Séances d'information

Règlement général sur la protection des données

Les codes de conduite et certifications

18 octobre 2017

Esch-sur-Alzette (Belval)

Alain Herrmann

Service informatique

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

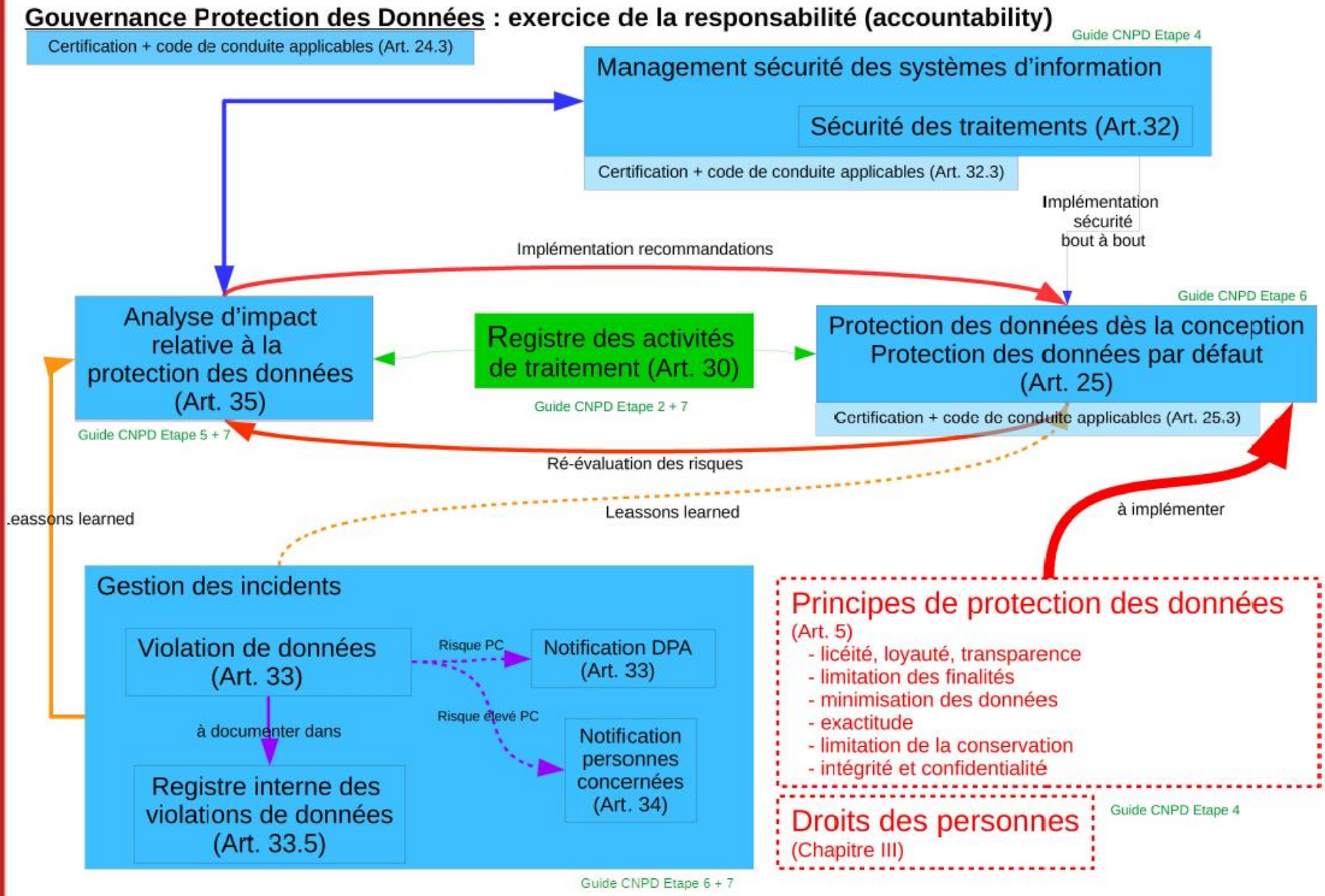
Transfert de données vers des pays tiers

Qu'est-ce qui peut être certifié?

