Le règlement européen relatif à la protection des données

JCA 2017

20 octobre 2017

Alain Herrmann (Conformité)

Certifications / Codes de conduite

Violation de données

Agenda

A propos de la CNPD

Une evolution nécessaire

RGPD: outils et mécanismes

Nos missions

Assurer le respect des dispositions de la règlementation sur la protection des données

Notifications, autorisations	Plaintes	Investigations
Sanctions administratives + engager des procedures judiciaires	Coopérer avc les autres DPA + representer le Luxembourg au WP de l'"Article 29"	Conseiller le législateur et donner des recommendations en matière de PDD au gouvernement
Sensibiliser le public	Guidance aux responsables de traitement et sous-traitants	Tenir un registre public des traitements

Chiffres clés 2016

+130%

30 avis sur les textes légaux

185 Plaintes

+30%

1’449 Demandes d’autorisation

77 investigations

+39%

1’003 Notifications

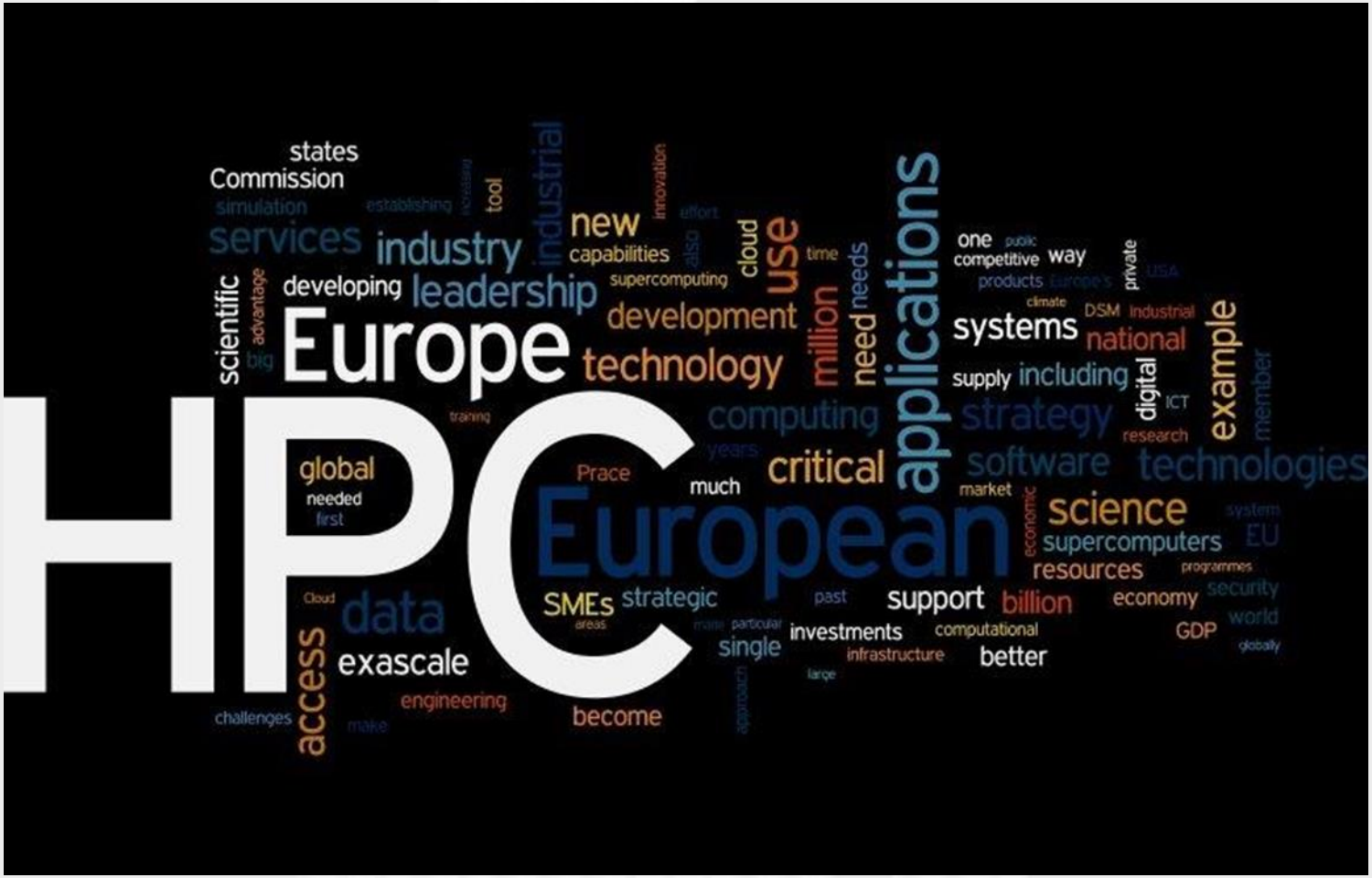
430 demandes d’information écrites

+27%

198 réunions de guidance

Une evolution nécessaire

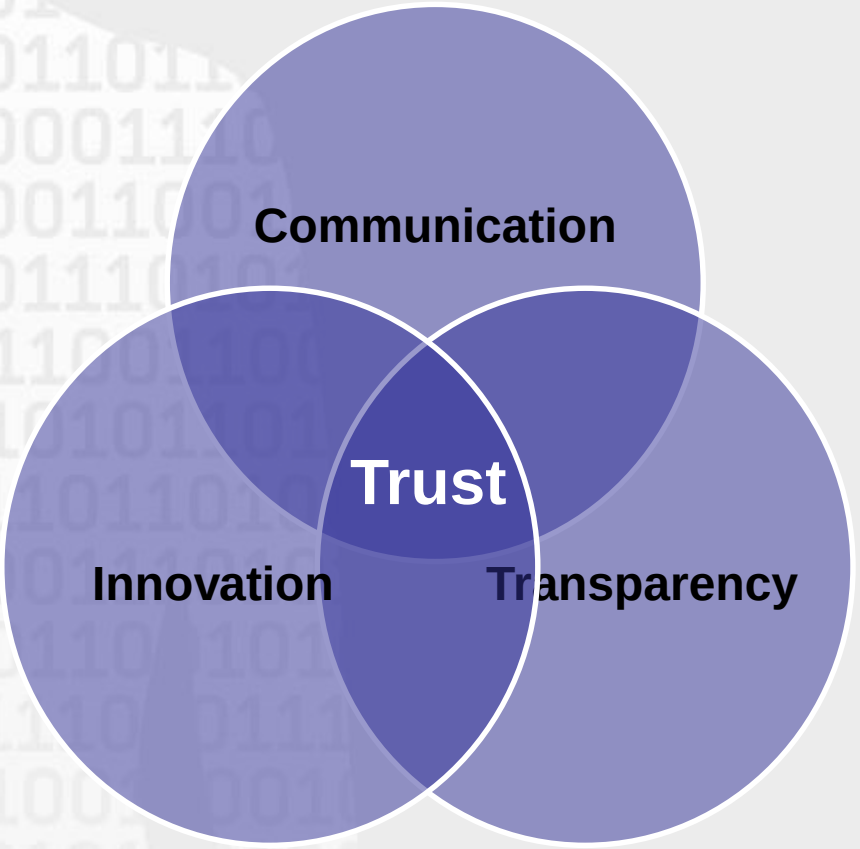
Pourquoi une réforme?



Data protection – créer de la confiance

- De nouvelles règles sont nécessaires pour assurer la confiance et la transparence

