

Bientôt l'entrée en vigueur du RGPD: Entrepreneurs, préparez-vous à temps

*7 étapes pour se préparer à l'entrée
en vigueur du RGPD*



Luxembourg
25 novembre 2017



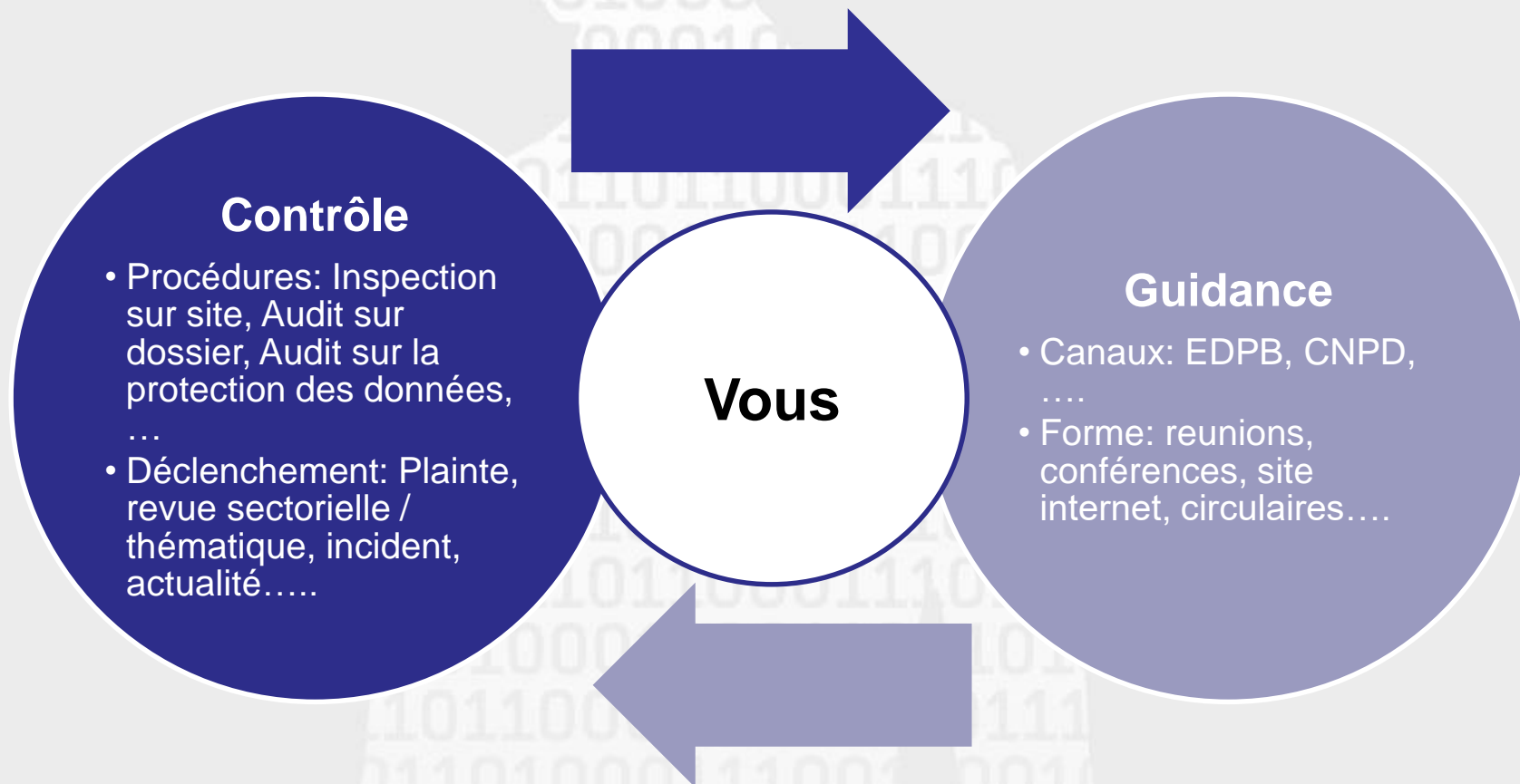
Christophe Buschmann (Commissaire)
Mathilde Stenersen (Service juridique)

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



La bonne balance





Chiffres clés 2016

+130%



30 avis sur les projets législatifs et réglementaires



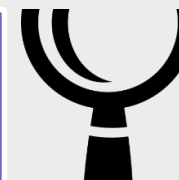
185 plaintes

+30%

1'449 demandes d'autorisation



77 investigations



+39%



1'003 notifications reçues



430 demandes de renseignement par écrit

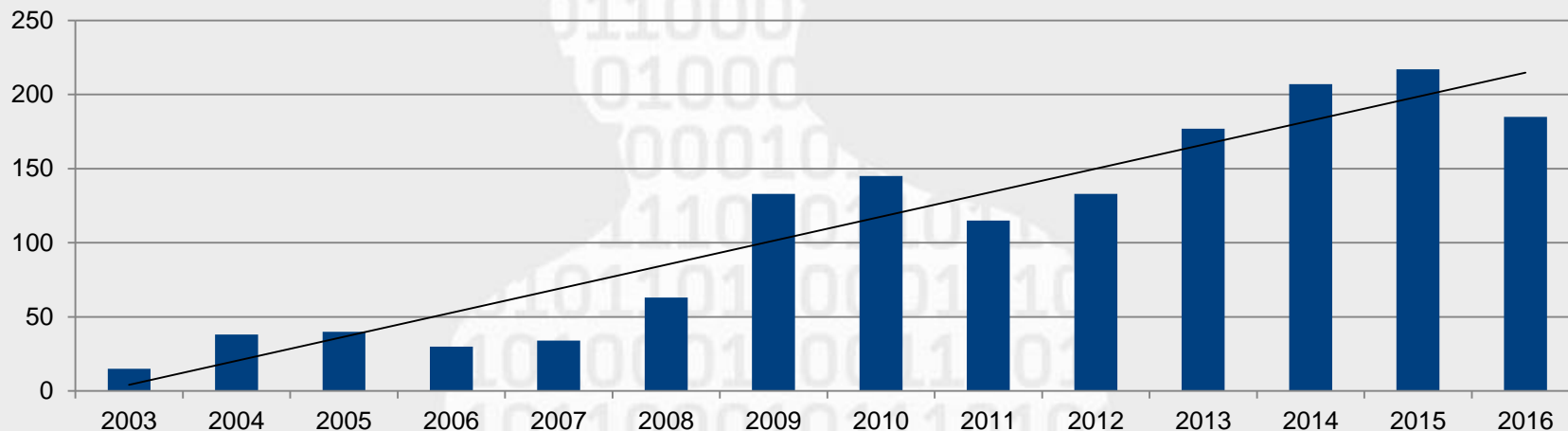
+27%

198 réunions avec les acteurs privés et publics

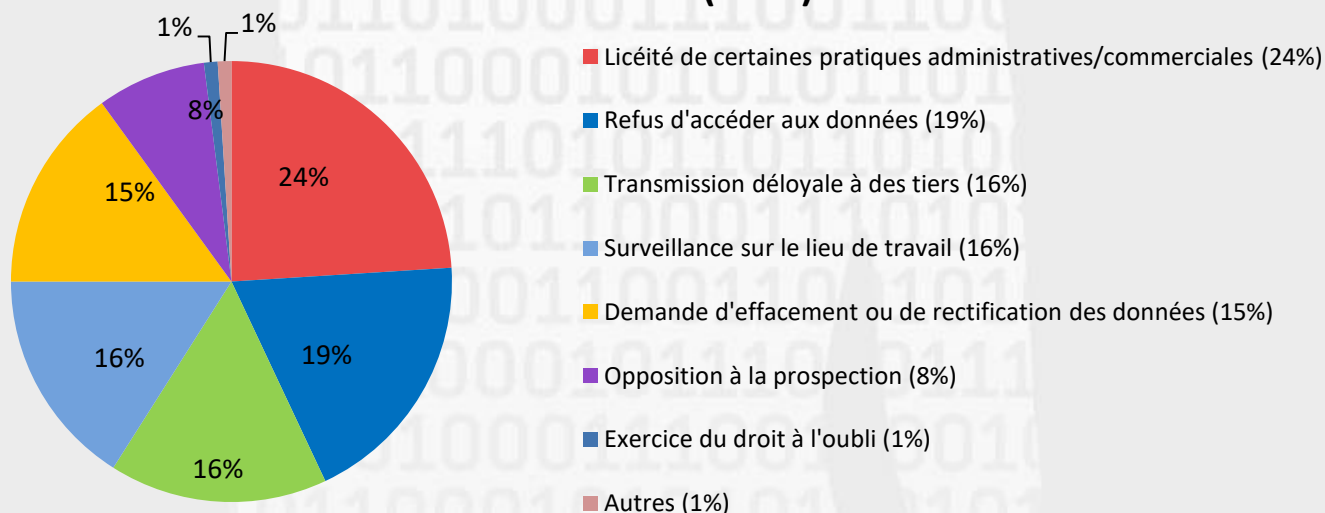




Evolution du nombre des plaintes



Motifs (2016)