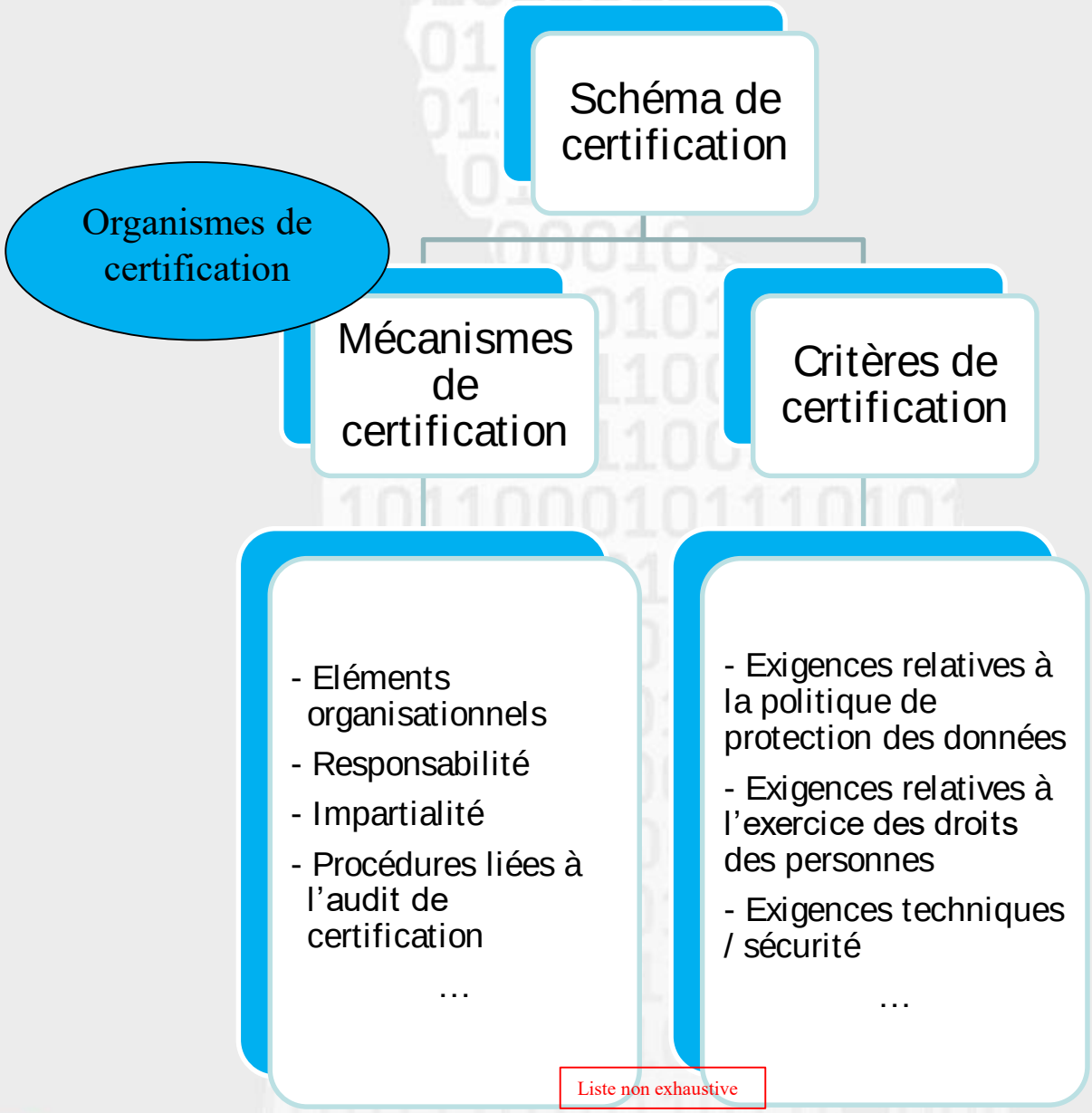
Les opérations de traitements d'un responsable de traitements ou d'un sous-traitant.