- Protection des données
  - Du papier aux personnes
  - De tâches administratives à une mise en oeuvre effective



Pourquoi une réforme?

Législation actuelle existe depuis 1995

Évolution de la manière dont les données sont collectées et utilisées

- Émergence de nouvelles technologies et services en ligne
- Effets de la globalisation

Disparités dans la mise en œuvre de la directive de 1995 ont donné lieu à des incohérences

Règlement général sur la protection des données (RGPD)

4.5.2016 FR Journal officiel de l'Union européenne L 119/1

I

(Actes législatifs)

RÈGLEMENTS

GDPR

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)

Règlement général sur la protection des données (RGPD)

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

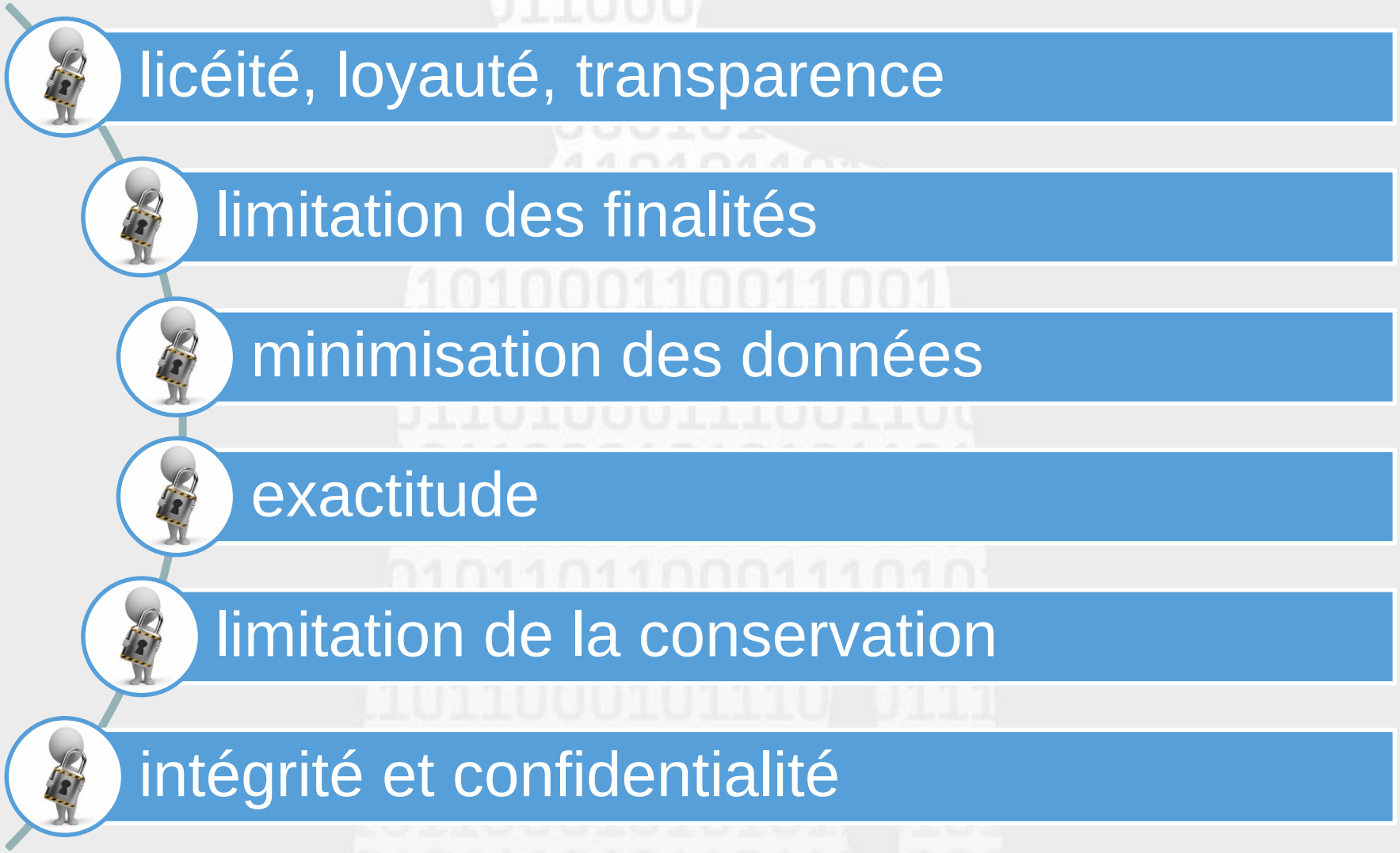
Harmonisation

- Mêmes règles pour les 28 pays membres de l'UE

Directement applicable

- à partir du 25 mai 2018
- à tous les acteurs actifs sur le territoire de l'UE

Principes de protection des données



Droits des personnes

- Droit à l'information
- Droit d'accès
- Droit de rectification
- Droit à l'effacement ("droit à l'oubli") *
- Droit à la limitation du traitement
- Droit à la portabilité *
- Droit d'opposition et prise de décision individuelle automatisée *

