Formation CNPD:
Introduction à la protection des données

Les notions élémentaires

Esch-sur-Alzette

4 septembre 2018

Carmen Schanck

Service juridique

Programme

1. Introduction
2. **Les notions élémentaires**
3. Les droits des personnes concernées
4. Les obligations du responsable du traitement
5. Le rôle de la CNPD

Notions élémentaires

1. Le cadre légal
2. Les données personnelles
3. Le traitement des données personnelles
4. Les acteurs autour des données personnelles
5. Les grands principes de la protection des données

1. Le cadre légal (1/3)

1. **Règlement (UE) 2016/679 du 27 avril 2016 « RGPD »**
2. Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 « police-justice »
3. Loi du 11 août 1982 sur la protection de la vie privée
4. Loi modifiée du 2 août 2002 transposant la directive 95/46/CE a été **abrogée**
5. **Loi du 1er août 2018** portant organisation de la CNPD et du régime général sur la protection des données
6. Loi du 1er août 2018 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel en matière pénale ainsi qu'en matière de sécurité nationale
7. Loi modifiée du 30 mai 2005 transposant la directive 2002/58/CE
   - *« secteur des communications électroniques »*

1. Le cadre légal (2/3)


Journal officiel de l'Union européenne L 119/1

I

(Actes législatifs)

RÈGLEMENTS

RGPD

RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL

du 27 avril 2016

relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données)

(Texte présentant de l'intérêt pour l'EEE)

- ***Harmonisation:***
  - ✓ Mêmes règles pour les 28 Etats membres de l'UE
  - ✓ directement applicable depuis le 25 mai 2018
  - ✓ à tous les acteurs actifs sur le territoire de l'UE

- ***Nouveau cadre législatif***:
  - ✓ Un renforcement des droits des individus
  - ✓ Une responsabilité accrue des responsables du traitement
  - ✓ Un rôle plus important pour les autorités de contrôle de la protection des données

1. Le cadre légal (3/3)

Changement de paradigme

Formalités préalables

Contrôle a priori

Nouvelle approche **moins bureaucratique**, mais **plus exigeante** pour tous les acteurs

Principe de la responsabilisation

“ Accountability”

Contrôle a posteriori

2. Les données personnelles (1/3)

“ Toute information se rapportant à une personne physique identifiée ou identifiable […]”

Art. 4 (1) RGPD

2. Les données personnelles (2/3)

- *Les données "en clair":*

  les données permettant l'identification immédiate d'une personne

- *Les données pseudonymisées :*

  possibilité d'identifier une personne moyennant un effort de recherche plus ou moins important

- *Les données anonymisées :*

  impossibilité totale d'établir un lien avec une personne physique

2. Les données personnelles (3/3)

Catégories particulières de données = les données sensibles:

- ✓ l'origine raciale ou ethnique ;
- ✓ les opinions politiques ;
- ✓ les convictions religieuses ou philosophiques ;
- ✓ l'appartenance syndicale ;
- ✓ les données concernant la santé ;
- ✓ la vie sexuelle ;
- ✓ les données génétiques;
- ✓ les données judiciaires;
- ✓ ***les données biométriques***.

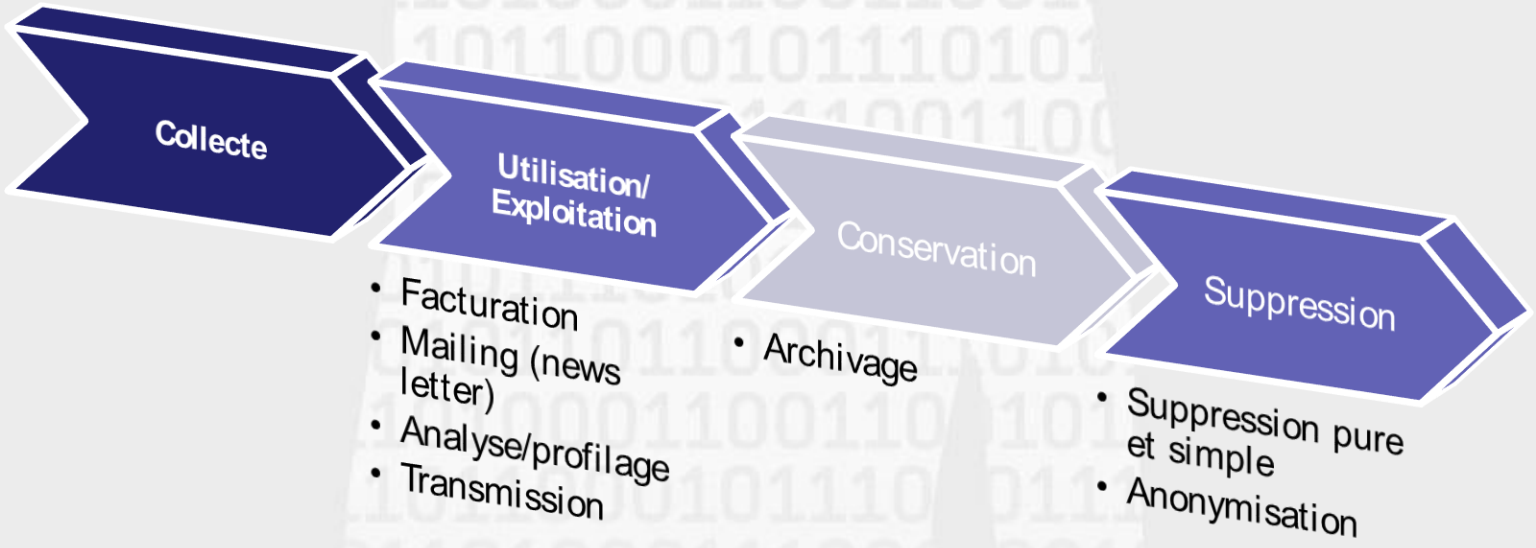
3. Le traitement de données à caractère personnel (1/2)

“ Toute opération ou tout ensemble d’opérations effectuées ou non à l’aide de procédés automatisés et appliquées à des données ou ***des ensembles de données à caractère personnel****, telles que la collecte, l’enregistrement, l’organisation,* ***la structuration****, la conservation, l’adaptation ou la modification, l’extraction, la consultation, l’utilisation, la communication par transmission, la diffusion ou tout autre forme de mise à disposition, le rapprochement ou l’interconnexion, la* ***limitation****, l’effacement ou la destruction”*

Art.4 (2) RGPD

3. Le traitement de données à caractère personnel (2/2)

Les traitements “in concreto”:



4. Les acteurs autour des données personnelles (1/3)

- Les personnes concernées
- Les tiers
- Les autorités de contrôle
- Le responsable du traitement
- Les sous-traitants
- Le délégué à la protection des données (DPO)

4. Les acteurs autour des données personnelles (2/3)

- *Le responsable du traitement*

  détermine les finalités et les moyens du traitement

- *Le sous-traitant*

  agit pour le compte et sur instruction du responsable du traitement

4. Les acteurs autour des données personnelles (3/3)

- Le délégué à la protection des données (DPO)
  - ✓ désignation obligatoire dans certaines hypothèses;
  - ✓ qualités professionnelles et connaissances spécialisées;
  - ✓ indépendance;
  - ✓ temps et ressources appropriés pour exercer sa mission.

5. Les grands principes de la protection des données (1/7)

5. Les grands principes (2/7)

5.1 Licéité = base légale

- *« régime général » = traitement autorisé si:*

✓ consentement,

✓ obligation légale,

✓ nécessaire à l'exécution d'un contrat,

✓ mission d'intérêt public,

✓ intérêt légitime,

✓ intérêt vital.

5. Les grands principes (3/7)

5.1 Licéité – catégories particulières de données

- *Cas particuliers = traitement interdit sauf exceptions*

  ✓ Consentement explicite, si la loi n'interdit pas de lever l'interdiction par le consentement ;

  ✓ Traitement nécessaire aux fins de la médecine préventive ou de la médecine du travail […], si traitement effectué par un professionnel de la santé soumis au secret médical;

  ✓ Etc.

5. Les grands principes (4/7)

5.2 Limitation des finalités

- *<u>Finalité</u> = objectif poursuivi par le traitement de données à caractère personnel*
  - ✓ La(les) finalité(s) doi(ven)t être définie(s) à l'avance
  - ✓ Collecte uniquement pour des finalités spécifiques, explicites et légitimes
  - ✓ Pas de traitement ultérieur incompatible avec finalité initiale (critère = attente raisonnable de la personne concernée)

5. Les grands principes (5/7)

5.3 Minimisation

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

- ✓ données adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités

5.4. Exactitude

= données exactes et, si nécessaire, mises à jour

- ✓ Prendre toute mesure raisonnable pour effacer ou recitifier les données inexactes ou incomplètes

5. Les grands principes (6/7)

5.5 Durée de conservation limitée

= pas de conservation au-delà de ce qui est nécessaire pour la réalisation des finalités

- ✓ Finalité réalisée = données supprimées / anonymisées
- ✓ Appréciation relative à la conservation: dépend de la détermination de la finalité → analyse au cas par cas
- ✓ Pas de conservation indéfinie « au cas où »

5. Les grands principes (7/7)

5.6 Responsabilisation

= mettre en place des mesures appropriées + être capable de démontrer la conformité

- Comment?
  - ✓ Mesures organisationnelles et techniques
  - ✓ Mise en place d'une documentation pour démontrer la conformité aux règles
  - ✓ Transparence vis-à-vis des personnes concernées et de la CNPD

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

Formation CNPD:
Introduction à la protection des données

Les droits des personnes concernées

Esch-sur-Alzette

4 septembre 2018

Laurent Magnus

Service juridique

Programme

1. Introduction
2. Les notions élémentaires
3. **Les droits des personnes concernées**
4. Les obligations du responsable du traitement et du sous-traitant
5. Le rôle de la CNPD

Droits des personnes concernées

Droit à l'information

La collecte des données se fait de façon:	Directe	Indirecte
L'identité et les coordonnées du RT (& représentant)	☑	☑
Les coordonnées du DPO (si applicable)	☑	☑
La finalité du traitement, sa base légale et la precision des intérêts légitimes (si le traitement est fondé sur les intérêts légitimes)	☑	☑
Les catégories de données traitées		☑
Les (catégories de) destinataires	☑	☑
Les transferts de données vers des pays tiers (y compris les garanties)	☑	☑
La durée de conservation (ou les critères utilisés pour la déterminer)	☑	☑
Les droits des PC	☑	☑
Le droit de retirer le consentement (si applicable)	☑	☑
Le droit d'introduire une réclamation auprès d'une autorité de contrôle	☑	☑
L'origine des données		☑
Le caractère réglementaire ou contractuel de la fourniture des données, le caractère facultatif ou obligatoire et les conséquences d'un éventuel refus	☑	
L'existence d'une décision dite automatisée, y compris profilage, la logique sous-jacente ainsi que l'importance et les conséquences	☑	☑
Traitement ultérieur des données	☑	☑

Droit à l'information

Quand?