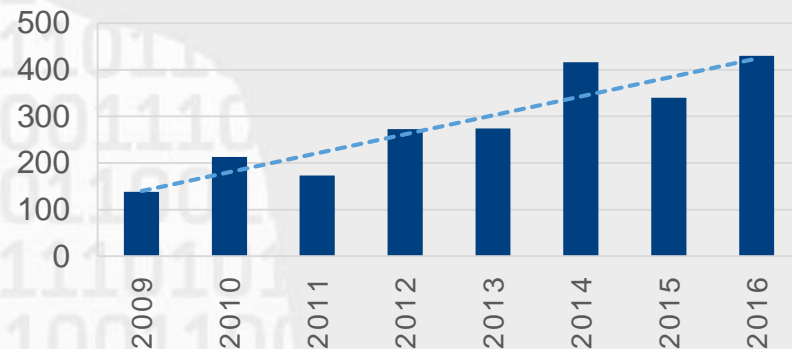


Une année chargée pour la CNPD

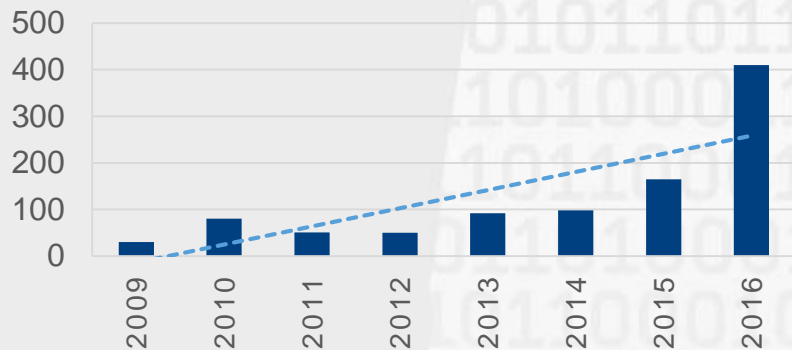
AVIS



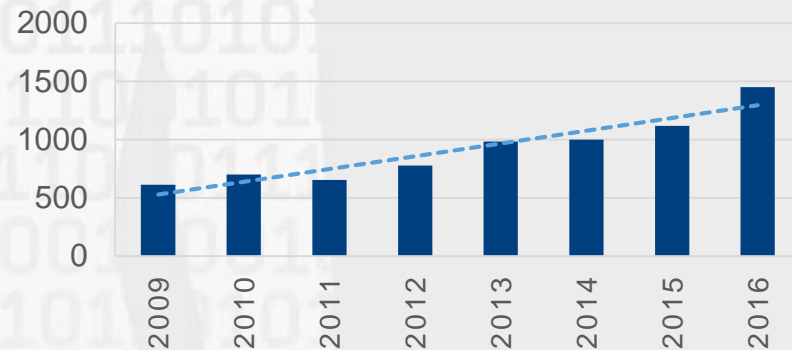
DEMANDES DE RENSEIGNEMENT



TRANSFERTS VERS DES PAYS TIERS



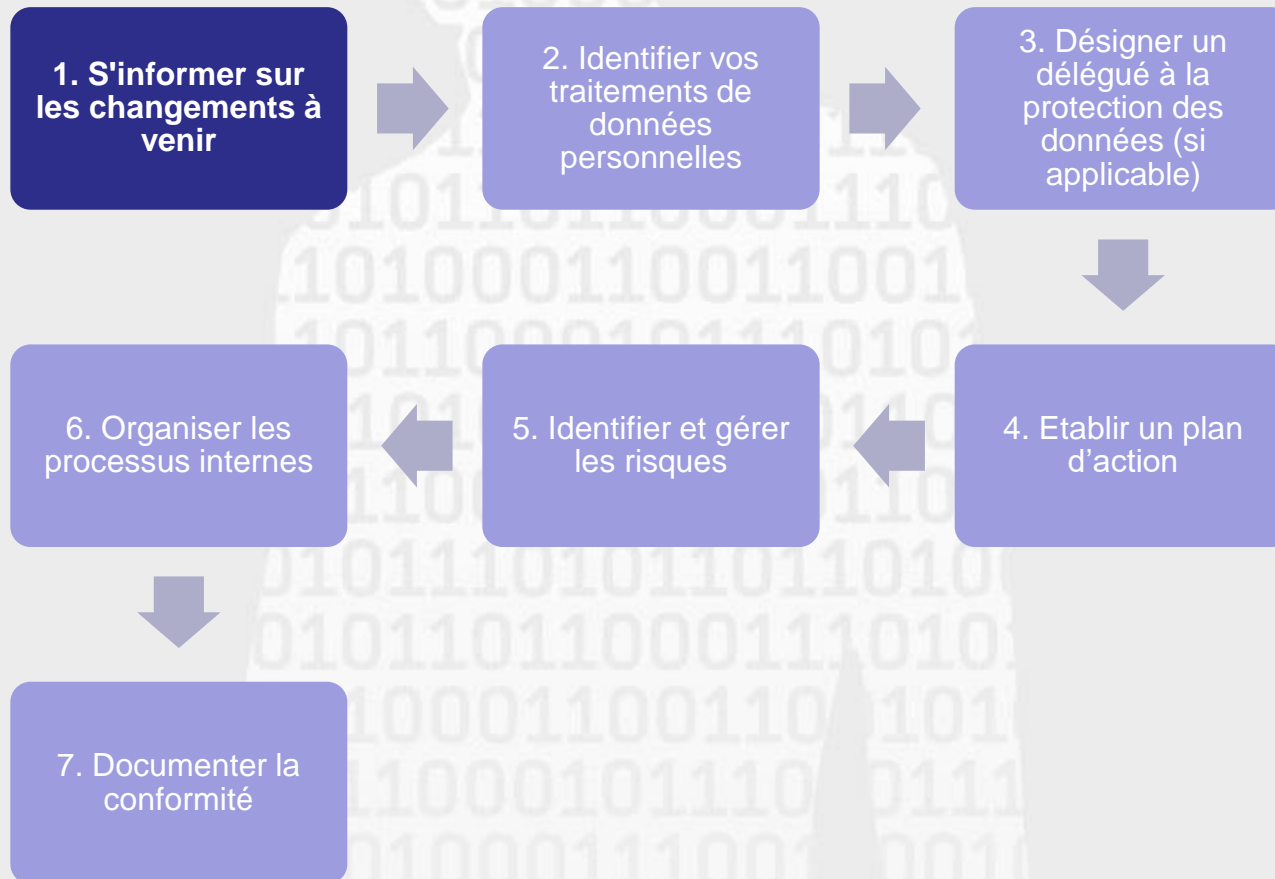
DEMANDES D'AUTORISATION





Les 7 étapes pour préparer sa conformité au RGPD

Les 7 étapes pour préparer sa conformité



Etape 1/7 : S'informer sur les changements à venir

4.5.2016

FR

Journal officiel de l'Union européenne

L 119/1

I

(Actes législatifs)

RÈGLEMENTS

RGPD – LES CHANGEMENTS CLÉS

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)

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

Etape 1/7 : S'informer sur les changements à venir

Renforcement des droits des personnes:

- Définition restreinte du **consentement** (+ consentement du responsable parental pour les mineurs de < 16 ans);
- Droit à la **portabilité** des données;
- Droit à **l'oubli** (*Right to be forgotten*);
- Le droit d'être informé en cas de **violation de données**;
- Introduction du principe des **actions collectives**;

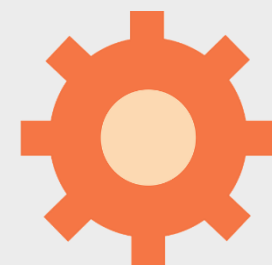
- Autres droits déjà existants ont été renforcés:
 - Droit à **l'information**;
 - Droit **d'opposition**.