Changement de paradigme

Formalités préalables

Contrôle a priori

Principe de la responsabilisation

"Accountability"

Contrôle a posteriori

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

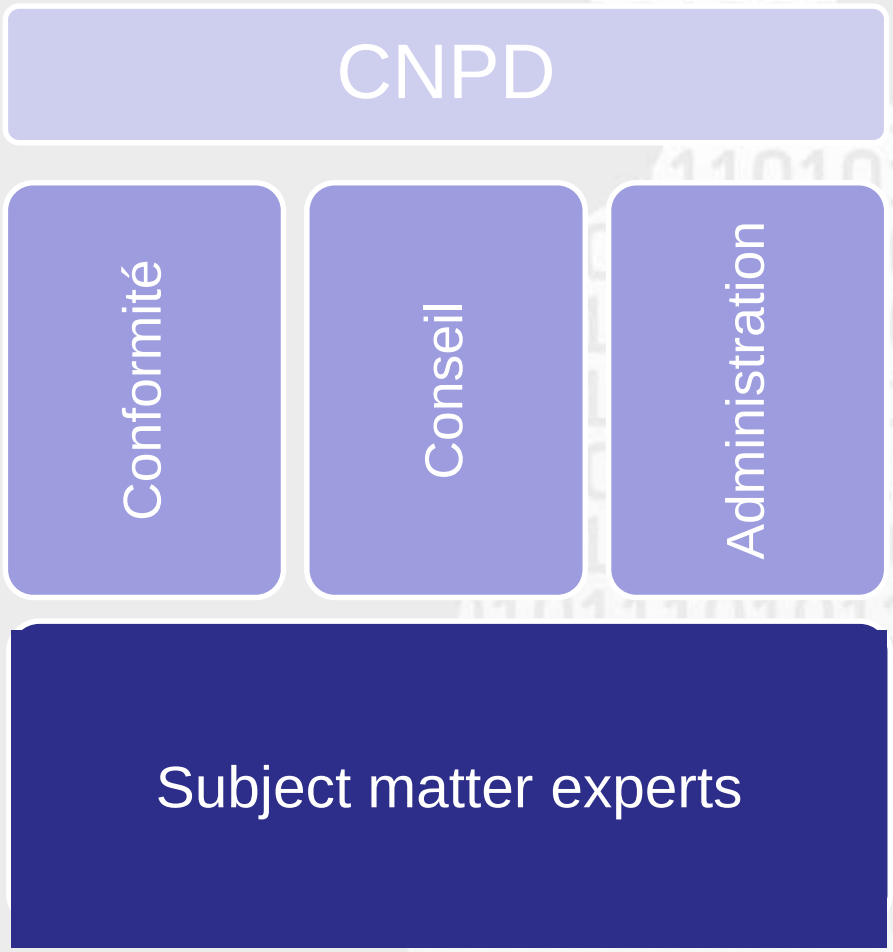
Outils et mécanismes innovateurs

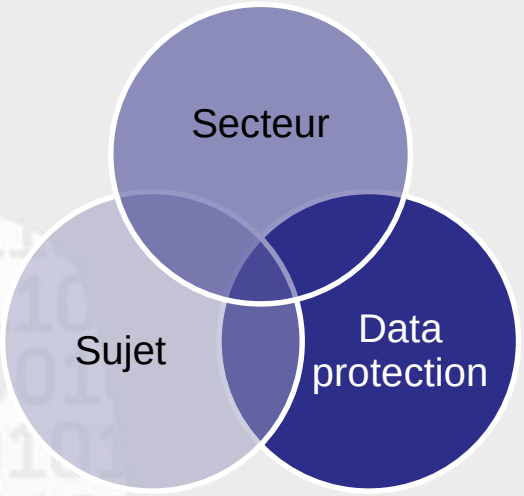
- Analyses d'impact relative à la protection des données (AIPD)
- Codes de conduite et certifications
- « Data protection by design » & « Data protection by default »
- Obligation de notification des violations de données
- Développement du rôle du délégué à la protection des données
- Amendes administratives

Le délégué à la protection des données

- Mission d'avis, de conseil, de contrôle et de point de contact
- Indépendant, ressources nécessaires, accès aux données
- Désignation obligatoire ou facultative
- Possibilité d'un délégué unique

Réorganisation de la CNPD





Collaboration

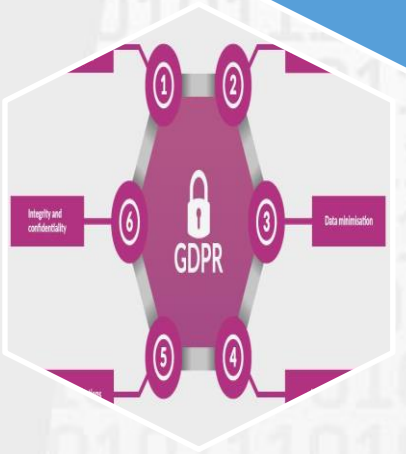
- Notre agenda digital (Case management, procédures internes, nouvel environnement IT pour permettre une adoption des e-Services plus rapide, systèmes collaboration EU,…)
- Nous (continuons) de recruter – juridique et compétences IT

Analyse d'impact sur la protection des données

Objectifs d'un AIPD

Créer des traitement / produit / service qui respecte la vie privée

Évaluer les impacts sur la vie privée des personnes concernées



Démontrer le respect des principes fondamentaux du RGPD

Exemples d'impact sur les individus

Impacts corporels

Préjudice d'agrément, d'esthétique ou économique lié à l'intégrité physique

Perte subie ou gain manqué concernant le patrimoine des personnes.

