ex. principes de qualité des données)

  → *certaines sont renforcées ou deviennent plus détaillées*

- Nouvelles obligations
  - ex. le principe d'« accountability » → le responsable du traitement doit pouvoir démontrer le respect de ses obligations

mais :

- Suppression des formalités administratives (autorisation, notification)

Questions?

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