Etape 1/7 : S'informer sur les changements à venir

Responsable du traitement & sous-traitant:

- **Accountability:** le RGPD repose sur une logique de conformité dont les acteurs (RT & ST) sont responsables (les formalités préalables, comme les notifications et autorisations, vont être fortement réduites);
- **Responsabilité des sous-traitants étendue:** nouvelles obligations en matière de sécurité, de confidentialité, d'*accountability*, de conseil auprès du RT pour la conformité à certaines obligations et de conditions de recrutement d'un ST secondaire.



Etape 1/7 : S'informer sur les changements à venir

Les concepts clé

Délégué à la protection des données (Data Protection Officer)

Notification de faille de sécurité à l'autorité de contrôle

L'analyse d'impact (Data Protection Impact Assessment)

Codes de conduite, Certification

Le registre des traitements

Privacy by design
↔ Privacy by default

Mesures de sécurités renforcés

Etape 1/7 : S'informer sur les changements à venir

Champ d'application territorial plus large:

- soit un RT ou un ST sont établis sur le territoire de l'UE, soit un RT ou un ST fournissent des biens et/ou des services aux résidents européens ou essaient de cibler les résidents européens;



Etape 1/7 : S'informer sur les changements à venir

Le « one stop shop » et une coopération européenne renforcée:

- Un point de contact pour les entreprises → soit l'autorité du lieu de leur siège central dans l'UE, soit l'établissement au sein duquel seront prises les décisions relatives aux finalités et aux modalités du traitement. Cet autorité sera désignée comme **autorité « chef de file »**;
- Coopération renforcée entre les autorités européennes pour que les entreprises reçoivent une **décision unique** partagée par toutes les autorités concernées.



Etape 1/7 : S'informer sur les changements à venir

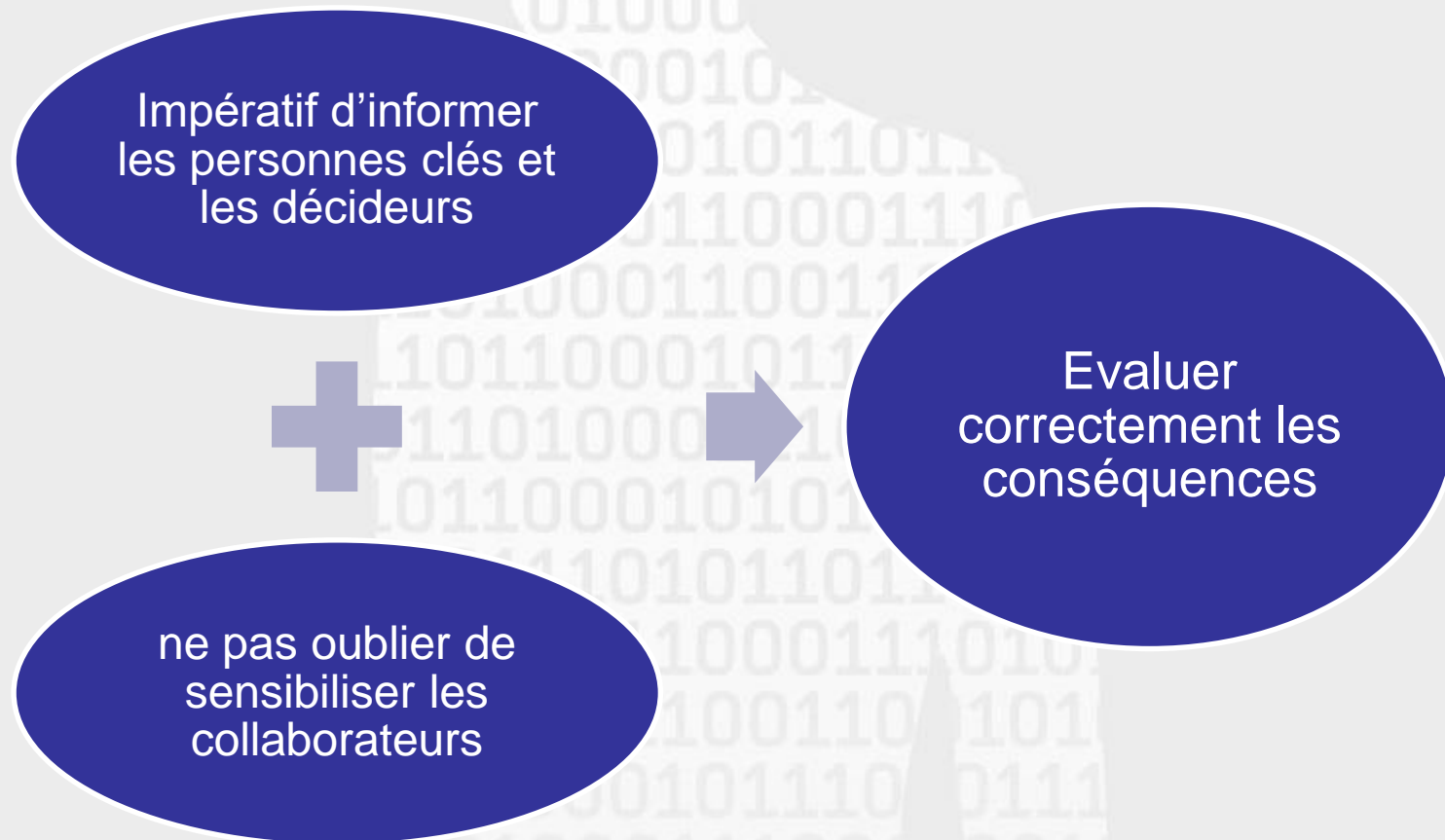
Réclamations et sanctions:

- **Réclamation:** peut être introduite auprès de l'autorité de la résidence habituelle, du lieu de travail de la personne concernée ou de celle où la violation aurait été commise
- **Sanctions administratives:** imposées par l'autorité de contrôle en complément ou à la place des mesures correctrices