- Collecte directe:
  - Au moment de la collecte des données
- Collecte indirecte:
  - Dans un délai raisonnable (max. 1 mois après la collecte), ou
  - Collecte pour communiquer avec la PC ou envoyer les données à un autre destinataire: au plus tard lors de la première communication

Exceptions (directe)

- La PC dispose déjà des informations

Exceptions (indirecte)

- La PC dispose déjà des informations
- L'obtention ou la communication est prévue par le droit de l'Union ou de Luxembourg
- Impossible ou efforts disproportionnés
- Secret professionnel

Droit d'accès

Éléments

Le droit d'obtenir la confirmation que les données la concernant sont ou ne sont pas traitées et dans l'affirmative, des informations sur:

- Les finalités du traitement et les catégories de données
- Les destinataires (en particulier dans des pays tiers)
- La durée de conservation (ou les critères permettant de la déterminer)
- Les droits des personnes concernées
- le droit d'introduire une réclamation auprès d'une autorité de contrôle
- La source des données personnelles (le cas échéant)
- L'existence d'une décision automatisée, y compris le profilage

Le droit d'obtenir (gratuitement) une copie des données

Délai

- Dans les meilleurs délais et en tout cas endéans un mois de la demande (sauf prolongation)

Exceptions

- Le droit n'affecte pas les droits et libertés d'autrui

Droit de rectification

Contenu

- Le droit de demander :
  - Si informations **inexactes** -> rectification
  - Si informations **incomplètes** -> complétion

Délai

- Dans les meilleurs délais et en tout cas endéans un mois de la demande (sauf prolongation de deux mois)

Notification

- Obligation de notifier la rectification à chaque destinataire auquel les données ont été communiquées (sauf impossibilité ou efforts disproportionnées)
- Sur demande de la PC, le RT l'informe de ces destinataires

Droit à l'effacement

Eléments

- Droit d'obtenir l'effacement des données personnelles, si :
  - Les données ne sont plus nécessaires
  - Retrait du consentement
  - Exercice du droit d'opposition
  - Traitement illicite
  - Obligation légale

Délai

- Dans les meilleurs délais et en tout cas endéans un mois de la demande (sauf prolongation de deux mois)

Exceptions

- Pour respecter une obligation légale qui requiert le traitement
- La constatation, l'exercice ou la défense de droits en justice
- Liberté d'expression et d'information
- Finalité d'archivage (cas spécifique)
- Motifs d'intérêt publique (santé publique)

Notification

- Données ont été rendu publiques, le RT *doit* informer les autres RT
- Obligation de notifier à chaque destinataire auquel les données ont été communiquées (sauf impossibilité ou efforts disproportionnées)
- Sur demande de la PC, le RT l'informe de ces destinataires

Droit à la limitation du traitement

Contenu

- Le droit d'obtenir la limitation du traitement

Quand?

- Demande de rectification
- Demande d'opposition car traitement illicite
- Demande d'opposition car motifs légitimes
- Données ne sont plus nécessaires

Conséquences:

- Conservation des données
- « Traitement interdit »

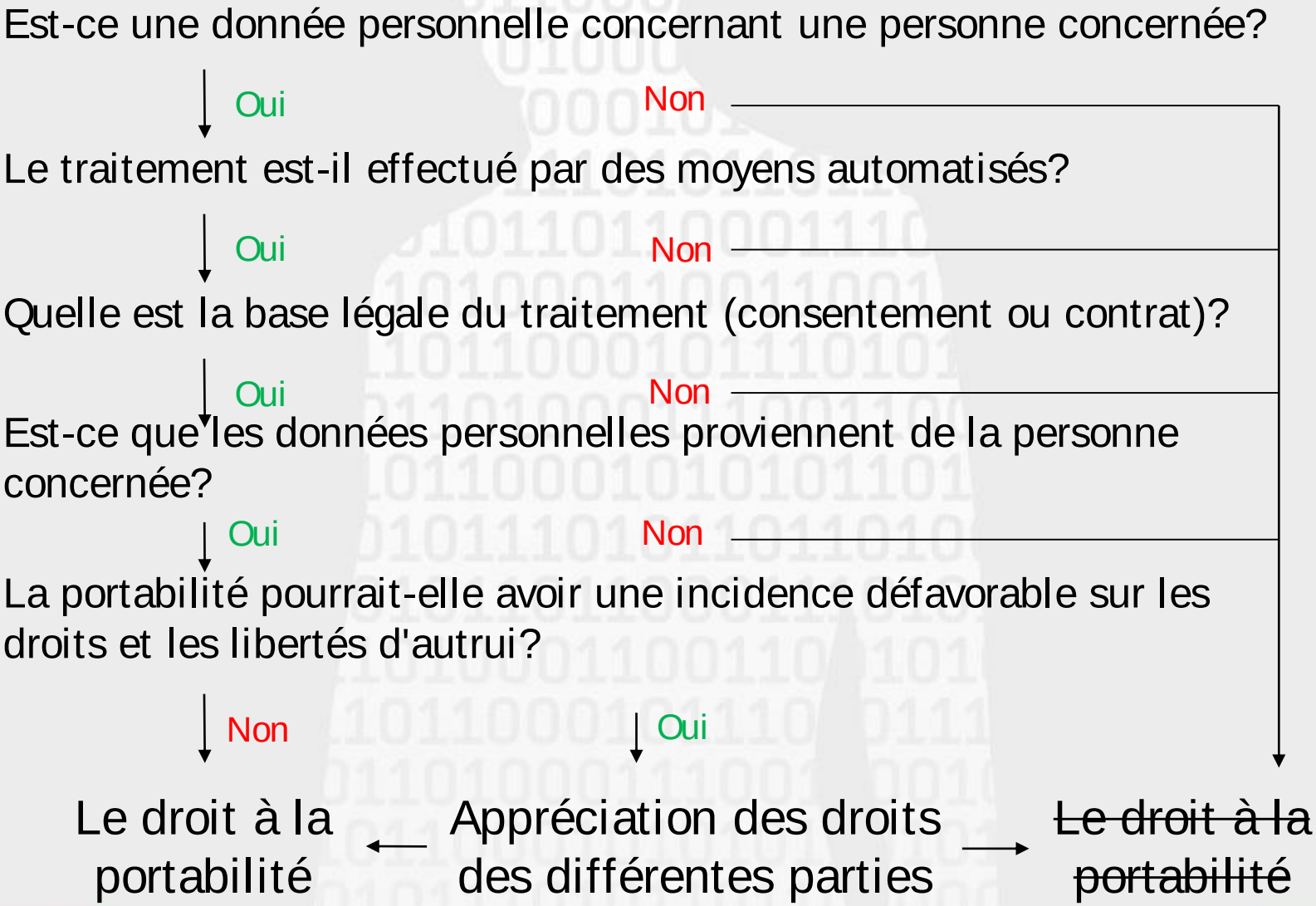
Droit à la portabilité

La personne concernée a le droit de recevoir ses données personnelles dans un format structuré, couramment utilisé et lisible par machine

-

La personne concernée a le *droit* de les transmettre, directement ou indirectement, à un nouveau responsable du traitement

Droit à la portabilité



Droit d'opposition

Le droit d'opposition

Le droit de s'opposer à tout moment, au traitement de ses données personnelles

Conditions de l'exercise

Les raisons tenant à la situation particulière de la PC
+
Intérêts légitimes **ou** l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique

Traitement à des fins de prospection (y compris profilage)

Exceptions

Motifs légitimes et impérieux du RT, qui prévalent sur les intérêts, droits et libertés de la PC

La constatation, l'exercice ou la défense de droits en justice

Conséquences et délai

- Limitation du traitement pendant le temps nécessaire pour vérifier les motifs légitimes du RT
- effacement si demandé

Dans les meilleurs délais et en tout cas endéans un mois de la demande (sauf prolongation de deux mois)

Le RT ne peut plus traiter les données à des fins de prospection

Principe - Décision individuelle automatisée

- ***Le droit de ne pas faire l'objet d'une decision…***
- ***… basée uniquement sur le traitement automatisé, y compris le profilage,…***
- ***… produisant des effets juridiques …***
- ***… ou l'affectant de manière significative de façon similaire***

Bases légales – Décision individuelle automatisée

- Le traitement peut être effectué, s'il est :

A. nécessaire à la conclusion ou à l'exécution d'un contrat

B. autorisée par le droit de l'Union ou le droit luxembourgeois et qui prévoit des mesures appropriées

C. fondée sur le consentement explicite de la personne concernée

Transparence et modalités

- Mettre en place des **procédures et mécanismes** pour faciliter l'exercice des droits
  - Revoyez les notes d'informations
    - ✓ Format concis, transparent, compréhensible et aisément accessible
    - ✓ Utilisez des termes clairs et simples
  - Revoyez les procédures actuelles relatives à l'exercice des différents droits des personnes concernées
    - ✓ Tenir compte des délais strictes pour répondre
    - ✓ Fournir un accès facile à l'exercice des différents droits
    - ✓ Mesures techniques et organisationnelles
      - ✓ Ex. organisation interne, formation des employés, contrats avec les sous-traitants, structure informatique, mise à jour de la liste des destinataires

Transparence et modalités

- Principe de gratuité, sauf si la demande est manifestement infondée ou excessive, notamment en raison du caractère répétitif
  - Possibilité de rejeter la demande ou demander le paiement des frais raisonnables
- Bonne collaboration du RT dans l'exercice des droits de la PC
  - Réactivité
  - Ponctualité
  - Transparence

Transparence et modalités

Définir le service ou personne en charge des demandes → Vérification de l'identité de la PC → *Analyser la nature du/des droits* → *Accusé bonne réception de la demande*

Fournir des informations sur les mesures prises dans les meilleurs délais

Informations communiquées endéans 1 mois

Informations ne peuvent pas être communiquées endéans 1 mois:

- informer la PC endéans 1 mois de la réception de la demande
- indiquer les motifs du report
- prolongation de 2 mois

Si le RT ne donne pas suite:

- informer la PC endéans 1 mois de la réception de la demande
- indiquer les motifs et le droit d'introduire une plainte

Voies de recours

Droit d'introduire une réclamation auprès de la CNPD

- **OU?**
  - autorité de sa **résidence habituelle**,
  - autorité de son **lieu de travail**
  - Autorité du lieu où la **violation aurait été commise**.