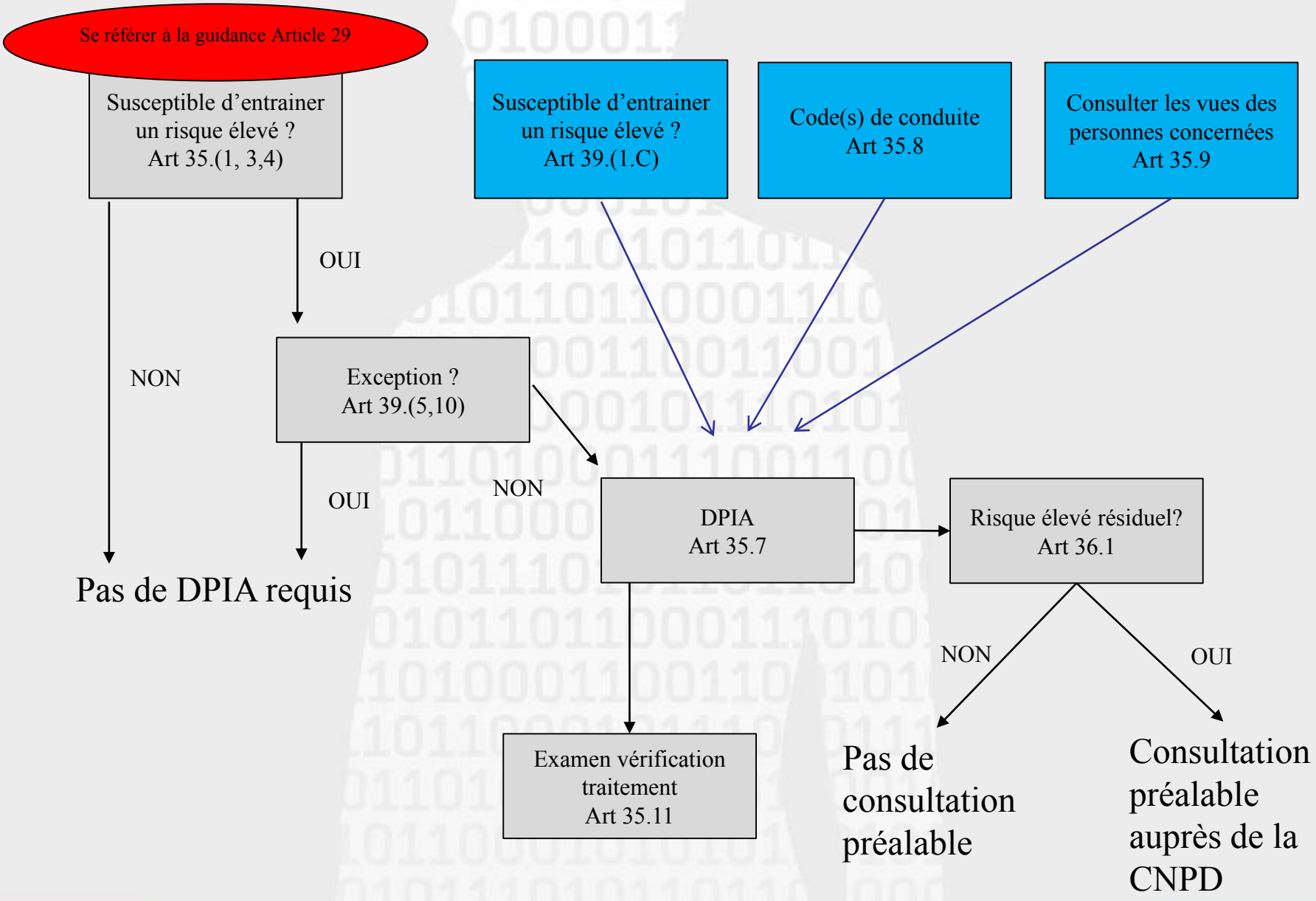
Impacts matériels

Impacts moraux

Souffrance physique ou morale, préjudice esthétique ou d'agrément

(Source: CNIL)

Principes de base



Certifications
Et
Codes de conduite

Définitions

Certification

- Assurance écrite (sous la forme d'un certificat) donnée par une tierce partie qu'un produit, service ou système est conforme à des exigences spécifiques (ISO).

Code de conduite

- Un «engagement pris volontairement par une société ou une organisation d'appliquer certains principes et normes de comportement à la conduite de ses activités ou opérations» (OCDE).

Démontrer le respect des obligations incombant au responsable de traitement

Démontrer le respect des exigences de protection des données dès la conception / par défaut

Certifications / Codes de conduite

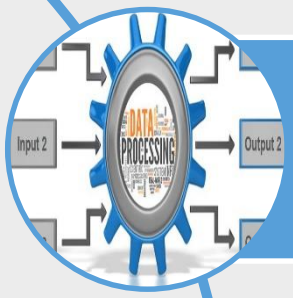
Sous-traitant:

Démontrer l'existence des garanties suffisantes conformément aux exigences du RGPD