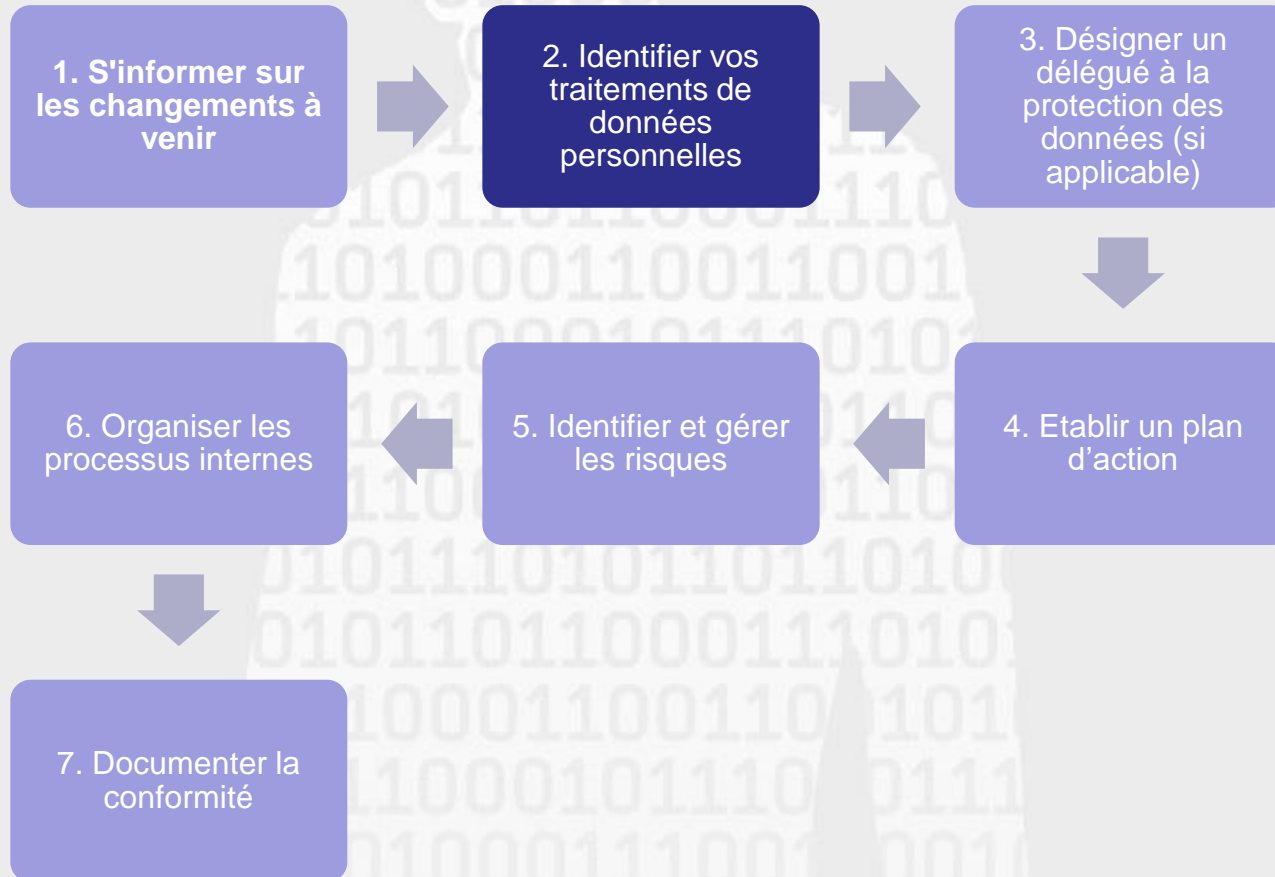


Une amende peut aller, au maximum, jusqu'à **20.000.000 EUR** ou, dans le cas d'une entreprise, à 4% de son chiffre d'affaires annuel total au niveau mondial.

Etape 1/7 : S'informer sur les changements à venir



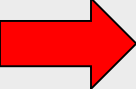
Les 7 étapes pour préparer sa conformité



Etape 2/7 : Identifier vos traitements de données personnelles

Impossible de se conformer sans connaître:

- Les **données** collectées
- Les **flux** de données
- Les **traitements** effectués

 Solution: Inventaire des traitements de données dès maintenant.



Obligation de tenir un **registre des traitements** de données dès mai 2018 (sauf exceptions).

Etape 2/7 : Identifier vos traitements de données personnelles

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
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, etc.)		
Données de connexion (adress IP, logs, etc.)		
Données de localisation (déplacements, données GPS, GSM, etc.)		

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

Illustratif

@ CNIL

@ CPVP

@ CNPD & LIST



GDPR-CST

Registre des activités de traitement

Partie 2: Traitements

Title: **Contract management**

Creat. on: 18 July 2017 Updat. on: 05 October 2017
 Creat. by: Paul Richard Updat. by: Paul Richard

Draft

Partie 2: Traitements

Title: **Analyse**

Creat. on: 18 July 2017 Updat. on: 05 October 2017
 Creat. by: Paul Richard Updat. by: Paul Richard

Draft

Partie 2: Traitements

Title: **Invoicing**

Creat. on: 08 August 2017 Updat. on: 05 October 2017
 Creat. by: Paul Richard Updat. by: Paul Richard

Draft

Partie 2: Traitements

Title: **Payroll**

Creat. on: 05 October 2017 Updat. on: 05 October 2017
 Creat. by: Paul Richard Updat. by: Paul Richard

Draft

Partie 2: Traitements

Title: **Maintenance**

Creat. on: 06 October 2017 Updat. on: 06 October 2017
 Creat. by: Paul Richard Updat. by: Paul Richard

Draft

Partie 2: Traitements

Title: **Infrastructure**

Creat. on: 06 October 2017 Updat. on: 06 October 2017
 Creat. by: Paul Richard Updat. by: Paul Richard

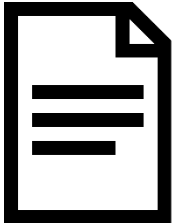
Draft

Etape 2/7 : Identifier vos traitements de données personnelles


Les questions essentielles:



QUI
est en charge du
traitement ?




QU'EST-ce
qui est traité?



POURQUOI
cela est traité?



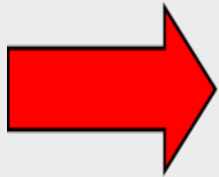
OÙ
est-ce que c'est traité?



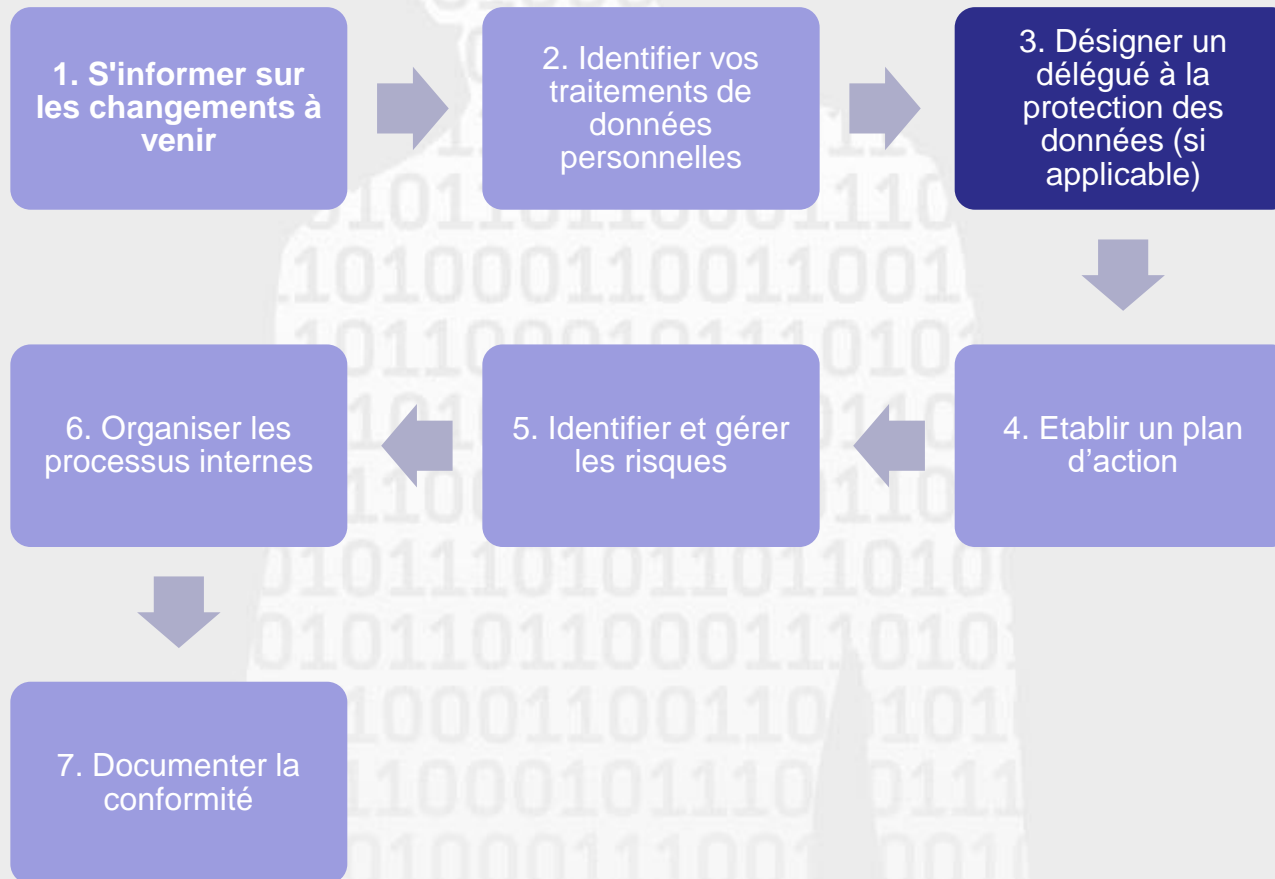
JUSQU'À QUAND
cela est traité ?