- L'autorité de contrôle doit informer la personne concernée dans un délai de 3 mois.

Droit à un recours juridictionnel contre l'autorité de contrôle

- Droit reconnu à toute personne physique ou morale de former un recours juridictionnel effectif contre une « **décision juridiquement contraignante de l'autorité de contrôle** qui la concerne », ou contre un **défaut de réponse dans un délai de 3 mois**.

- Sont compétentes les juridictions de l'État membre sur le territoire duquel l'autorité de contrôle est établie.

Droit de recours juridictionnel contre le responsable du traitement ou sous-traitant

- **Droit reconnu à toute personne physique de former un recours juridictionnel effectif** en cas d'atteinte à leurs droits, tant contre le responsable du traitement que contre le sous-traitant (soit devant les juridictions de l'État membre dans lequel le responsable dispose d'un établissement, soit devant les juridictions de l'État où la personne a sa résidence habituelle).

Voies de recours

Droit à réparation

Principe de la réparation du **préjudice matériel ou moral** subi par toute personne résultant d'une violation du Règlement, pouvant être obtenue du responsable du traitement ou du sous-traitant.

Sous-traitant: Non respect des obligations du RGPD qui lui incombent OU agit en-dehors des instructions licites du responsable du traitement

Si responsabilité du **responsable du traitement + sous-traitant** : responsabilité du dommage dans sa totalité

Merci pour votre attention !

Formation CNPD:
Introduction à la protection des données

Les obligations du responsable du traitement et du sous-traitant

Esch-sur-Alzette

4 septembre 2018

Arnaud Habran

Service juridique

Programme

1. Introduction
2. Les notions élémentaires
3. Les droits des personnes concernées
4. **Les obligations du responsable du traitement et du sous-traitant**
5. Le rôle de la CNPD

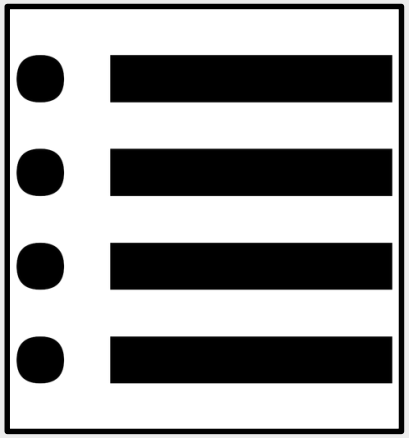

Obligations du responsable du traitement
Principes de qualité des données
Registre des activités
Sécurité et notification de violation de données
Analyse d'impact
Délégué à la protection des données
Sous-traitance
Transferts vers des pays tiers
Droits des personnes concernées
Gouvernance interne

1. Principes de qualité des données

Licéité, loyauté et transparence	Limitation des finalités	Minimisation des données
Exactitude des données	Durée de conservation	Intégrité et confidentialité

Responsabilisation

2. Registre des activités de traitement



Un document/fichier qui reprend la description de l'ensemble de vos traitements

RGPD: Registre qui, pour chaque activité de traitement, comporte notamment les informations suivantes:

a) le nom et les coordonnées du responsable du traitement (…)
b) les finalités du traitement;
c) une description des catégories de personnes concernées et des catégories de données à caractère personnel;
d) les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées (…)
e) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale(…)
f) dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données;
g) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles (…)

Exemples:

- « Compliance Support Tool » de la CNPD qui **permet aussi de générer un registre**
- Autres outils: CPVP (Commission belge), CNIL (Commission française)

Réutilisation: Le règlement n'est pas prescriptif quant à la forme du registre. Alors que les exemples ci-dessus peuvent vous aider à construire un registre nous vous recommandons de produire un registre qui est cohérent avec votre organisation – en terme de forme et vocabulaire utilisé.

2. Registre des activités de traitement

Checklist simplifiée

Objectif: Fournir une **aide pragmatique** afin d'évaluer de manière simple votre niveau de **maturité par rapport à un traitement de données**

La checklist proposée se concentre sur les principes de la protection des données du RGPD (art. 5). Sans être exhaustive elle peut cependant constituer un outil pragmatique. Ainsi elle peut constituer un élément de début – pour les question plus approfondies nous proposons de se référer aux chapitres respectifs du RGPD.

2. Registre des activités de traitement

Checklist simplifiée

Fiche signalétique

Rôles et responsabilités

- Analysez si vous êtes l'entreprise qui décide ce qui est fait avec les données ou si vous êtes exécutant

Données traitées

- Enumérer les types de données traitées (p.ex. noms, adresses, certificats de maladie, comptables,….)

Personnes concernées

- Enumérer les types personnes sur lesquelles porte le traitement (p.ex. clients, salariés, prospects, potentiels recrutés,…)

Finalité du traitement

- Décrire l'objectif que le traitement permet d'atteindre (p.ex. paiement des salaires, envoie de factures, prospection de potentiels clients,…)

Suppression

- Décrire quand les données seront effacées ou la durée de conservation

Flux de données

- Analysez si vous recevez ou transmettez les données à une autre organisation, y compris hors l'Union européenne

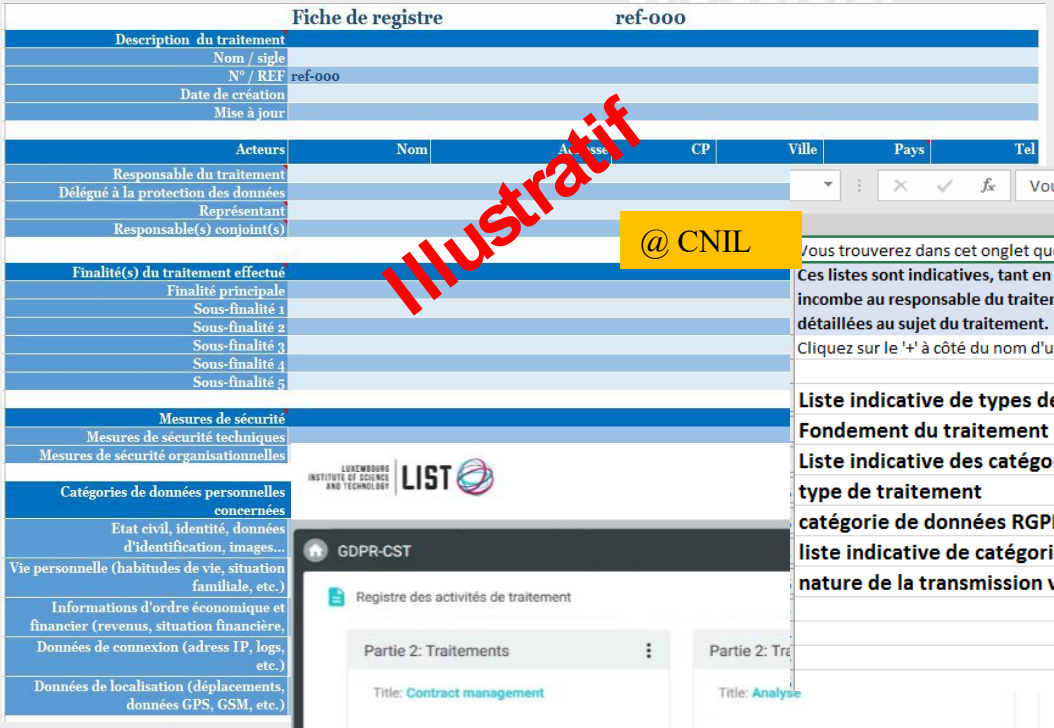
Cette fiche signalétique est inspirée des informations qui doivent figurer dans un « registre des activités de traitement » tel que défini dans l'article 30 du RGPD.

Questionnaire

	Questions	Remarque
1	Est-ce que j'ai le droit d'effectuer ce traitement?	**Principe: licéité**
2	Est-ce que les personnes concernées sont au courant du traitement?	**Principe: transparence**
3	Est-ce que je sais avec précision pourquoi je collecte ces données? / Est-ce que j'utilise ces données pour faire autre chose?	**Principe: limitation des finalités**
4	Est-ce que toutes les données sont nécessaires – pas seulement utiles?	**Principe: minimisation**
5	Est-ce que les données sont correctes et à jour?	**Principe: exactitude**
6	Est-ce que je dois supprimer les données à la fin du traitement – ou est-ce qu'il y a une nécessité (pas une utilité) de les garder?	**Principe: durée de conservation limitée**
7	Est-ce que les données sont sécurisées?	**Principe: sécurité**

Le questionnaire est inspiré des « principes relatifs au traitement de données à caractère personnel » tel que défini dans l'article 5 du RGPD.