Démontrer le respect des exigences prévues en matière de sécurité du traitement

Transfert de données vers des pays tiers

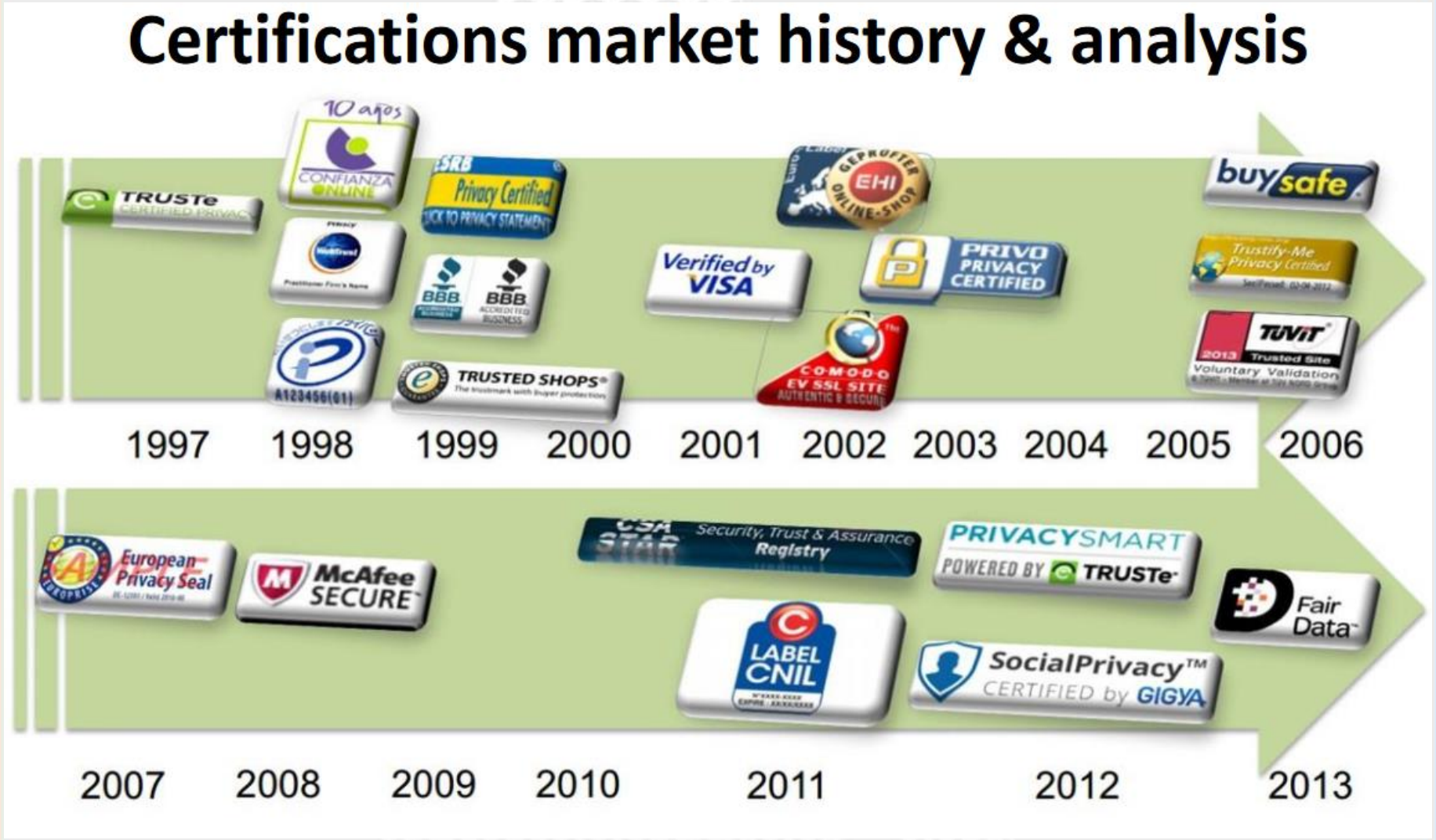
Qu'est-ce qui peut être certifié?



Les opérations de traitements d'un responsable de traitements ou d'un sous-traitant.

Un programme de gouvernance de la protection des données d'un responsable de traitement ou d'un sous-traitant.

Des produits et des services



(Source: CRISP workshop – Madrid – 30 September 2016)

Codes de conduite

Contribuer à la bonne application du RGPD

Spécificité des différents secteurs du traitement

Besoins spécifiques micro, petites, moyennes entreprises

Qui peut certifier?

Les organismes agréés par la CNPD (RGPD + nouvelle loi organique)

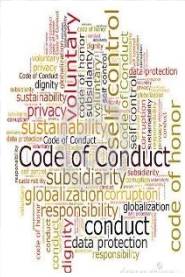
Accréditation	Exigences CNPD
(Exigences ‘standards’) ISO 17065 ISO 17021 ISAE …	Propres à la protection des données

Informations complémentaires

Durée maximale de 3 ans (renouvelable)

