Séances d'information

Règlement général sur la protection des données

Les analyses d'impact sur la protection des données (AIPD)

18 octobre 2017

Esch-sur-Alzette (Belval)

Alain Herrmann

Service informatique

Agenda

Objectifs

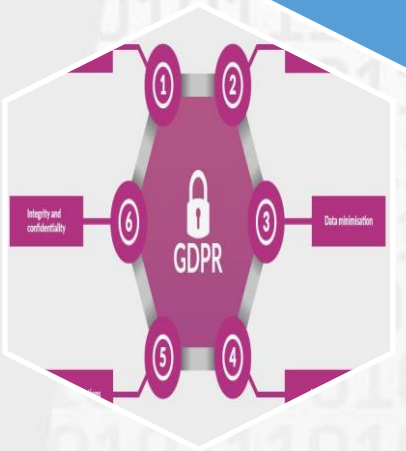
Principes de bases et critères

Les étapes d'un AIPD

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

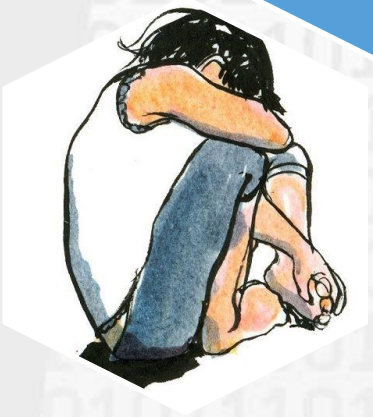
Exemples d'impact sur les individus

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

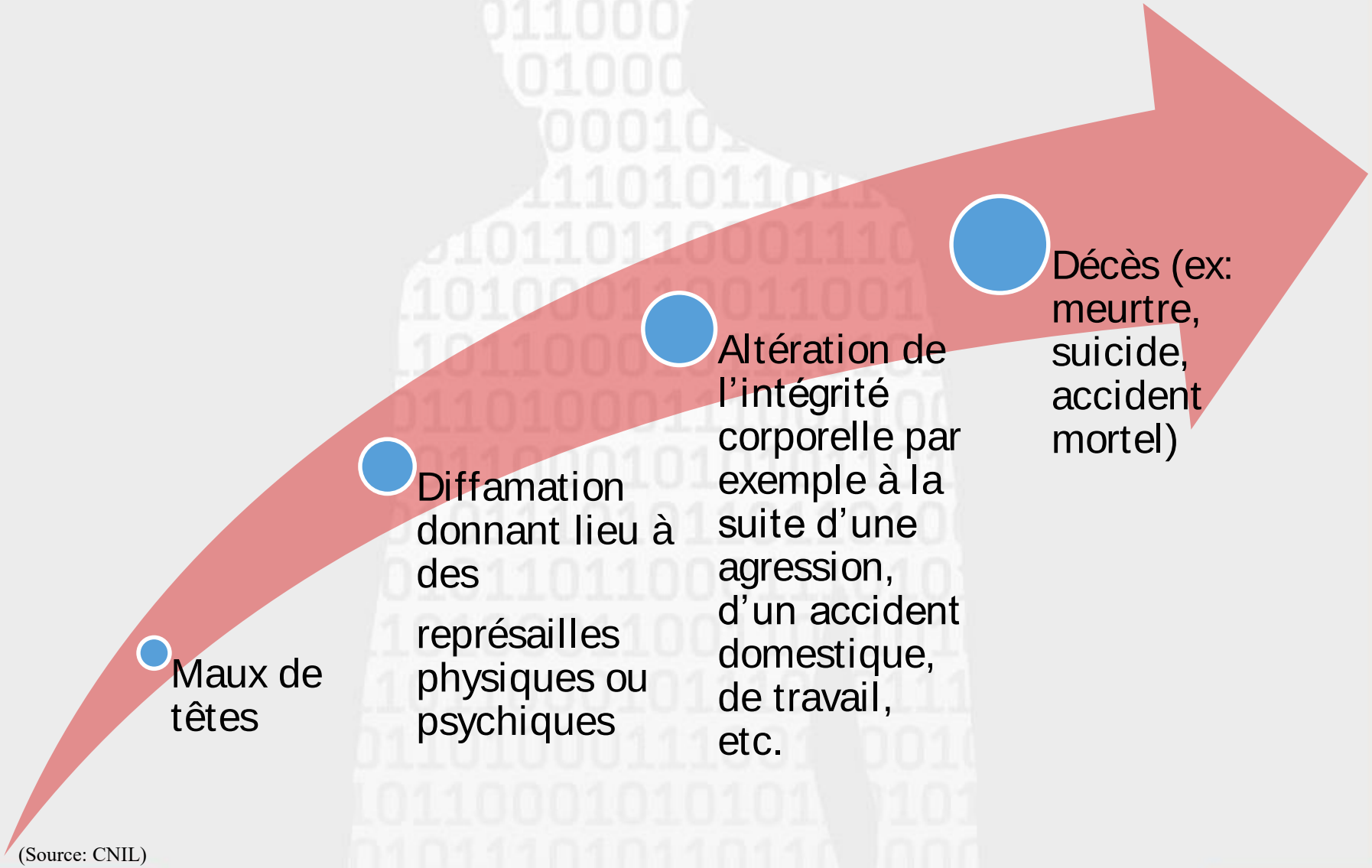


Impacts moraux

Souffrance physique ou morale, préjudice esthétique ou d'agrément

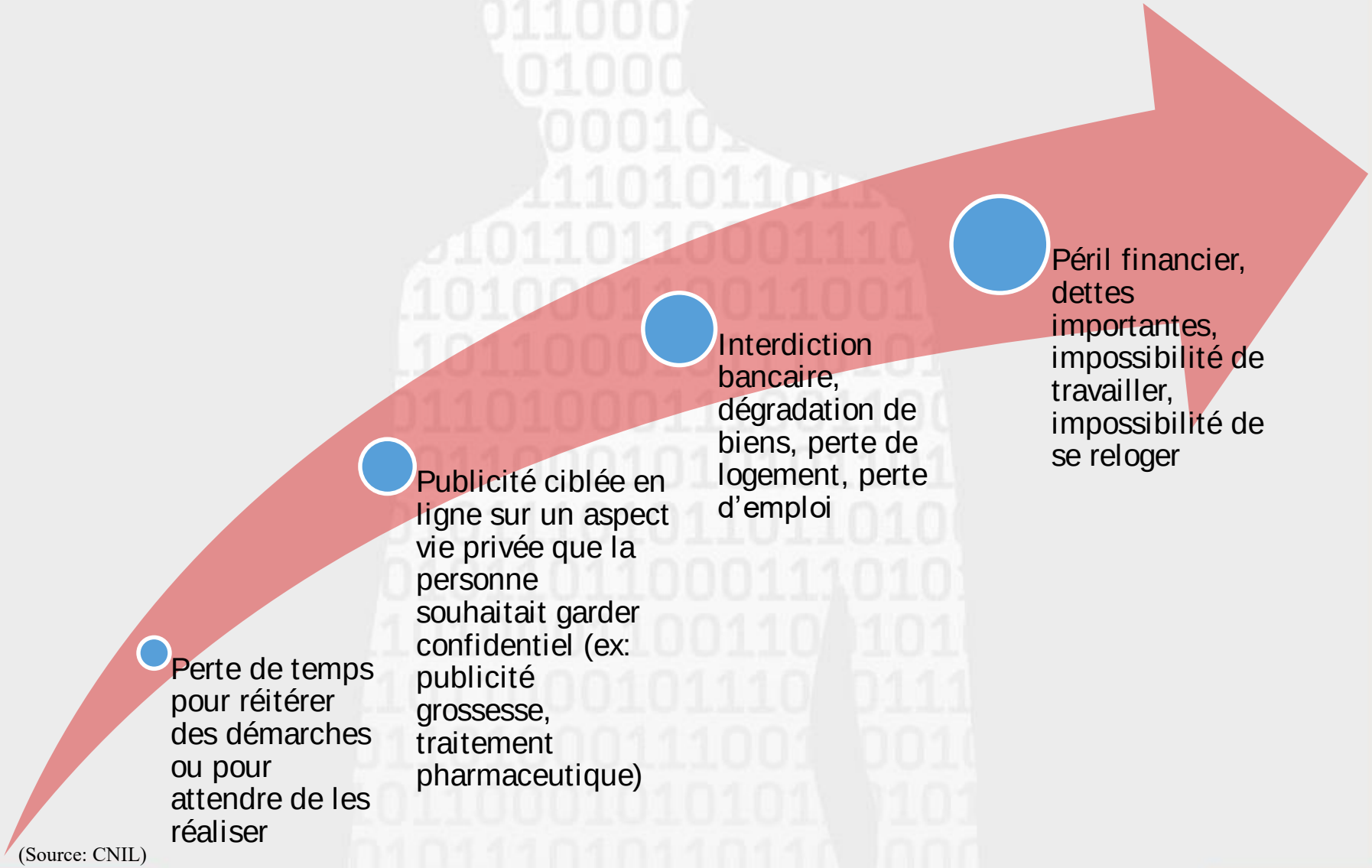
(Source: CNIL)