2. Registre – quelques exemples



Fiche de registre	ref-000
Description du traitement	
Nom / sigle	
N° / REF	ref-000
Date de création	
Mise à jour	

Acteurs	Nom	Adresse	CP	Ville	Pays	Tel
Responsable du traitement						
Délégué à la protection des données						
Représentant						
Responsable(s) conjoint(s)						

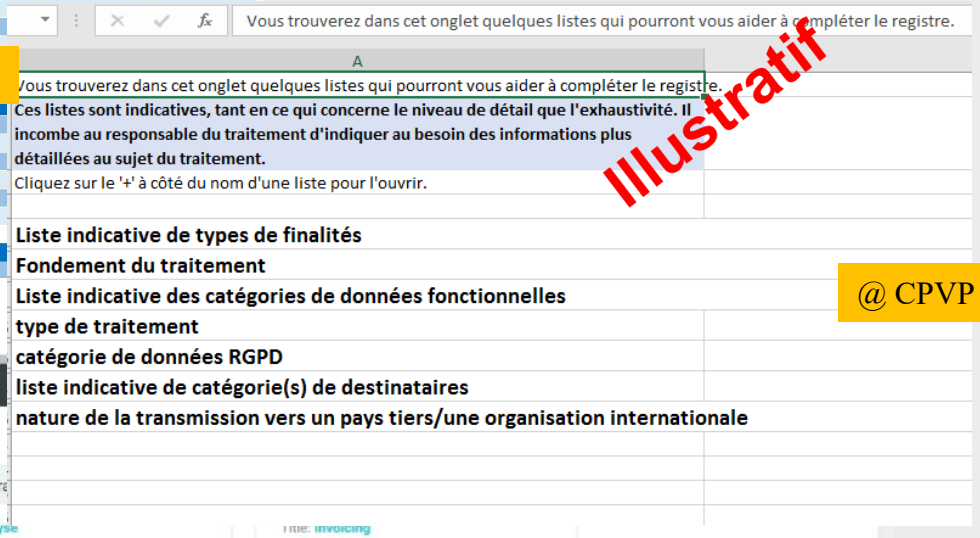
Finalité(s) du traitement effectué
Finalité principale
Sous-finalité 1
Sous-finalité 2
Sous-finalité 3
Sous-finalité 4
Sous-finalité 5

Mesures de sécurité
Mesures de sécurité techniques
Mesures de sécurité organisationnelles

Catégories de données personnelles concernées
Etat civil, identité, données d'identification, images...
Vie personnelle (habitudes de vie, situation familiale, etc.)
Informations d'ordre économique et financier (revenus, situation financière,
Données de connexion (adress IP, logs, etc.)
Données de localisation (déplacements, données GPS, GSM, etc.)

Illustratif

@ CNIL

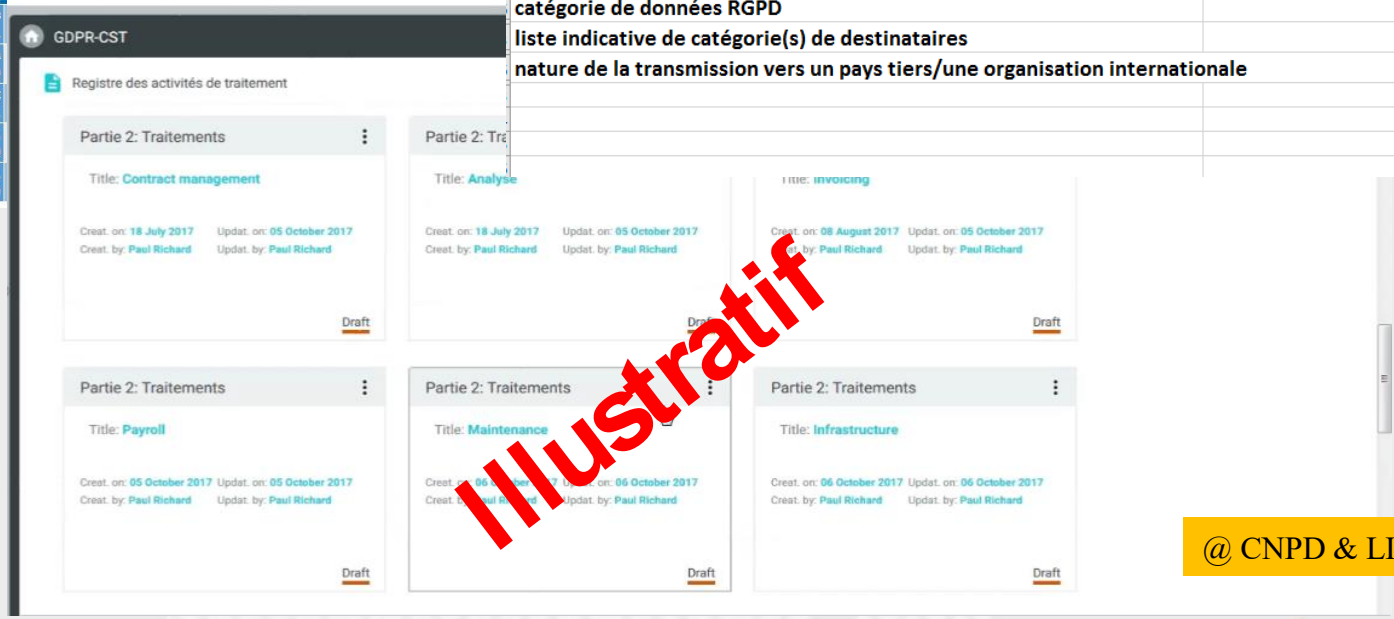


Vous trouverez dans cet onglet quelques listes qui pourront vous aider à compléter le registre.

A
Vous trouverez dans cet onglet quelques listes qui pourront vous aider à compléter le registre.
Ces listes sont indicatives, tant en ce qui concerne le niveau de détail que l'exhaustivité. Il incombe au responsable du traitement d'indiquer au besoin des informations plus détaillées au sujet du traitement.
Cliquez sur le '+' à côté du nom d'une liste pour l'ouvrir.
Liste indicative de types de finalités
Fondement du traitement
Liste indicative des catégories de données fonctionnelles
type de traitement
catégorie de données RGPD
liste indicative de catégorie(s) de destinataires
nature de la transmission vers un pays tiers/une organisation internationale

Illustratif

@ CPVP



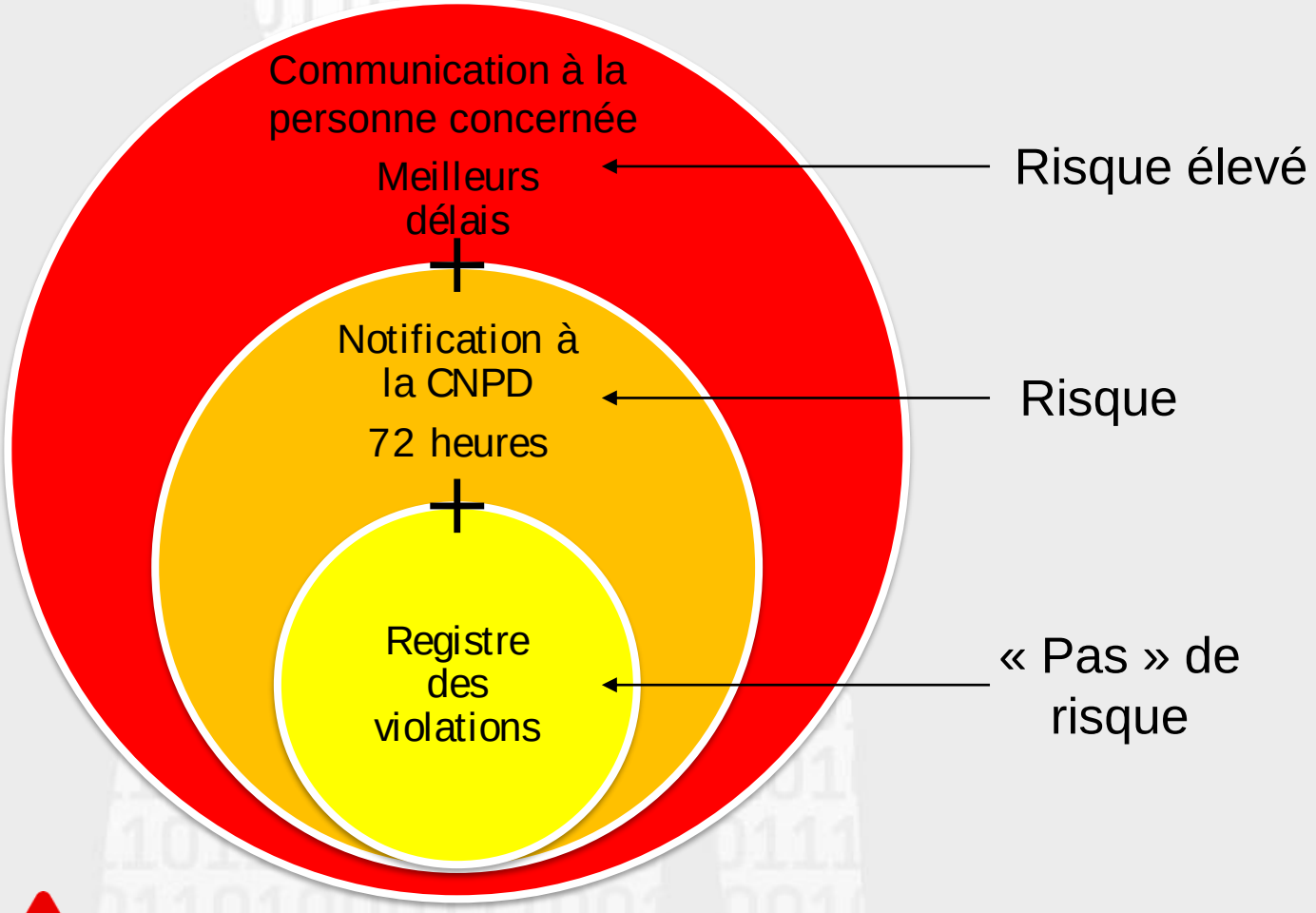
Illustratif

@ CNPD & LIST

3. Sécurité et notification de violations de données

- Mesures techniques et organisationelles selon :
  - “ l’état de l’art”
  - le risque pour les personnes concernées
- Mesures pour traiter les risques doivent être adaptées au contexte et aux spécificités du domaine concerné :
  - Analyse des risques en fonction de la nature des données, de prescriptions légales, de la complexité du système, etc.
- Mesures doivent être régulièrement mises à jour / adaptées :
  - Nouvelles menaces tous les jours
  - Nouvelles vulnérabilités découvertes
  - Changement du contexte de l'organisation → nouveaux risques

3. Sécurité et notification de violations de données



Obligation du sous-traitant de notifier au responsable du traitement toute violation de données dans les meilleurs délais après en avoir pris connaissance

4. Analyse d'impact

Lorsqu'un traitement est susceptible d'exposer les personnes à un risque élevé

Le RT doit effectuer une

analyse d'impact

relative à la protection des données pour évaluer la particularité et la gravité de ce risque

(***Data Protection Impact Assessment - DPIA***)

p.ex. service de location vélos avec géolocalisation

4. Analyse d'impact

Les critères suivants doivent être pris en compte pour déterminer la nécessité d'une analyse d'impact:

- Évaluation ou notation, y compris le profilage
- Décision individuelle automatisée avec effet juridique ou effet similaire significatif
- Surveillance systématique des personnes concernées
- Données sensibles ou données à caractère hautement personnel
- Données traitées à grande échelle
- Croisement ou combinaison d'ensembles de données
- Données concernant des personnes vulnérables
- Utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles
- Traitements qui empêchent les personnes concernées d'exercer un droit ou de bénéficier d'un service ou d'un contrat

5. Délégué à la protection des données

Délégué à la protection des données obligatoire après 25 mai 2018 si:

- Autorité ou organisme public
- Entreprise remplissant certains critères (p.ex. traitements à grande échelle de données sensibles)

Rôle: Mission d'information, de conseil, de contrôle interne et de point de contact avec l'autorité de contrôle.