Retrait de la certification

Examen périodique par la CNPD

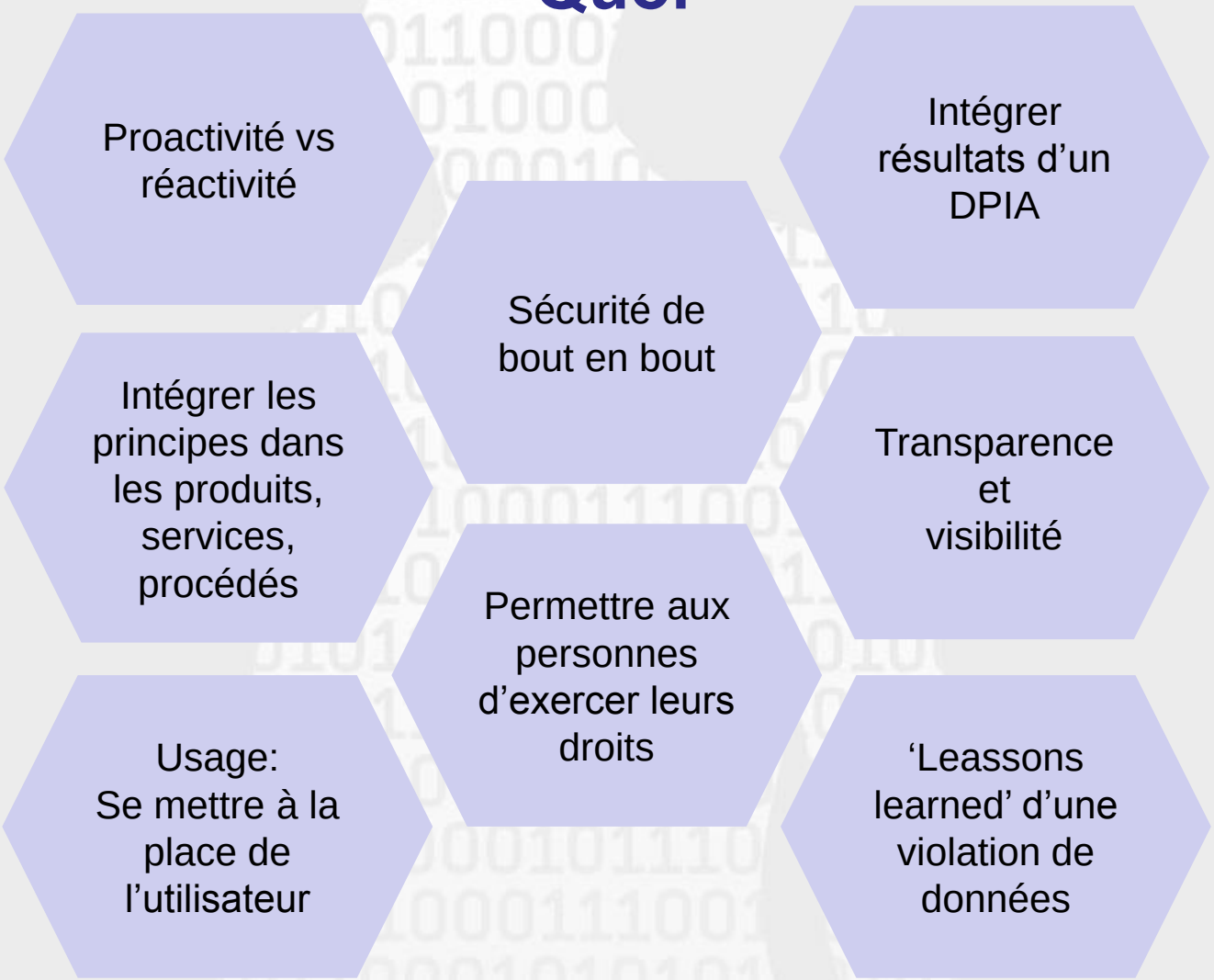


Codes de conduite: avisés, approuvés, enregistrés et publiés par CNPD

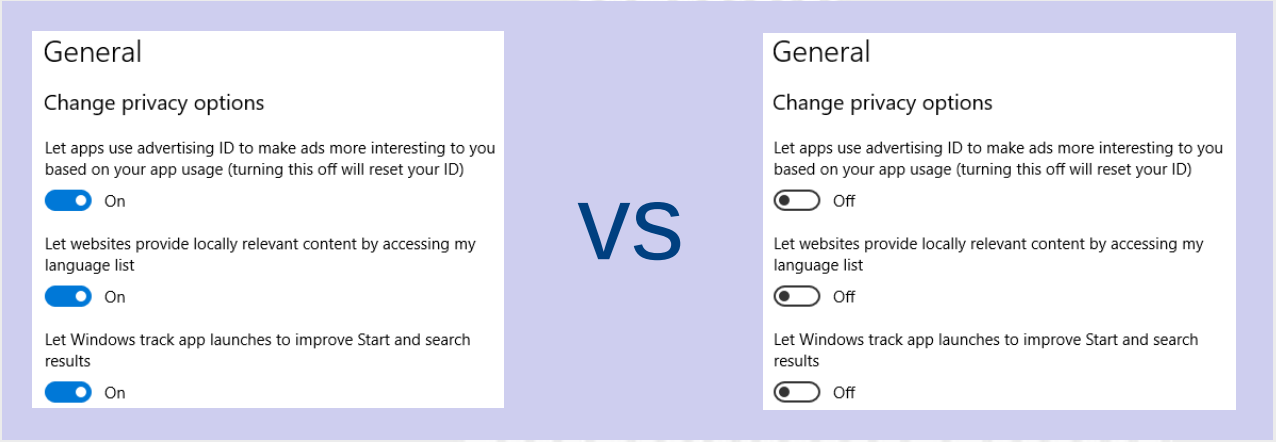
Sanctions: facteur aggravant ou atténuant

Protection des données dès la conception – Protection des données par défaut

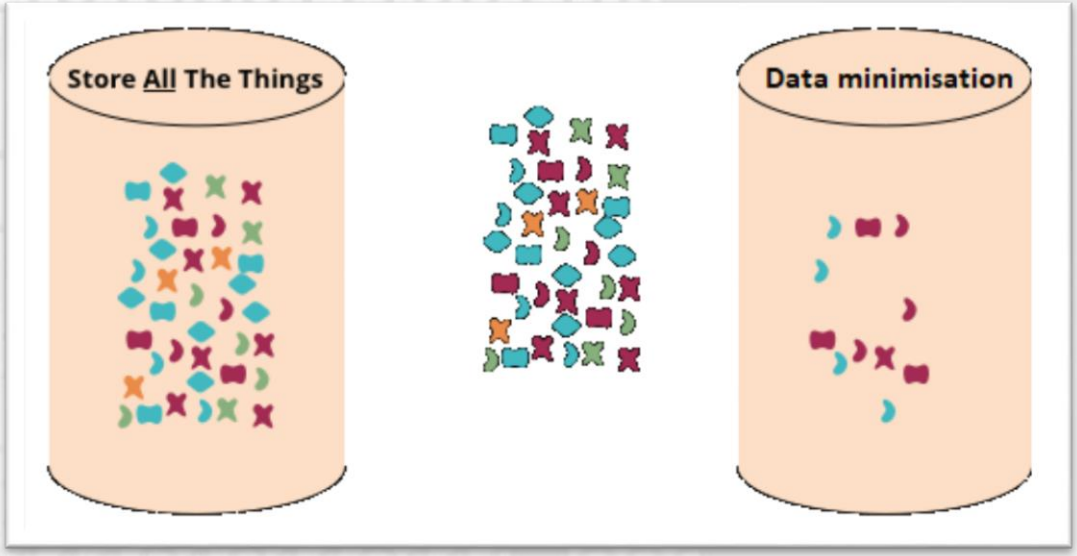
Protection des données dès la conception: Le ‘Quoi’