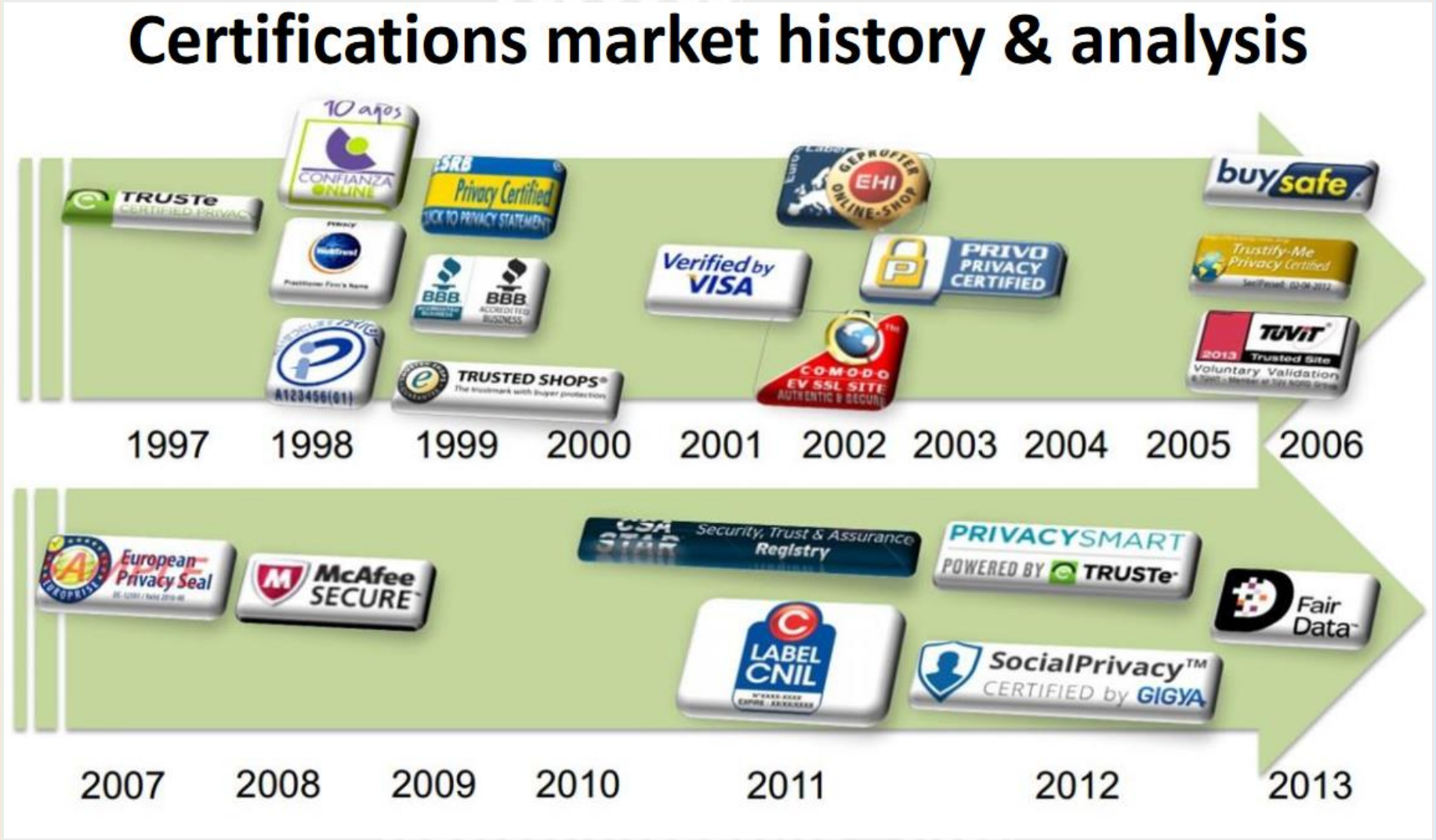
Un programme de gouvernance de la protection des données d'un responsable de traitement ou d'un sous-traitant.