5. Délégué à la protection des données

Pilote à bord!

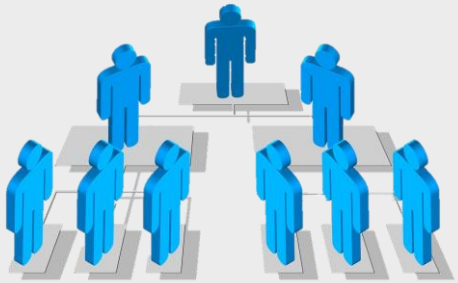
Atout majeur pour: respecter les obligations du RGPD, dialoguer avec les autorités de contrôle, réduire les risques de contentieux

6. Sous-traitance

- Le responsable du traitement doit :
  - Choisir un sous-traitant adéquat et toujours garder le contrôle de la sous-traitance
  - Maîtriser la sous-traitance en cascade
  - Conclure avec chaque sous-traitant un **contrat écrit** prévoyant, entre autres, que:
    - le sous-traitant ne traite les données que sur instruction documentée du responsable du traitement
    - les obligations du responsable du traitement (p.ex. en matière de mesures de sécurité, confidentialité) incombent également au sous-traitant
    - le sous-traitant doit assister le responsable du traitement (p.ex. droits des PC, violations de données)

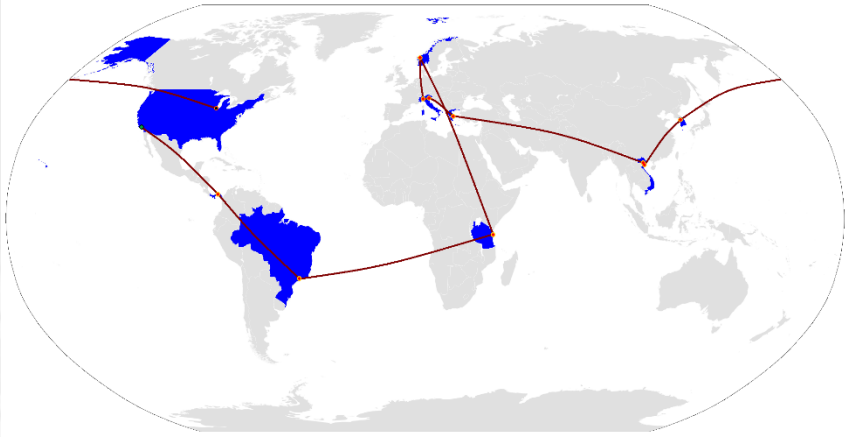
6. Sous-traitance

- Obligations des sous-traitants
  - Le sous-traitant ne traite les données que sur instruction documentée du responsable du traitement
    - Respect du contrat conclu avec le responsable du traitement
    - Si un sous-traitant détermine les finalités et les moyens du traitement, il devient le responsable du traitement
  - Sous-traitance en cascade
  - Mesures de sécurité
  - DPO
  - Registre
  - Transfert de données vers des pays tiers
  - Notification violations des données
  - Coopération avec la CNPD

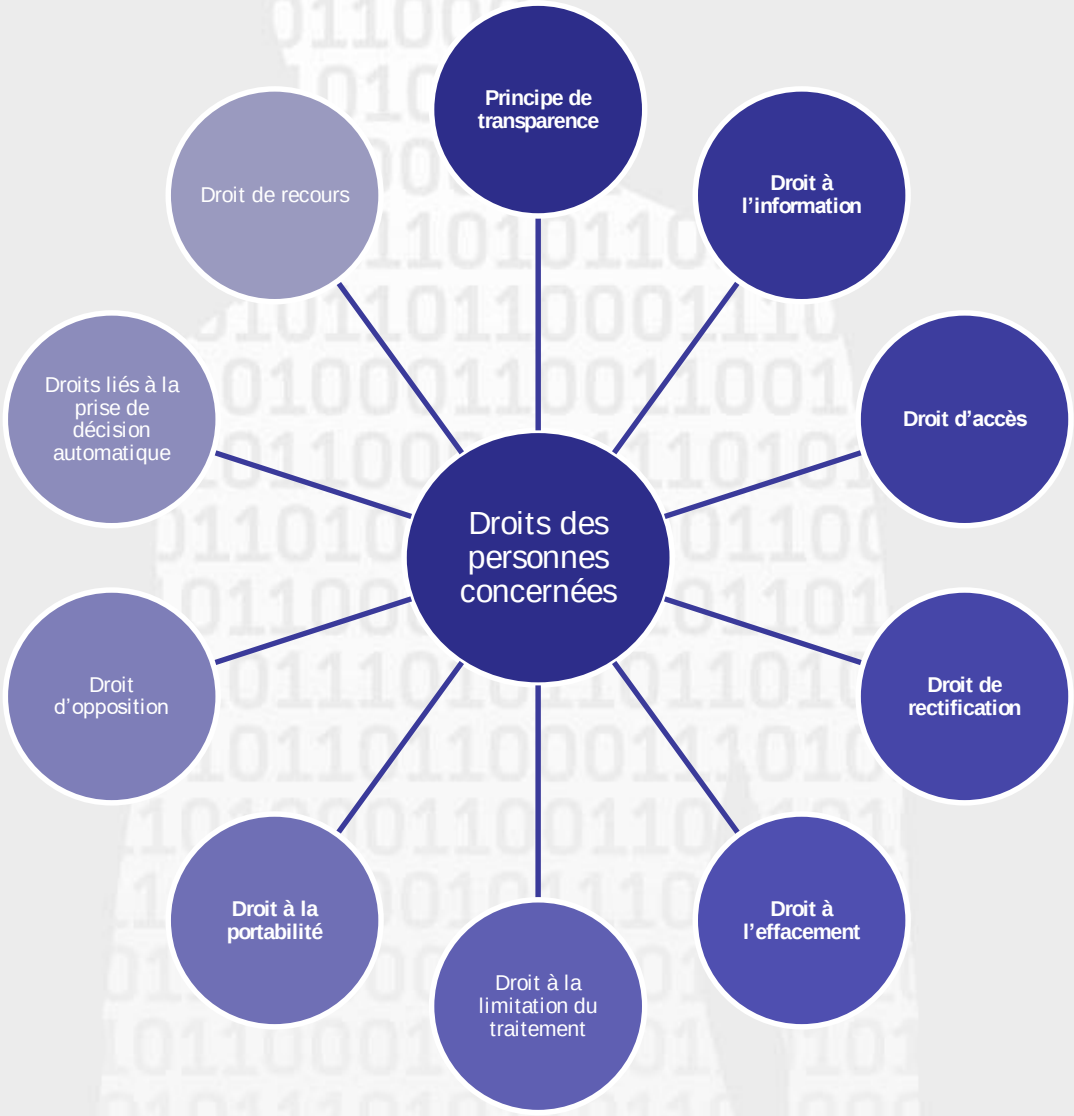


7. Transferts pays tiers

- Libre circulation des données au sein de l'UE/EEE
- Transferts de données vers des pays tiers (= en dehors de l'UE) uniquement possibles si:
  - Décision d'adéquation
  - Garanties appropriées (p.ex. BCR ou clauses contractuelles types, etc.)
  - Dérogations pour transferts spécifiques (p.ex. consentement, contrat, etc.)

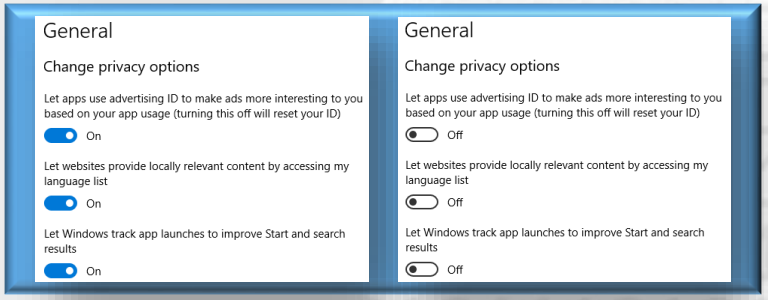


8. Droits des personnes concernées



9. Gouvernance interne

- Créer une **culture globale** de la protection des données
- Implémenter la protection des données **dès la conception et par défaut**



(*Privacy by design*)

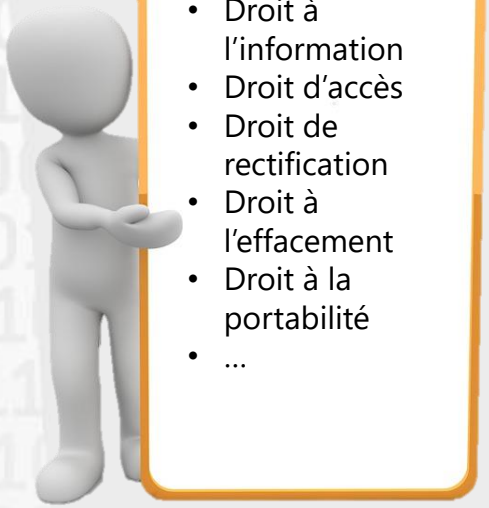
(*Privacy by default*)

- **Anticiper** dès le départ les risques et problèmes
- Etre prêt à réagir en cas de **violations de données**
- Développer une gestion sécurisée de l'information **tout le long du cycle de vie** des traitements de données

9. Gouvernance interne

- **Sensibiliser** vos collaborateurs
- **Organiser** des procédures internes (ex. internal reporting)