COMMENT
c'est protégé?



Les 7 étapes pour préparer sa conformité



Etape 3/7 : Désigner un délégué à la protection des données (si applicable)

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.

Etape 3/7 : Désigner un délégué à la protection des données (si applicable)

Pilote à bord!

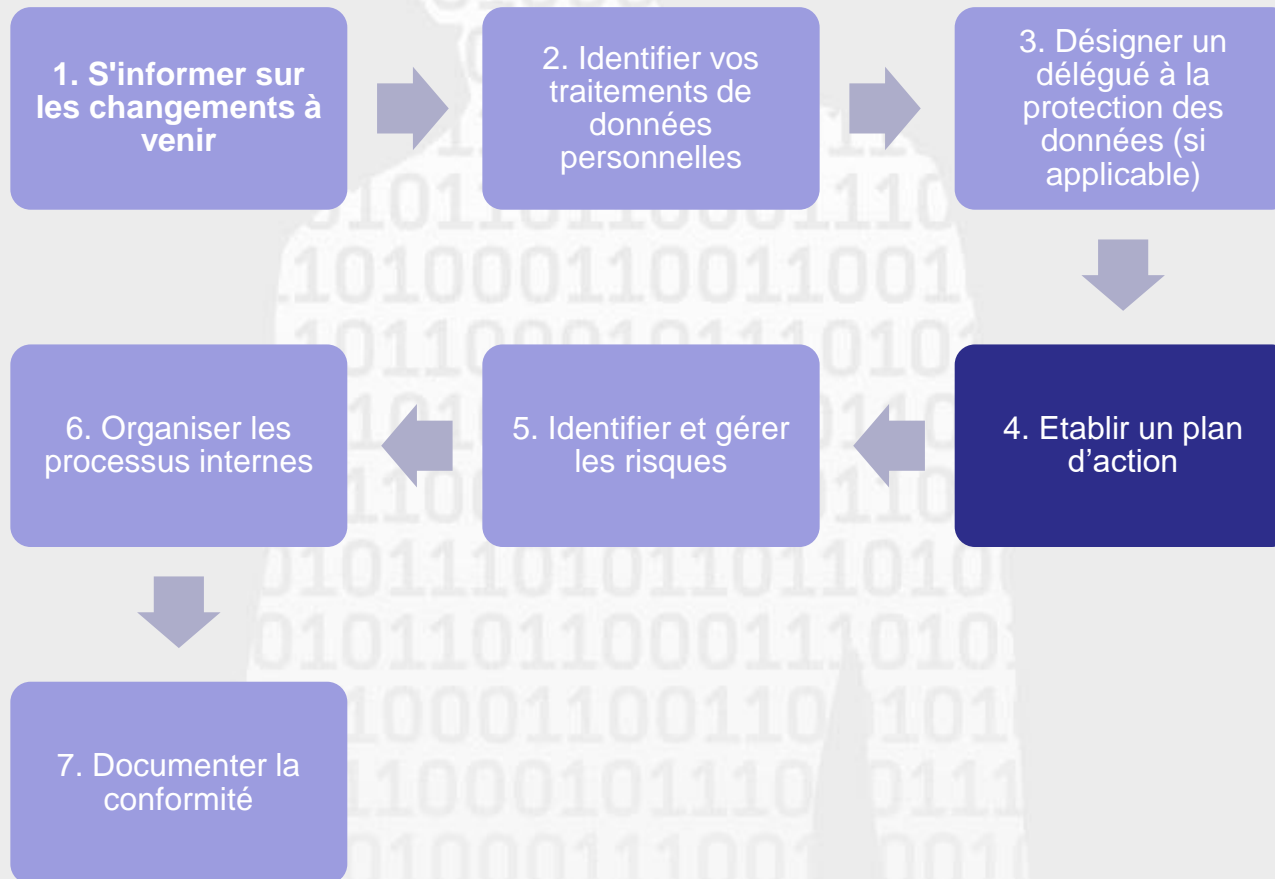
Mieux vaut prévenir: Nommer déjà à partir de maintenant un «chargé de la protection des données» (interne ou externe).

Atout majeur pour:

- respecter les obligations du RGPD,
- dialoguer avec les autorités de contrôle,
- réduire les risques de contentieux



Les 7 étapes pour préparer sa conformité



Etape 4/7 : Etablir un plan d'action

Points d'attention essentiels:

- Utilisez que **les données strictement nécessaires**;
- Identifiez **la base juridique** sur laquelle se fonde votre traitement:
 - Consentement de la personne concernée;
 - Nécessaire à l'exécution d'un contrat;
 - Obligation légale;
 - Nécessaire à la sauvegarde des intérêts vitaux;
 - Mission d'intérêt public / Exercice de l'autorité public;
 - Intérêt légitime;



Etape 4/7 : Etablir un plan d'action

Points d'attention essentiels:

- Révisez vos **mentions d'information**;
- N'oubliez pas vos **sous-traitants**: révisez l'ensemble des contrats avec les sous-traitants;
- Prévoyez les modalités d'exercice des **droits des personnes** concernées (p.ex. procédure de gestion des demandes de rectification ou d'accès);
- Vérifiez les **mesures de sécurité**.

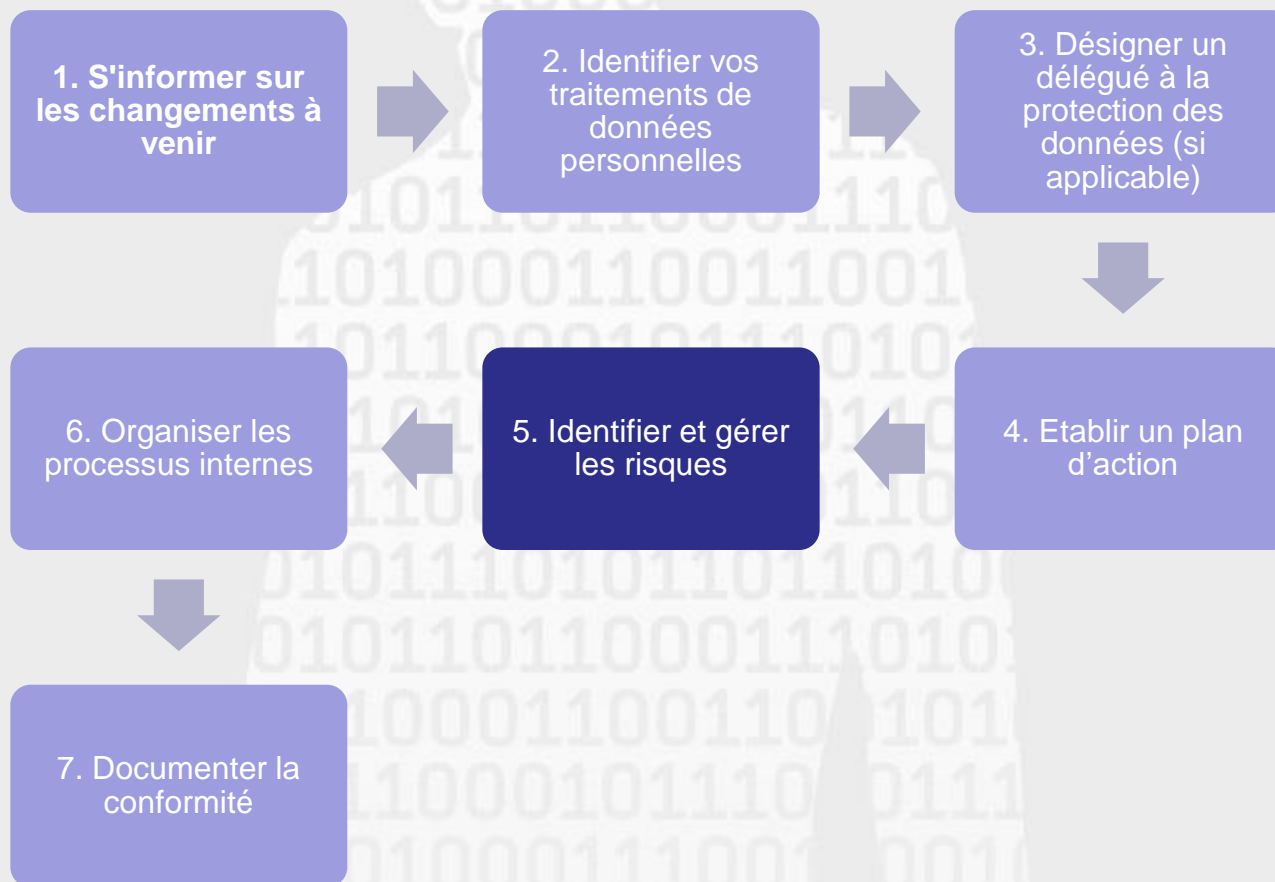
Etape 4/7 : Etablir un plan d'action

Une vigilance particulière pour:

- **Données sensibles** (santé, opinions politiques, appartenance syndicale, infractions pénales...);
- **Certains traitements** de données (surveillance systématique à grande échelle, profilage ...);
- Les transferts de données **hors UE**.



Les 7 étapes pour préparer sa conformité



Etape 5/7 : Identifier et gérer les risques

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



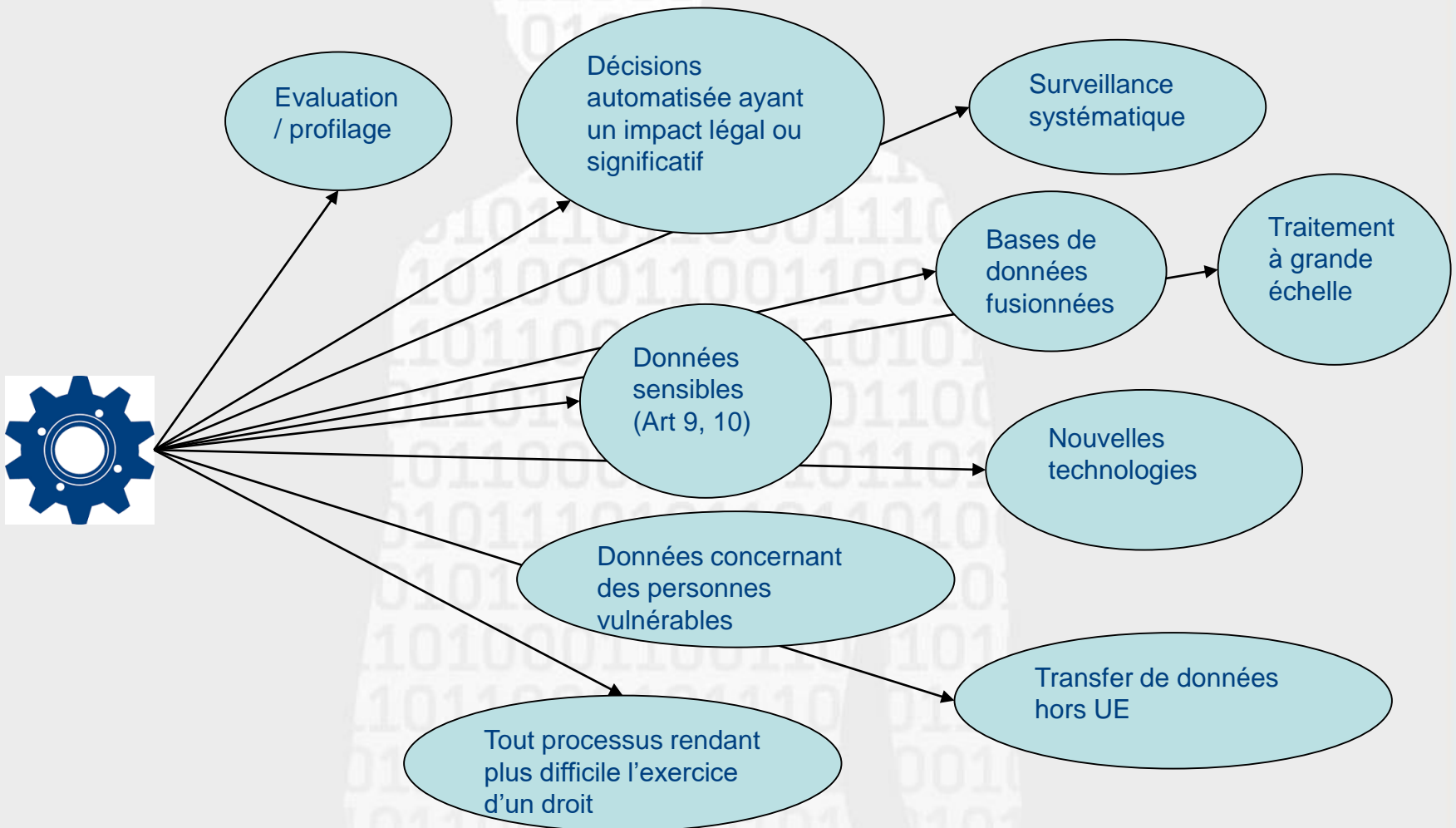
Le RT doit effectuer une analyse d'impact

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

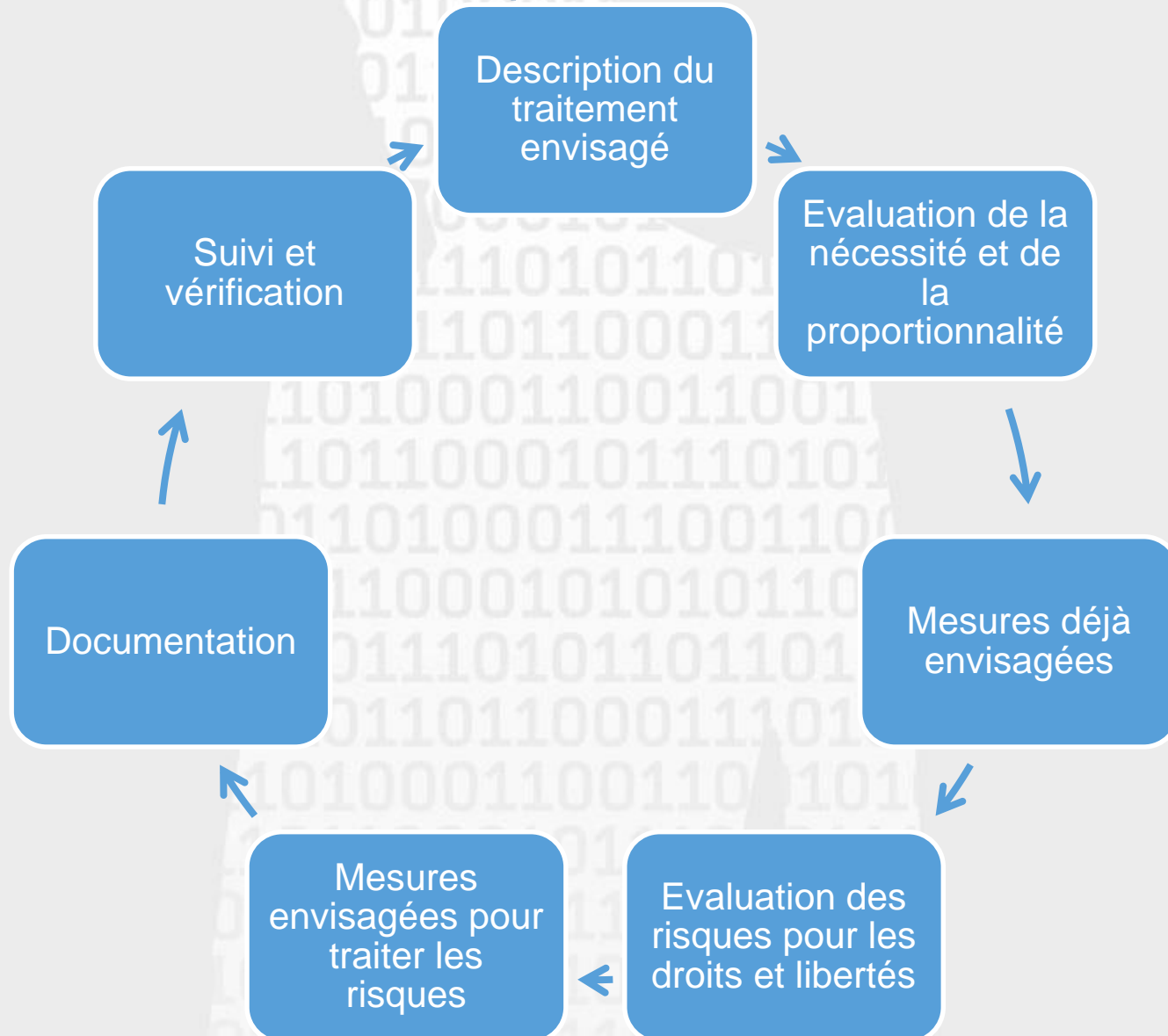
(*Data Protection Impact Assessment - DPIA*)