Exemples d'impacts corporels



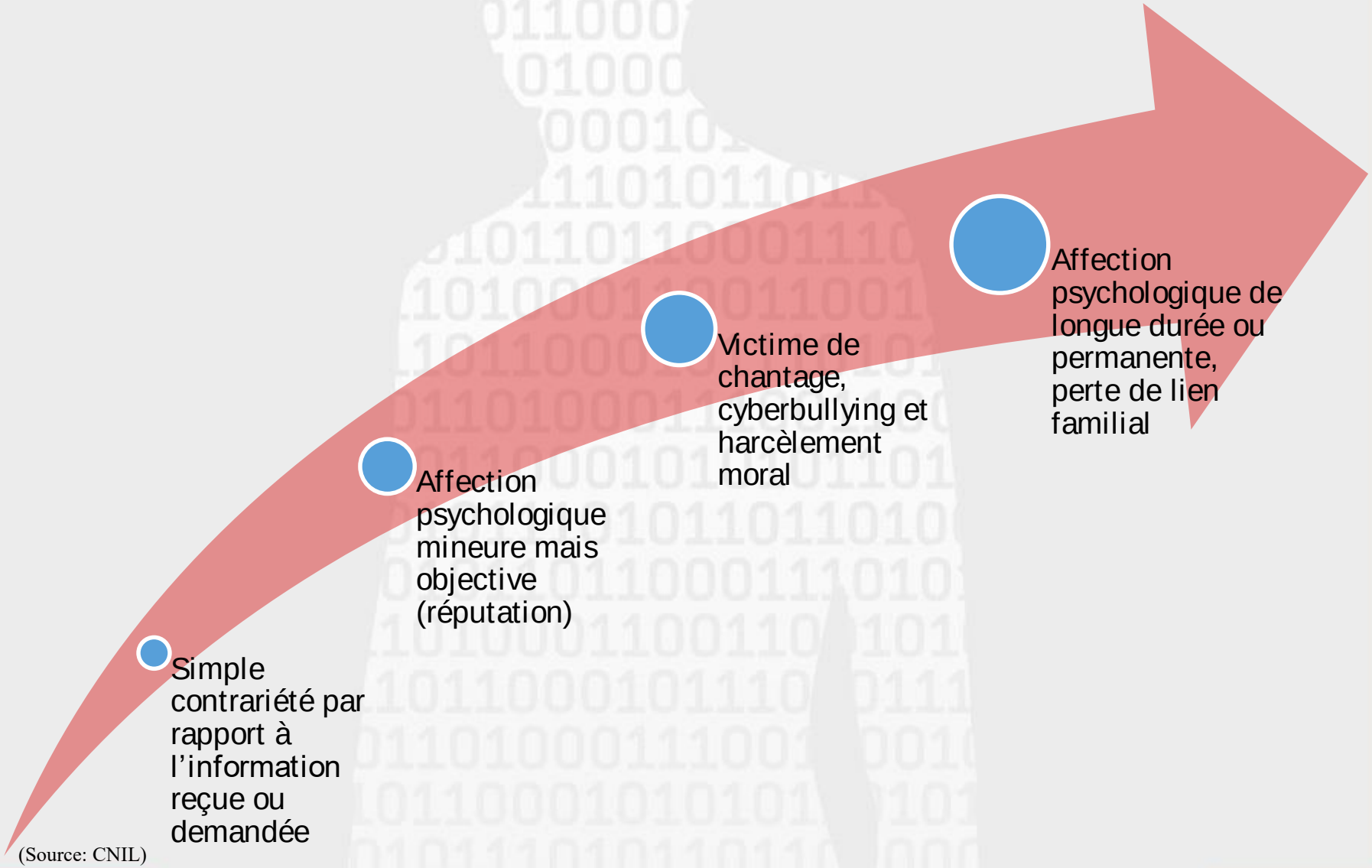
(Source: CNIL)

Exemples d'impacts matériels



(Source: CNIL)