- Mettre en place des procédures pour traiter les **réclamations** et les demandes des personnes concernées quant à **l'exercice de leurs droits**
- **Informer les PC en toute transparence** sur l'ensemble de leurs droits



9. Gouvernance interne

- **Documenter la conformité**
  - Registre des traitements,
  - DPIA,
  - Encadrement des transferts de données hors de l'UE,
  - Registre des violations,
  - Contrats avec sous-traitants,
  - …
- **Obligation de coopération avec la CNPD**

Formation CNPD:
Introduction à la protection des données

Présentation de l'autorité de contrôle luxembourgeoise

Esch-sur-Alzette

4 septembre 2018

Dani Jeitz

Service juridique

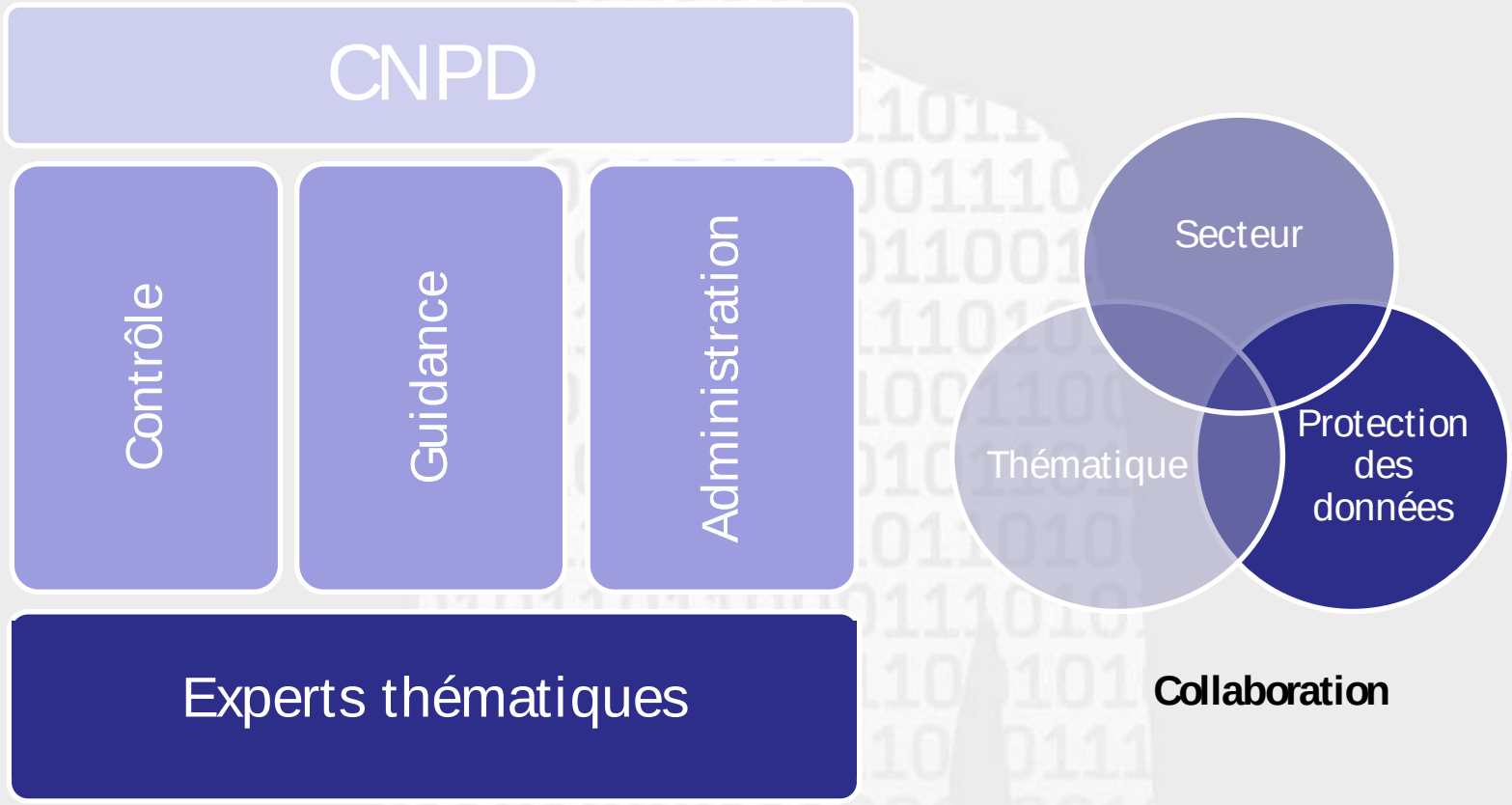
Programme

1. Introduction
2. Les notions élémentaires
3. Les droits des personnes concernées
4. Les obligations du responsable du traitement
5. **Le rôle de la CNPD**

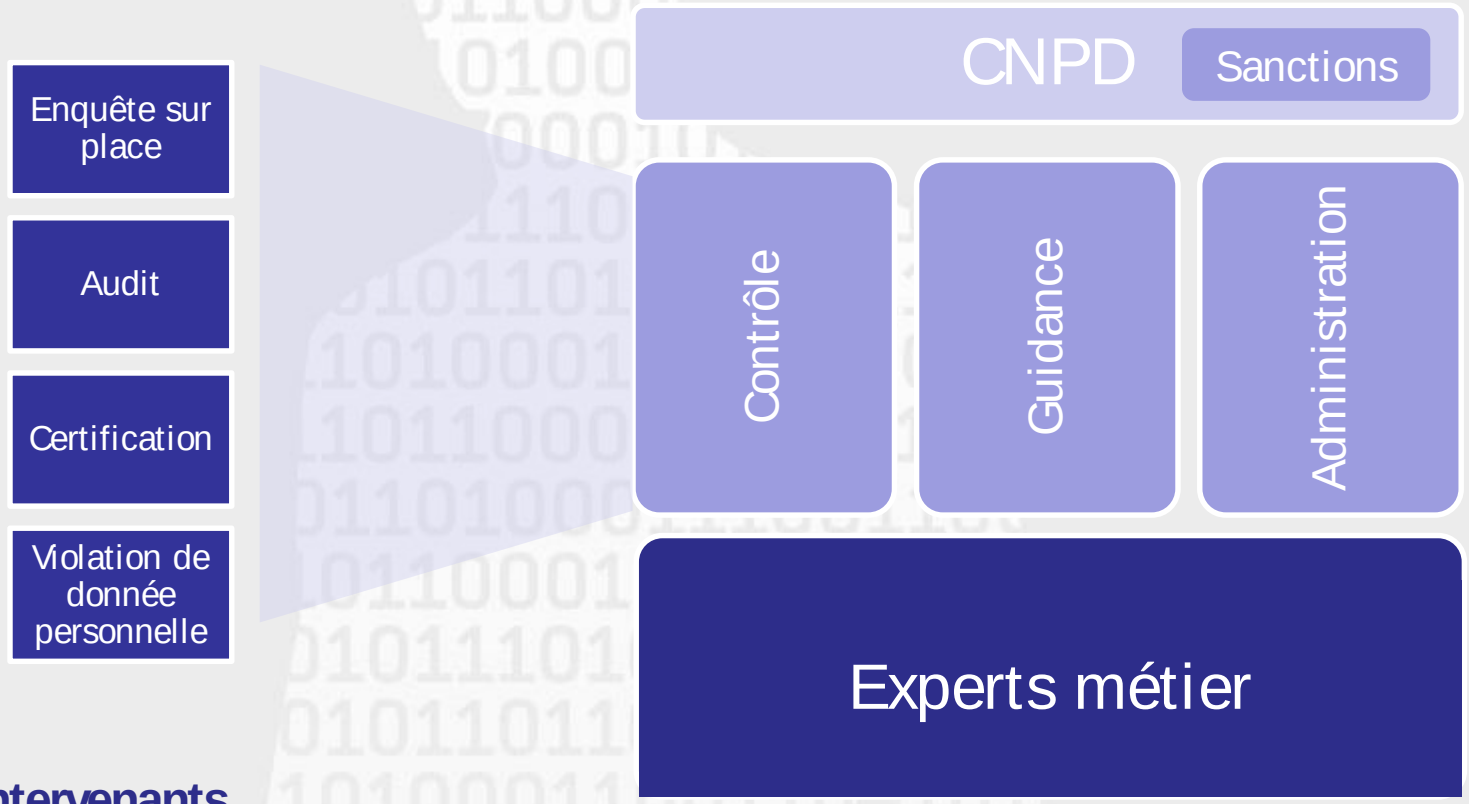
Introduction

- Autorité indépendante organisée par la loi du 1ier août 2018
- Etablissement public avec autonomie financière et administrative doté de la personnalité juridique
- Contrôle et vérifie la conformité au / à:
  - RGPD;
  - la loi du 1ier août 2018 ayant des dispositions spécifiques:
    - Liberté d'expression et d'information
    - Recherche scientifique / historique ou statistiques
    - Catégories particulières de données à caractère personnel
  - la loi du 1ier août 2018 en matière pénale / sécurité nationale;
  - la loi modifiée du 30 mai 2005 (communications électroniques).