Critères pour mener un DPIA

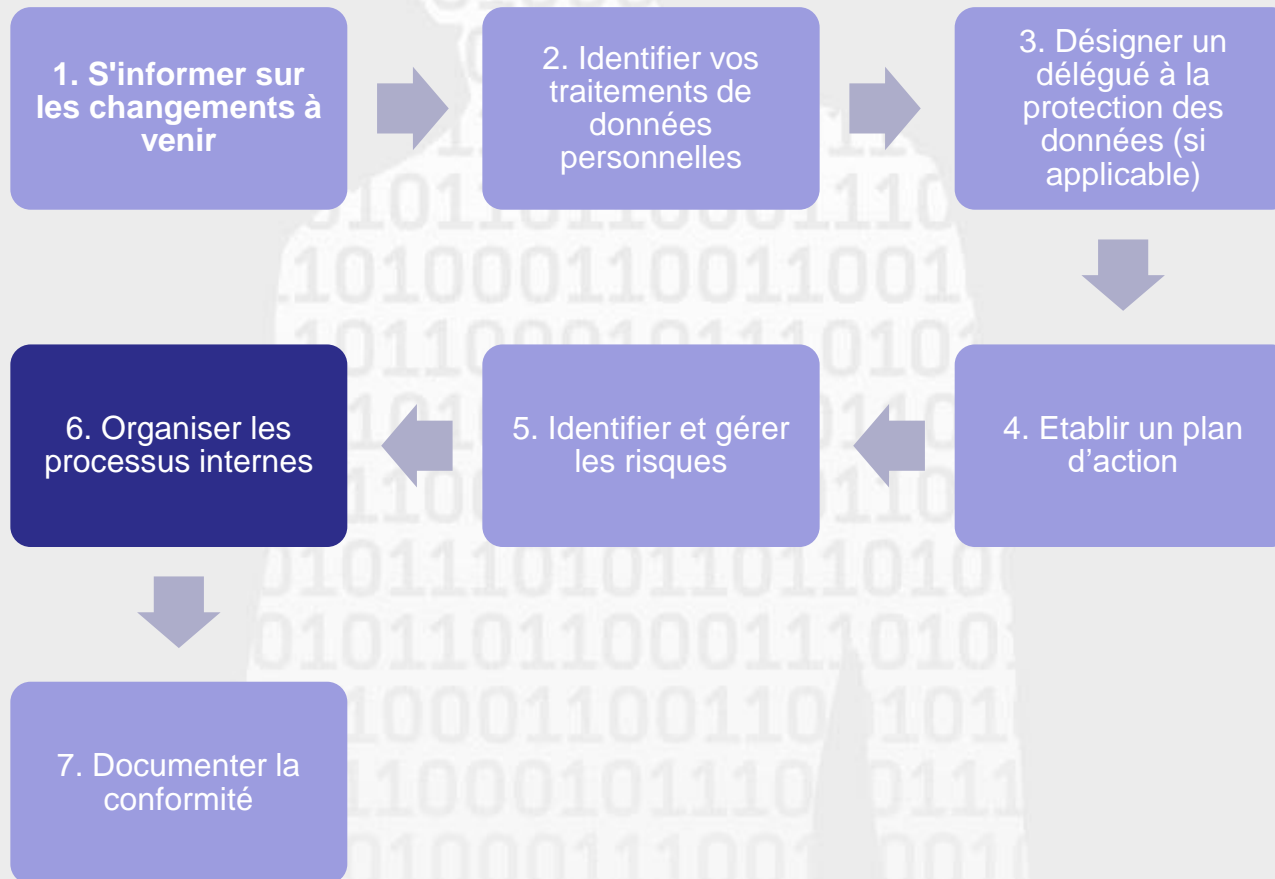
Un seul traitement ou un ensemble de traitements similaires



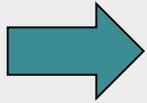
Les étapes d'un DPIA



Les 7 étapes pour préparer sa conformité



Etape 6/7 : Organiser les processus internes



Mise en place de **procédures internes**
pour pouvoir **anticiper les demandes et problèmes**
liés aux traitements de données



Exemple:

Une personne concernée veut faire une demande de rectification

- Si vous avez un site web, prévoyez un formulaire que la personne puisse remplir en ligne;
- Compétence interne pour le traitement de ces demandes?;
- Prise de décision par qui? Changement et/ou réponse négative à la personne concernée?

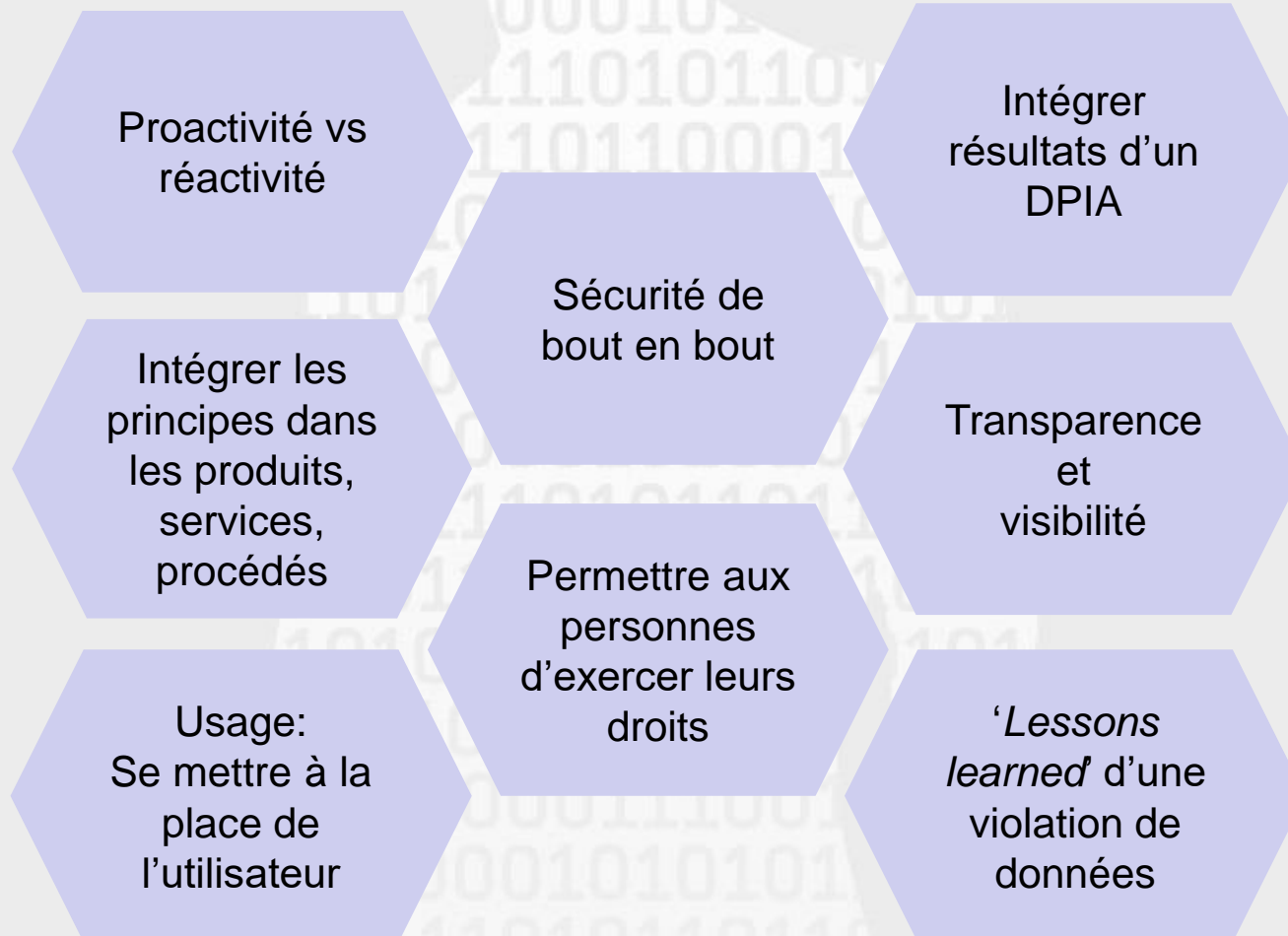
Etape 6/7 : Organiser les processus internes