Protection des données dès la conception



Protection des données par défaut



Violation de données

Principaux éléments à considérer

Sécurité du traitement

Violation de données à caractère personnel

Evaluation / Risque

Registre

Notification

Communication

Violation de données

Principes relatifs au traitement des données à caractère personnel: Les données à caractère personnel doivent être traitées de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité) (Art. 5 (f))

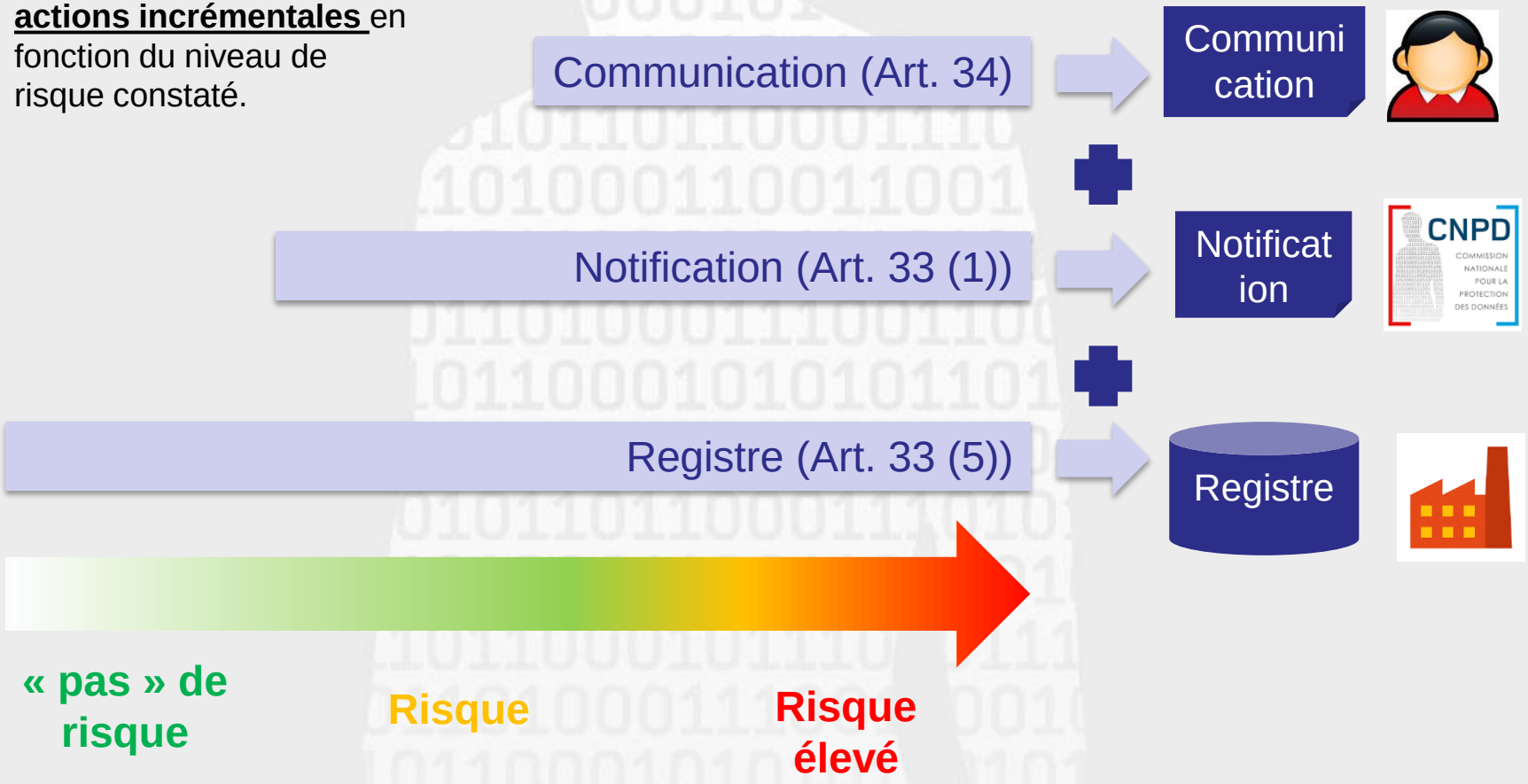
General Data Protection Regulation

- **Mesures de sécurité** obligatoires (éviter ou mitiger l'incident)
- Etre capable de **détecter et gérer** les incidents (mitiger l'impact)

- **Un incident peut toujours arriver – même si toutes les précautions possibles et raisonnables ont été prises**
  - **L'incident ne déclenche pas automatiquement de sanction** – il est tenu compte des mesures techniques et organisationnelles mises en œuvre (Art. 83 (d))
  - **La non-notification d'un incident est un critère aggravant** – il est tenu compte de la manière dont l'autorité de contrôle a eu connaissance de la violation, notamment si, et dans quelle mesure, le responsable de traitement ou le sous-traitant a notifié la violation (Art. 83 (h))

Actions exigées

Le RGPD exige des **actions incrémentales** en fonction du niveau de risque constaté.