Exemples d'impacts moraux



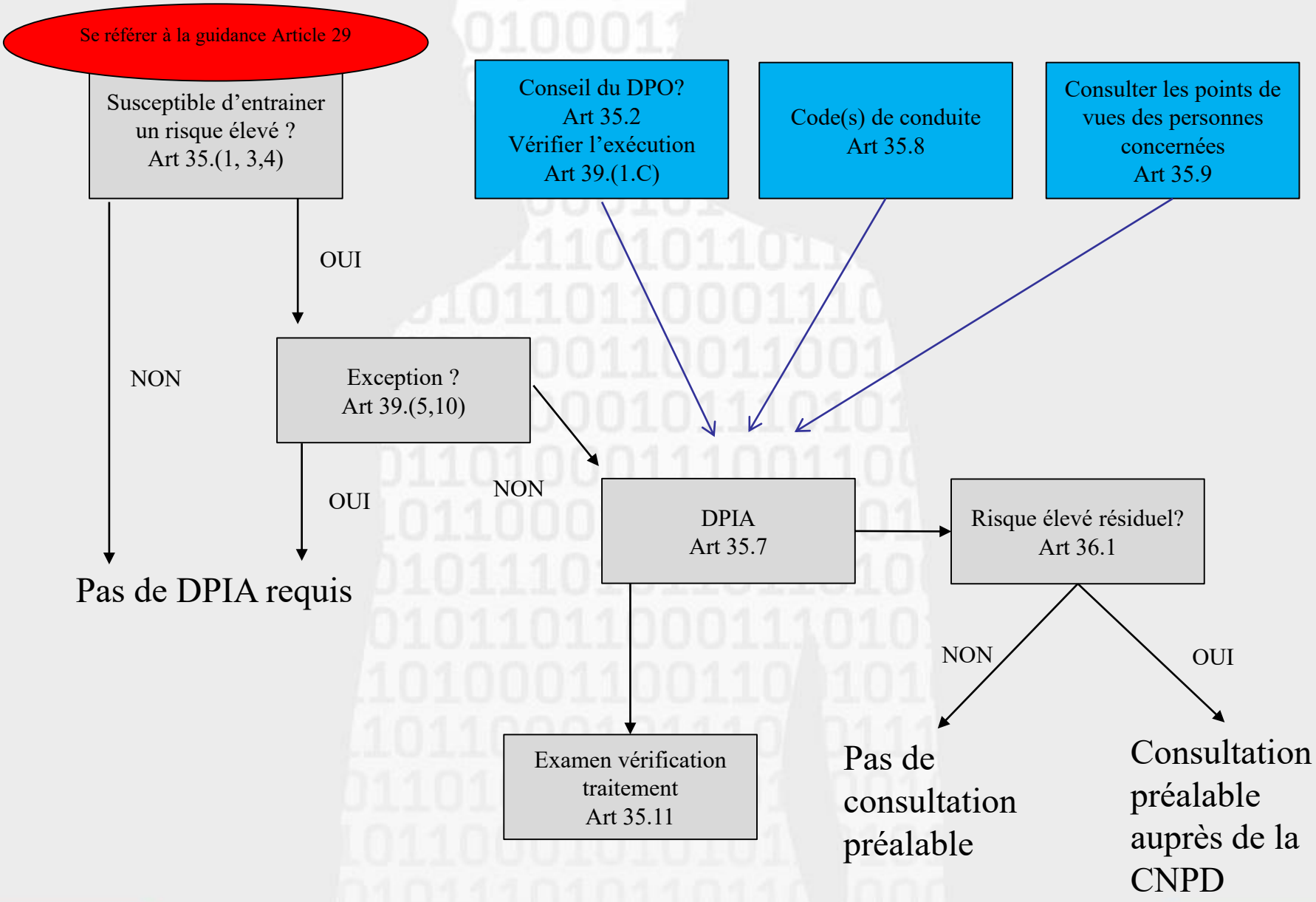
(Source: CNIL)

Qu'est ce qu'un DPIA évalue?