Des produits et des services


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

Les schémas de certifications





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

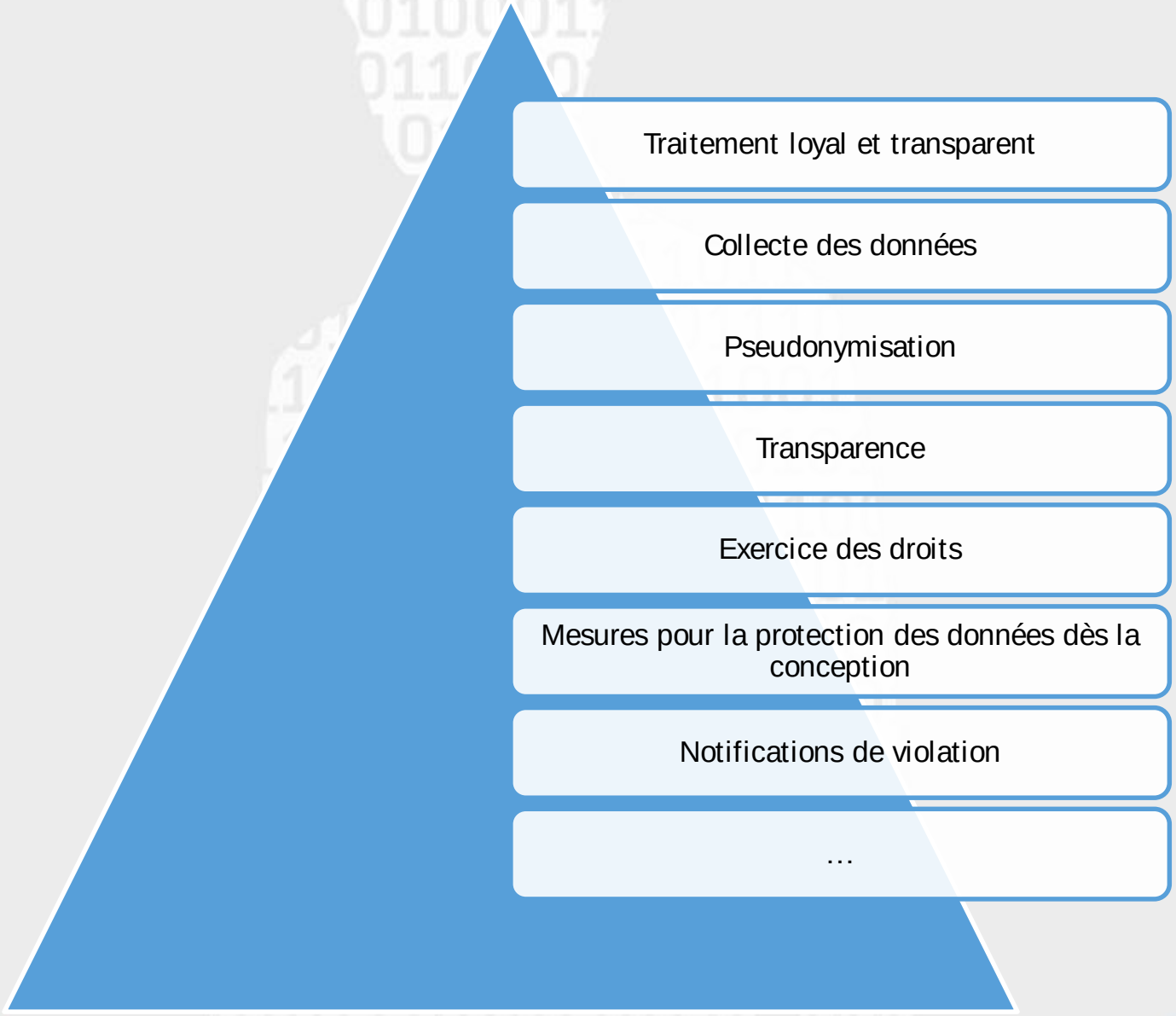
Codes de conduite

Contribuer à la bonne application du RGPD

Spécificité des différents secteurs du traitement

Besoins spécifiques micro, petites, moyennes entreprises

Contenu d'un code de conduite (liste non exhaustive)



Qui peut certifier?

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

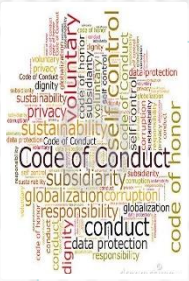
Accréditation	Exigences CNPD
(Exigences 'standards') ISO 17065 ISO 17021 ISAE …	Propres à la protection des données

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

N’attendez pas les certifications pour vous mettre en conformité!

Commission nationale pour la protection des données

Merci pour votre attention!