La relation responsable de traitement et sous traitant

Le sous-traitant notifie au responsable du traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance. (Art. 33 (2))

General Data Protection Regulation

Sans délai

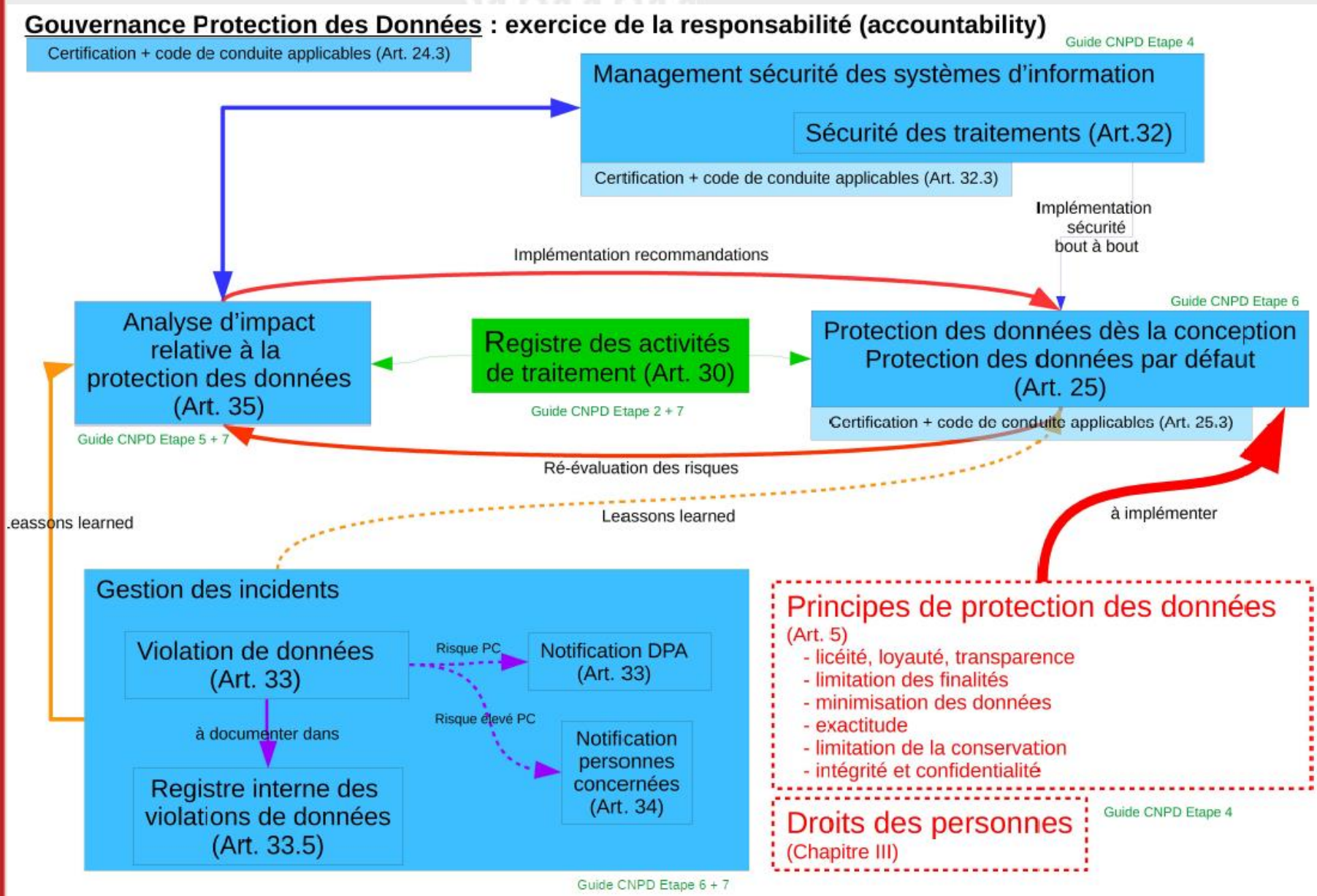
72H

CNPD COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

Sous traitant

Responsable de traitement

Gouvernance protection des données


Gouvernance Protection des Données : exercice de la responsabilité (accountability)
Certification + code de conduite applicables (Art. 24.3)
Guide CNPD Etape 4
Management sécurité des systèmes d'information
Sécurité des traitements (Art.32)
Certification + code de conduite applicables (Art. 32.3)
Implémentation sécurité bout à bout
Implémentation recommandations
Guide CNPD Etape 6
Analyse d'impact relative à la protection des données (Art. 35)
Guide CNPD Etape 5 + 7
Registre des activités de traitement (Art. 30)
Guide CNPD Etape 2 + 7
Protection des données dès la conception
Protection des données par défaut
(Art. 25)
Certification + code de conduite applicables (Art. 25.3)
Ré-évaluation des risques
.eassons learned
Leassons learned
à implémenter
Gestion des incidents
Violation de données (Art. 33)
Risque PC
Notification DPA (Art. 33)
Risque élevé PC
à documenter dans
Notification personnes concernées (Art. 34)
Registre interne des violations de données (Art. 33.5)
Guide CNPD Etape 6 + 7
Principes de protection des données
(Art. 5)
- licéité, loyauté, transparence
- limitation des finalités
- minimisation des données
- exactitude
- limitation de la conservation
- intégrité et confidentialité
Droits des personnes
(Chapitre III)
Guide CNPD Etape 4

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

CNPD
Alain Herrmann
INFORMATIQUE ET NOUVELLES TECHNOLOGIES

Commission nationale pour la protection des données
1, avenue du Rock'n'Roll I L-4361 Esch-sur-Alzette
Tél. : (+352) 26 10 60 51 I Fax : (+352) 26 10 60 29
alain.herrmann@cnpd.lu I www.cnpd.lu
OpenPGP Fingerprint :
34C1 6EC1 A122 8404 9A6E E53C 6924 269B BC71 31AB