Un seul traitement ou un ensemble de traitements similaires

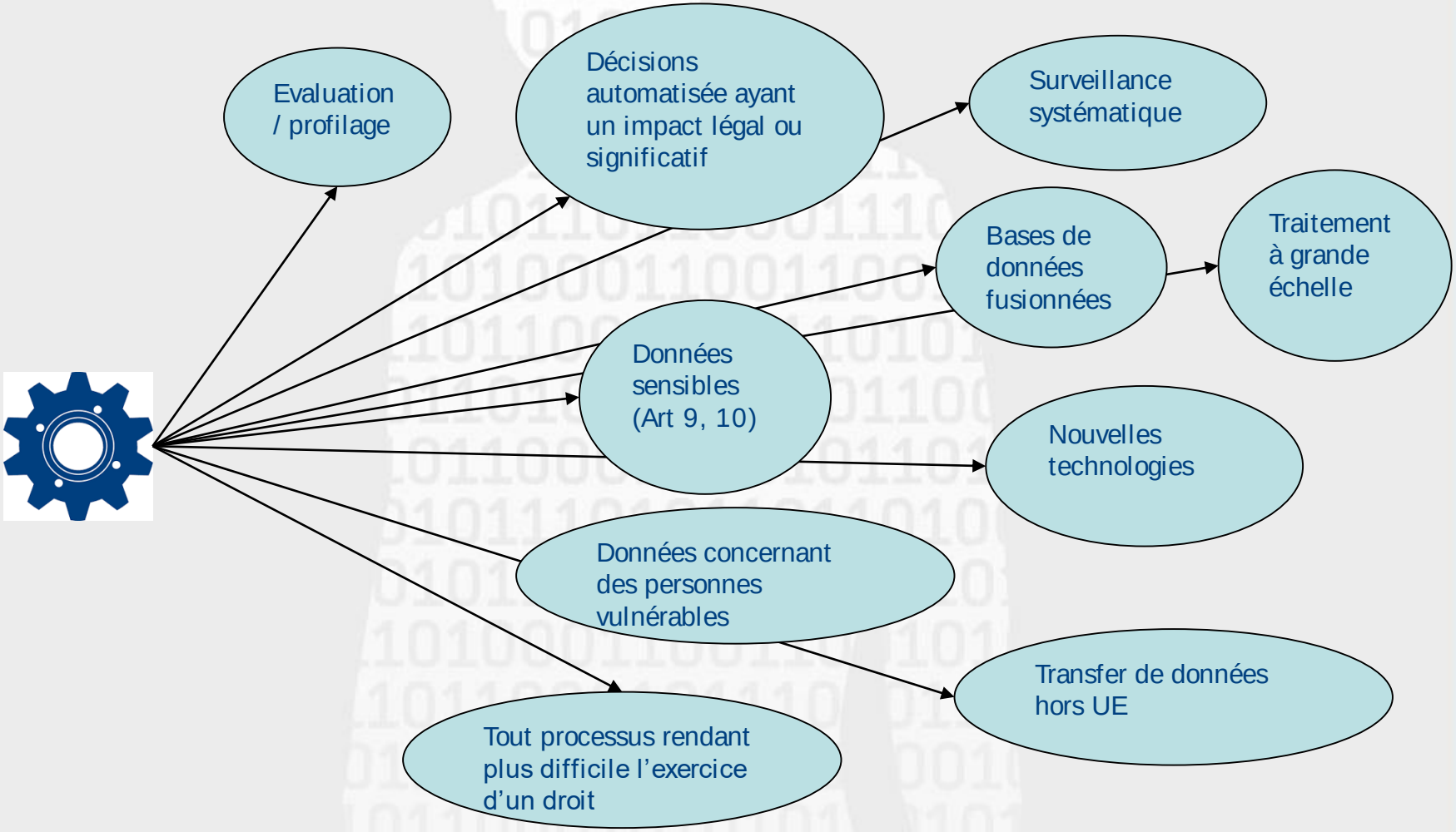
- Une « *seule et même analyse peut porter sur un ensemble d'opérations de traitement similaires qui présentent des risques élevés similaires* »
- Il «*existe des cas dans lesquels il peut être raisonnable et économique d'élargir la portée de l'analyse d'impact relative à la protection des données au-delà d'un projet unique* »