Nouvelle structure interne (1/2)



Nouvelle structure interne (2/2)



Les intervenants

Collège

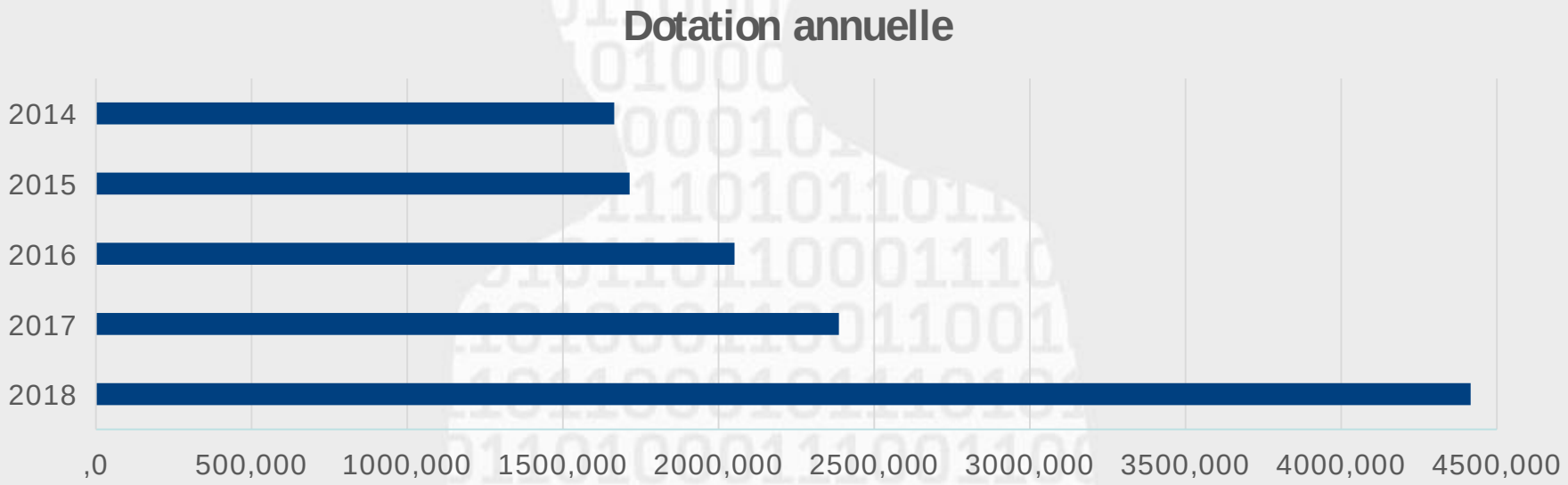
Chef d'enquête

Enquêteur

Expert

Coopération européenne

Evolution de la CNPD



Personnel

2014	2017	2018
15	25	35

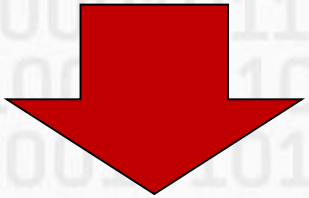
Compétence territoriale de la CNPD

- Compétence sur le territoire luxembourgeois
- L'introduction du **« guichet unique »**
  - Un point de contact pour les entreprises établies dans plusieurs États membres
  - l'**autorité « chef de file »** est:
    - lieu de l'établissement principal du responsable
    - lieu de l'établissement unique
- Coopération européenne renforcée entre l'autorité « chef de file » et les autorités « concernées »
  - But: prise de décisions uniques
  - En cas de désaccord→ décision contraignante par le « Comité européen pour la protection des données »

Changement de paradigme

Suppression des formalités préalables (notifications / autorisations)

Contrôle a priori



Principe de la responsabilisation

“Accountability”

Contrôle a posteriori

Nouvelle approche **moins bureaucratique**, mais **plus exigeante** pour tous les acteurs

Missions (1)

- Contrôler l'application et le respect de la législation relative à la protection des données
- Information et sensibilisation de tous les acteurs
- Avis au législateur et recommandations au gouvernement
- Traiter des réclamations et effectuer des enquêtes
- Agréer les organismes de certification
- Coopération avec les autres autorités de contrôle
- Publication d'un rapport annuel comprenant:
  - une liste des types de violations notifiées
  - une liste des types de sanctions imposées

Missions (2)

- Vérifier les notifications de violations de données
- DPIA: Consultation préalable de la CNPD si risque(s) résiduel(s) élevé(s) non traité(s)
- Surveillance sur le lieu du travail (art. L. 261-1 CT):
  - demande d'avis préalable à la CNPD:
    - par la délégation ou à défaut les salariés concernés
    - délai de 15 jours suivant l'information préalable
  - CNPD doit se prononcer dans le mois de la saisine
  - demande a un effet suspensif pendant ce délai.

Missions (3)

- Extension du champ de compétences aux traitements en matière pénale / sécurité nationale:
  - Situation ancienne: autorité de contrôle « article 17 » (Procureur général d'Etat + 2 membres de la CNPD)
  - Loi du 1ier août 2018 transposant la directive 2016/680:
    - Traitements mis en œuvre par des autorités compétentes à des fins pénales: compétence de la CNPD
    - Exception pour les traitements des juridictions + Ministère public lors de leurs fonctions juridictionnelles : contrôle d'une autorité de contrôle judiciaire, distincte de la CNPD

Pouvoirs d'enquête

- Article 58 du RGPD: Chaque autorité de contrôle dispose de tous les pouvoirs d'enquête suivants:
  - mener des enquêtes sous la forme d'audits sur la protection des données;
  - obtenir du responsable du traitement et du sous-traitant l'accès à toutes les données à caractère personnel […];
  - obtenir l'accès à tous les locaux du responsable du traitement et du sous-traitant […].

La bonne balance

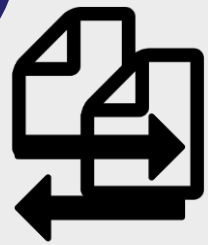
Types de contrôle

Enquête sur place

- Inspection sur site
- Périmètre ciblé
- Intervention ponctuelle

Enquête sur dossier

- Transmission d'un questionnaire
- Analyse des réponse / éléments fournis
- Adaptation de l'approche si nécessaire / utile



Audit sur la protection des données

- Revue plus approfondie
- Plusieurs échanges physiques et formels
- Périmètre plus large et adapté en fonction de l'évolution du dossier

Pouvoir d'adopter des mesures correctrices

- Pouvoir d'avertissement et de rappel à l'ordre
- Ordonner la mise en conformité d'un traitement
- Limiter (temporairement / définitivement) ou interdire un traitement
- Pouvoir d'imposer des amendes administratives
  - Innovation majeure pour le Grand-Duché
  - Imposées en complément ou à la place des autres mesures correctrices

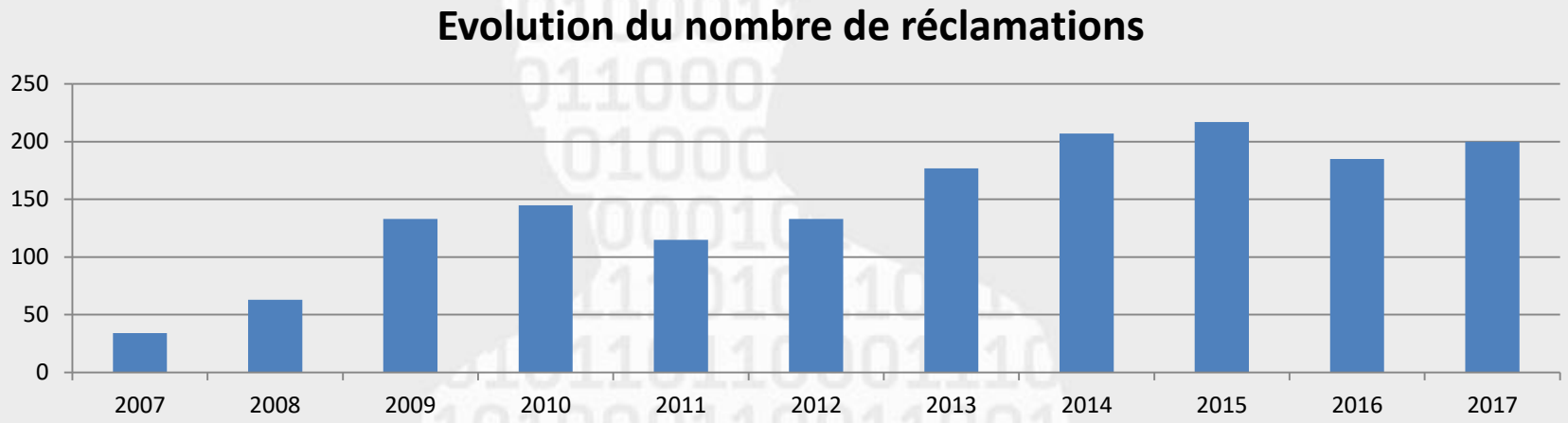
Une amende peut aller, au maximum, jusqu'à **20.000.000 EUR** ou, dans le cas d'une entreprise, à 4% de son chiffre d'affaires annuel total au niveau mondial.

Voies de Recours

- Droit pour tout individu d'introduire une réclamation
  - Auprès de l'autorité de sa résidence habituelle, de son lieu de travail ou de celle où la violation aurait été commise

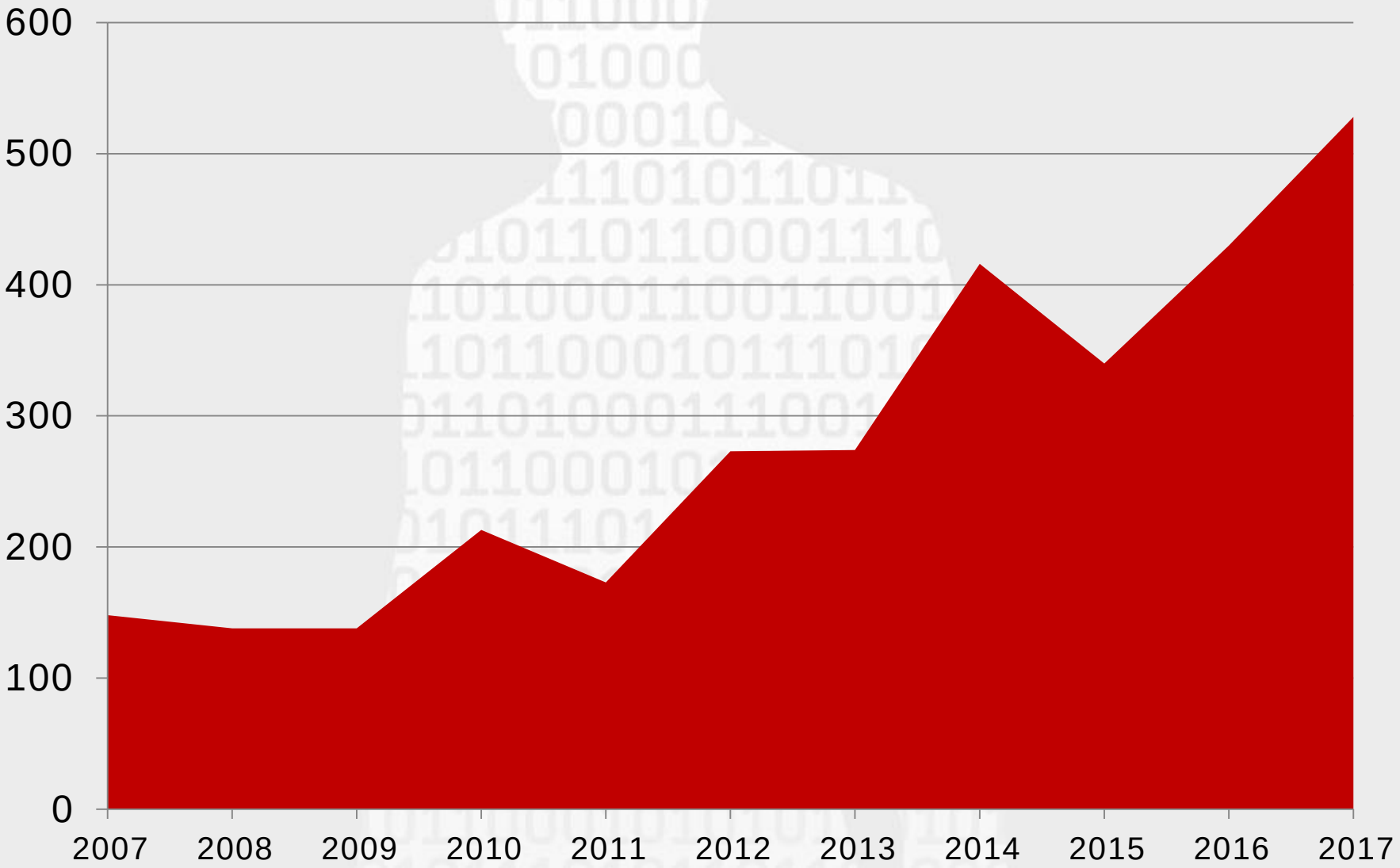
- Droit à un recours juridictionnel effectif contre l'autorité de contrôle
  - contre une *« décision juridiquement contraignante qui la concerne »*
  - contre un défaut de réponse dans un délai de 3 mois
  - compétence des juridictions de l'État membre sur le territoire duquel l'autorité de contrôle est établie
    - compétence du Tribunal administratif luxembourgeois qui statue comme juge du fond