Principes de base



Critères pour mener un DPIA

Un seul traitement ou un ensemble de traitements similaires



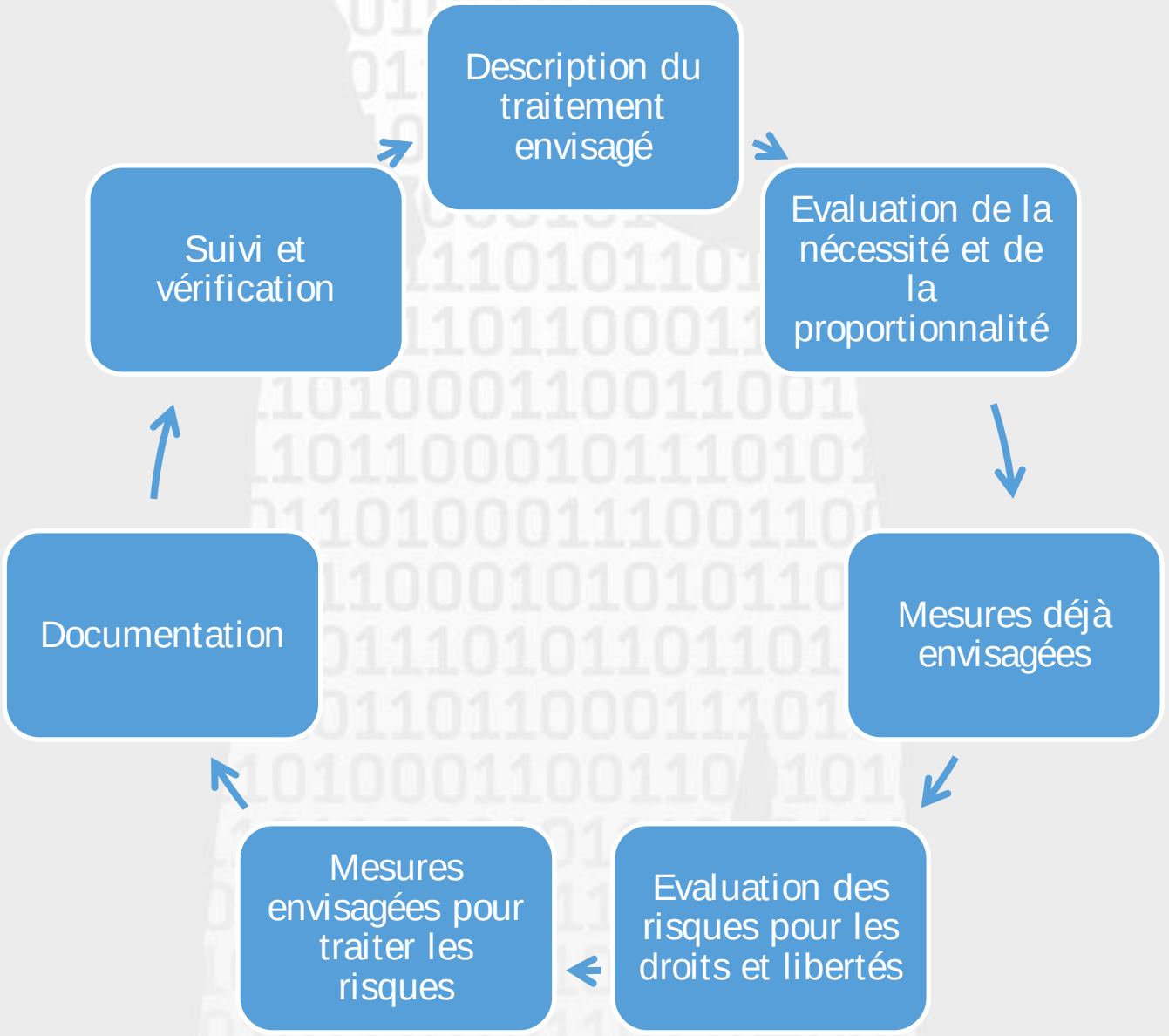
Exemples

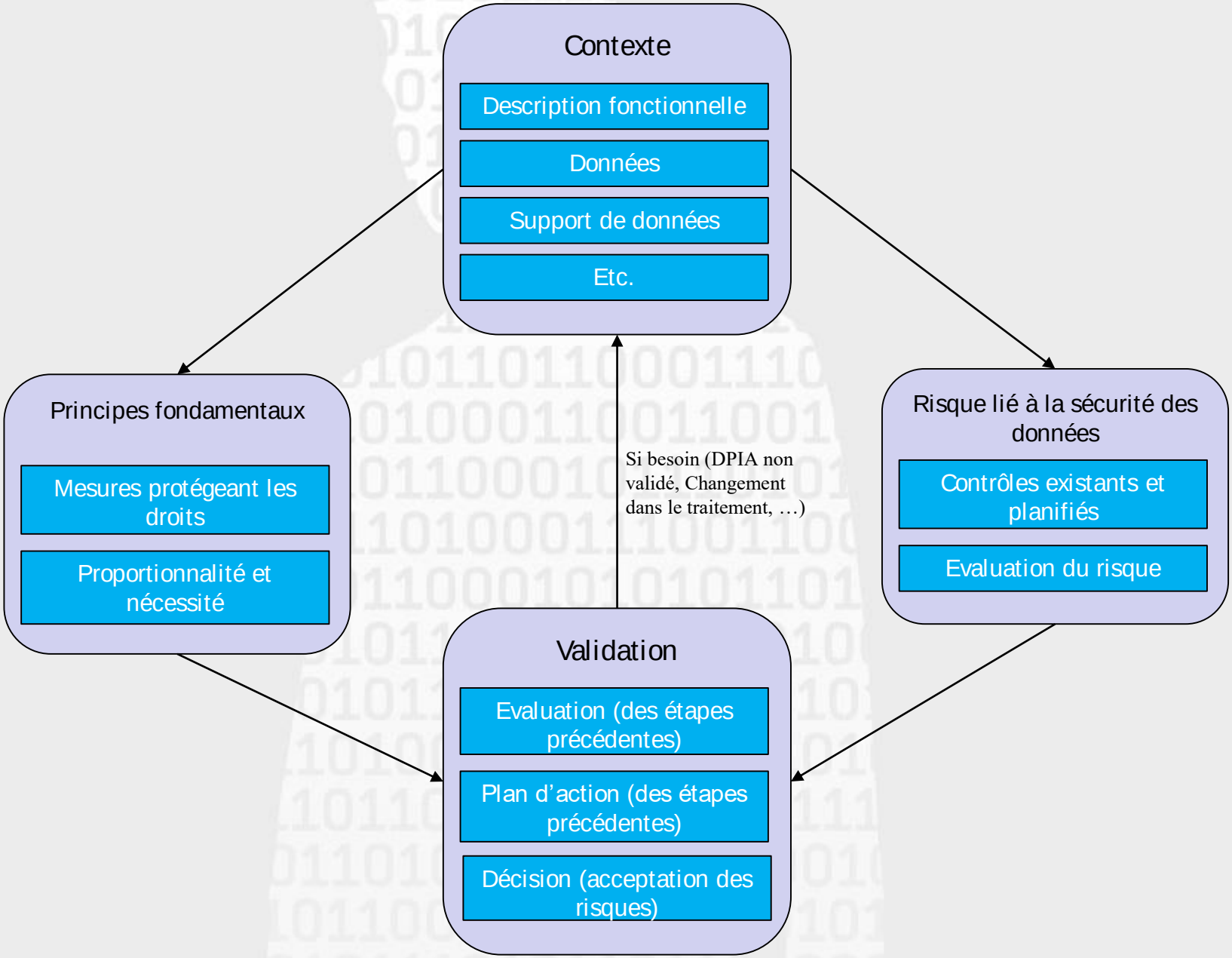
Exemples de traitement	Critères possible	DPIA nécessaire ?
Un hôpital traite les données génétiques et de santé de ses patients	- Données sensibles - Données concernant des personnes vulnérables	OUI
Utilisation d'un système de surveillance vidéo pour surveiller le comportement des automobilistes sur l'autoroute. Le RT envisage l'utilisation d'analyse intelligente pour lire les plaques d'immatriculation	- Surveillance systématique - Nouvelles technologies	
Une entreprise surveille l'activité de ses employés incluant leur poste de travail, internet, etc …	- Surveillance systématique - Personnes vulnérables	
La récolte par des entreprises privées de données concernant les publications de personnes dans des médias sociaux dans le but d'en faire un annuaire de contact	- Evaluation / Profilage - Traitement à grande échelle	
Site internet utilisant la mailing list de ses abonnés pour envoyer une newsletter	Aucun	NON
Un site de commerce en ligne affichant des publicités ciblées basé sur les habitudes de consommation des visiteurs	Evaluation / Profilage mais pas systématique ni extensif	

Quand une AIPD n'est-elle pas nécessaire ?

- Le risque (pour les personnes concernées) n'est pas élevé
- Une AIPD similaire existe: appliquer ses mesures
- Le droit règlemente l'opération et l'AIPD y est incluse
- Le traitement fait partie de la liste des traitements exempts de la nécessité d'établir un DPIA, émise par la CNPD

Les étapes d'un DPIA




Contexte
Description fonctionnelle
Données
Support de données
Etc.
Principes fondamentaux
Mesures protégeant les droits
Proportionnalité et nécessité
Si besoin (DPIA non validé, Changement dans le traitement, …)
Risque lié à la sécurité des données
Contrôles existants et planifiés
Evaluation du risque
Validation
Evaluation (des étapes précédentes)
Plan d'action (des étapes précédentes)
Décision (acceptation des risques)