Augmentation des réclamations (2017)

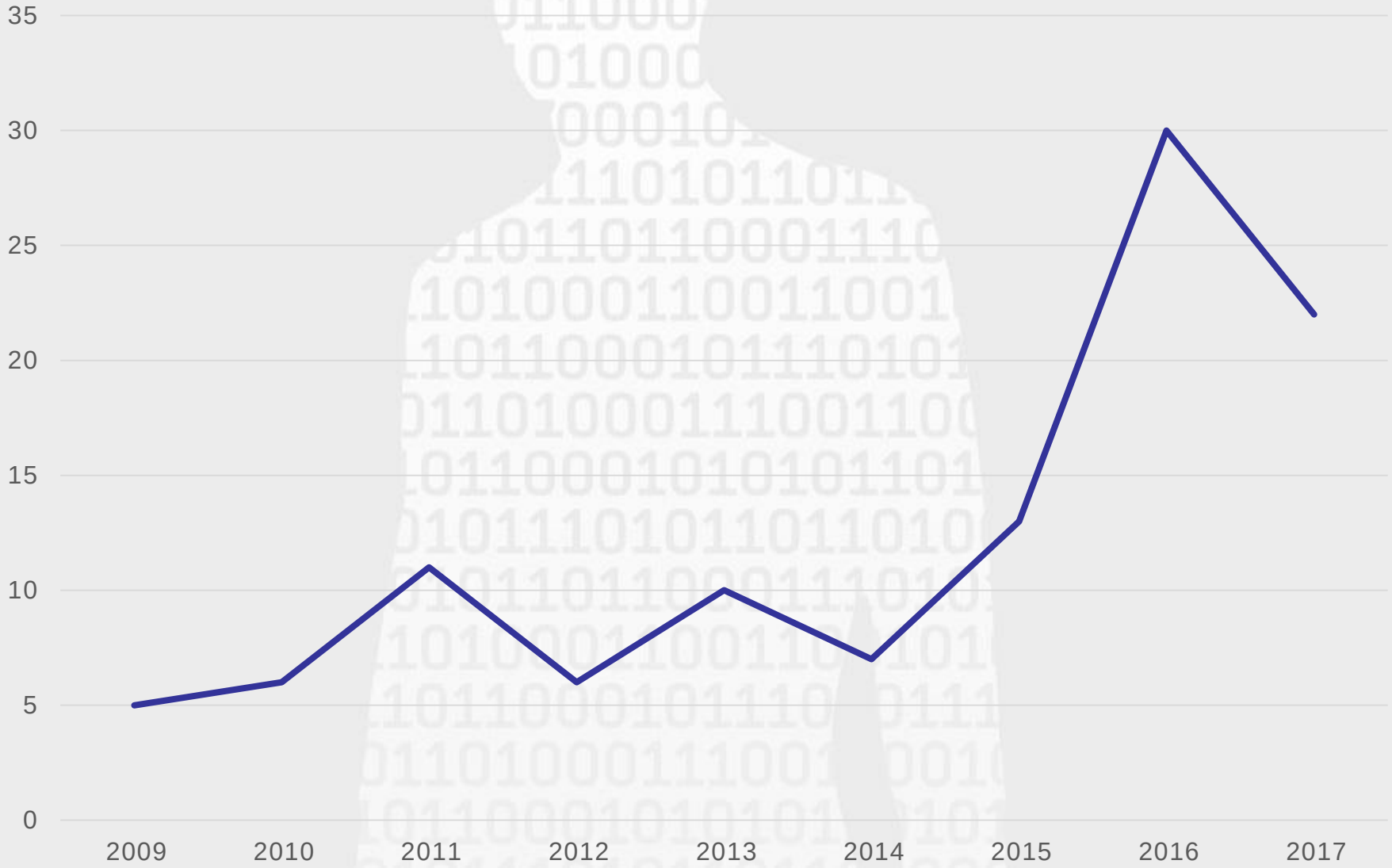


- Licéité de certaines pratiques administratives/commerciales (30%)
- Refus d'accéder aux données (13,5%)
- Transmission déloyale à des tiers (18.5%)
- Surveillance sur le lieu de travail / vidéosurveillance (12%)
- Demande d'effacement ou de rectification des données (12%)
- Opposition à la prospection (5%)
- Exercice du droit à l'oubli (5%)
- Autres (4%)

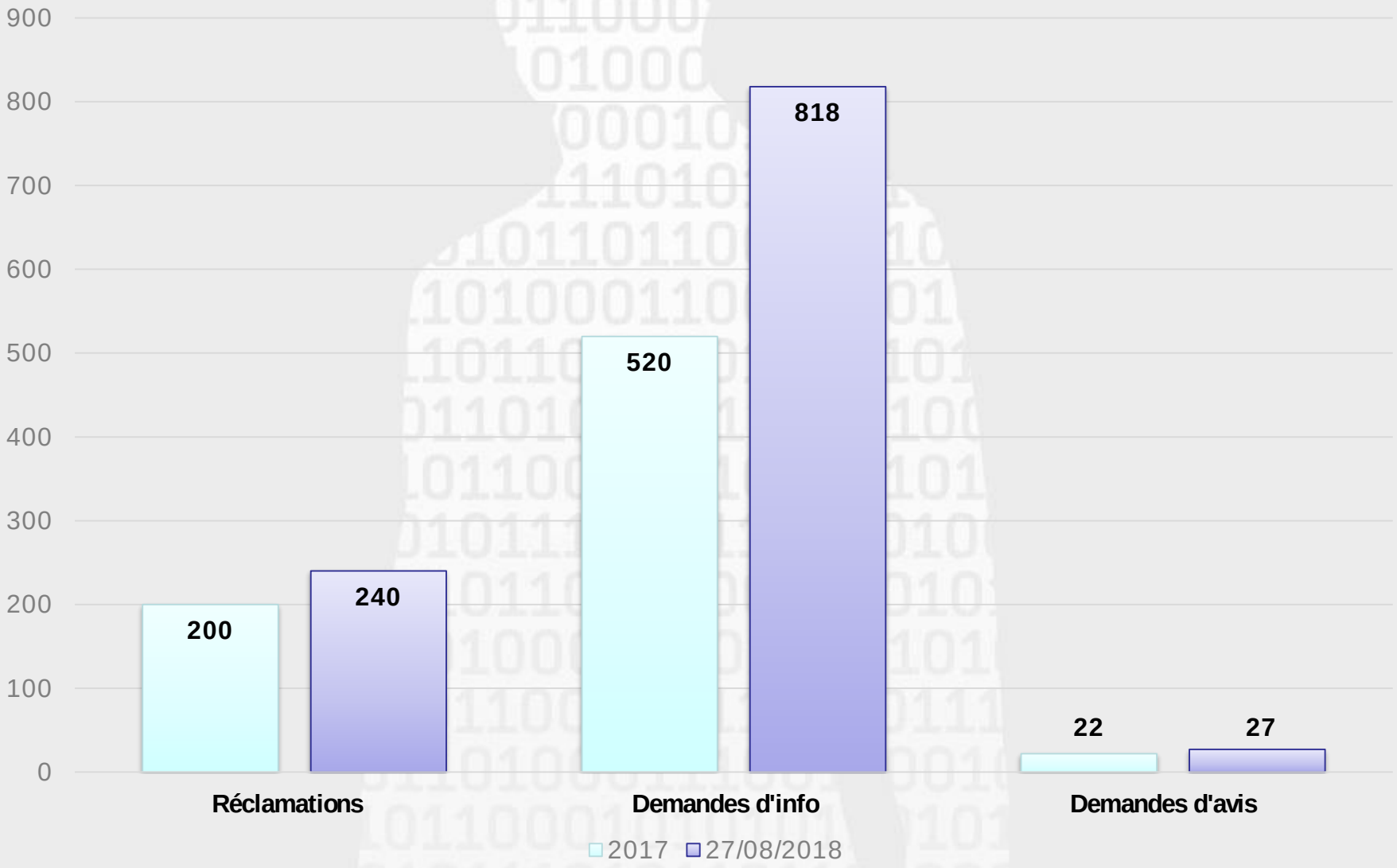
Augmentation des demandes écrites de renseignement (2017)



Avis sur des textes législatifs - 2017



Statistiques pour 2018



Commission nationale pour la protection des données

Merci pour votre attention!