Publication et consultation

Consultation préalable à la CNPD

Requise en cas de risque élevé résiduel

Transparence: un résumé de l'AIPD peut être rendu disponible au public

L'AIPD peut être demandé lors d'un contrôle

Les acteurs du DPIA

Le responsable de traitement

Data Protection Officer

Chief Information Security Officer

Les experts 'métier'

Les experts sectoriels: juridique, éthique, économique

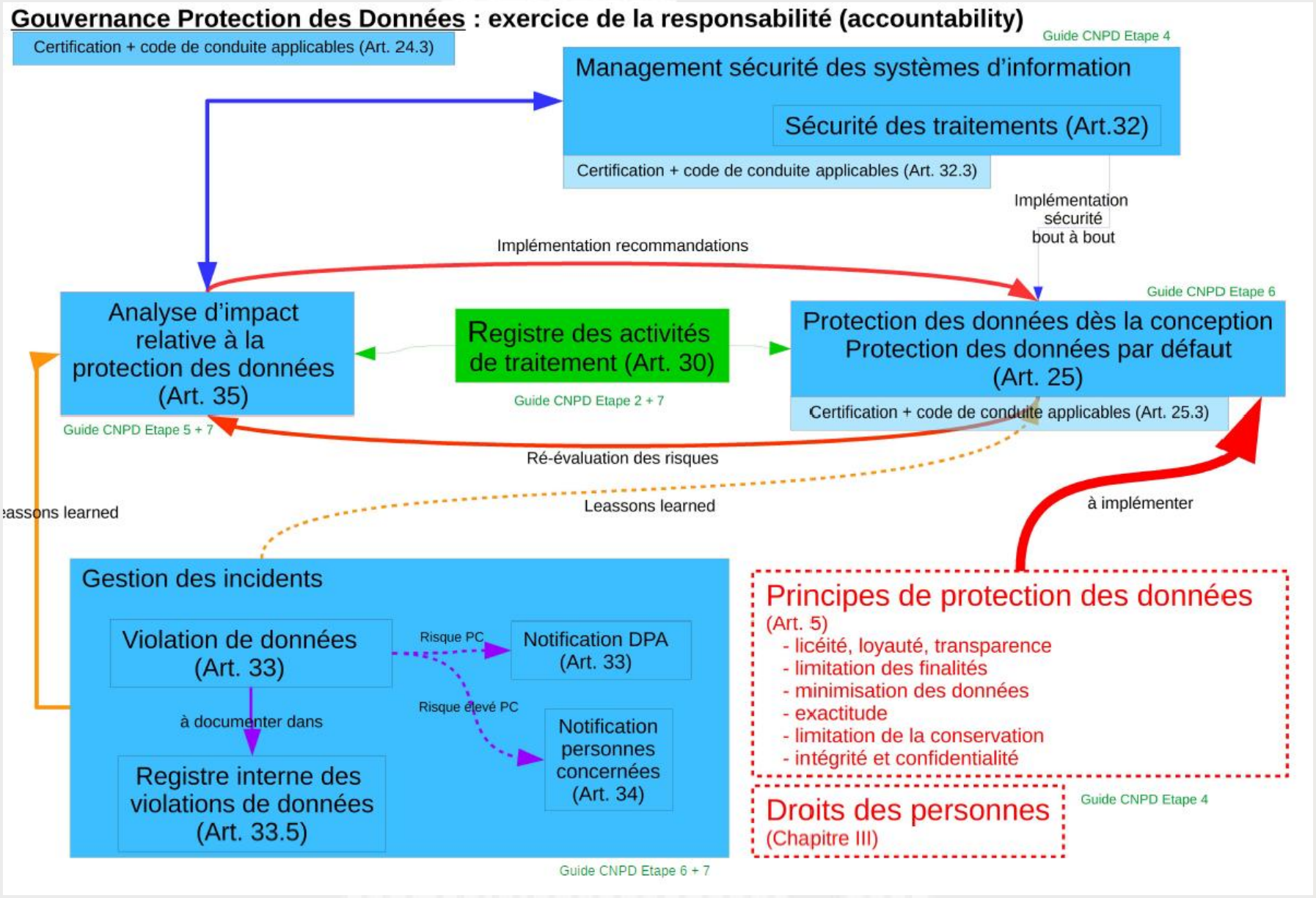
Définir et documenter les rôles et responsabilités des acteurs impliqués dans la réalisation du DPIA.

Informations complémentaires

AIPD et codes de conduite

Les outils pour vous aider

Guidances du groupe de l'article 29


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)
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)
Guide CNPD Etape 5 + 7
Ré-évaluation des risques
Leassons 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

Merci pour votre attention!