Organiser les processus implique notamment :

- de prendre en compte la protection des données personnelles **dès la conception et par défaut (*Privacy by design / Privacy by default*)**;
- de **sensibiliser** vos collaborateurs et d'**organiser** la remontée d'information;
- de traiter les **réclamations** et les demandes des personnes concernées quant à **l'exercice de leurs droits**;
- d'anticiper les **violations de données**.

Etape 6/7 : Organiser les processus internes

Protection des données dès la conception



Etape 6/7 : Organiser les processus internes

Protection des données dès la conception

General

Change privacy options

Let apps use advertising ID to make ads more interesting to you based on your app usage (turning this off will reset your ID)

On

Let websites provide locally relevant content by accessing my language list

On

Let Windows track app launches to improve Start and search results

On

General

Change privacy options

Let apps use advertising ID to make ads more interesting to you based on your app usage (turning this off will reset your ID)

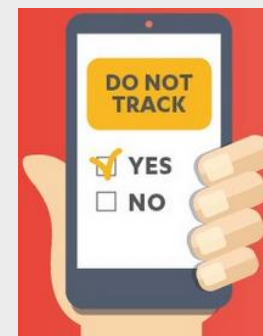
Off

Let websites provide locally relevant content by accessing my language list

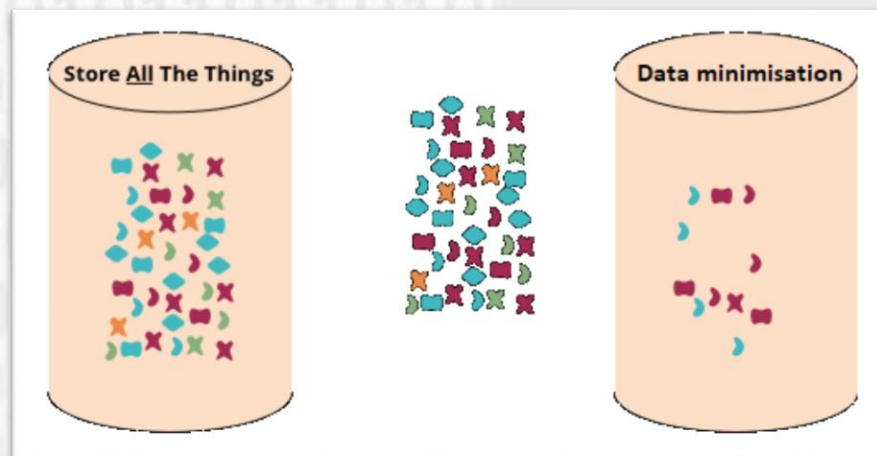
Off

Let Windows track app launches to improve Start and search results

Off



Protection des données par défaut

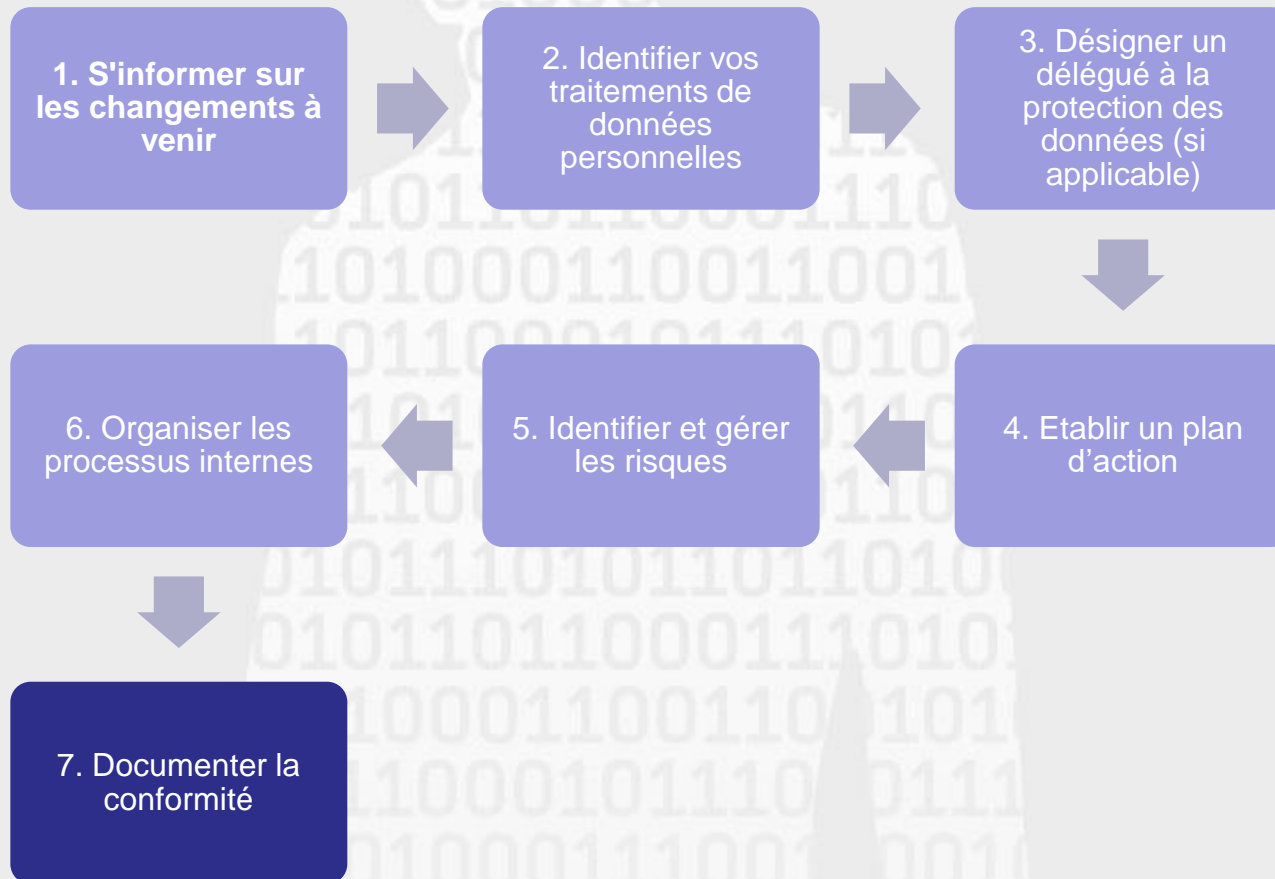


Etape 6/7 : Organiser les processus internes

Objectifs principaux:

- Créer une **culture globale** de la protection des données;
- **Anticiper** dès le départ les risques et les problèmes;
- Développer une gestion sécurisée de l'information **tout le long du cycle de vie** des données;
- **Informé en toute transparence** sur l'ensemble de droits.

Les 7 étapes pour préparer sa conformité



Etape 7/7 : Documenter la conformité

Obligation de prouver votre conformité



Preuve par la documentation
(qui englobe aussi les procédures)
qui doit être régulièrement
réexaminée et actualisée



Etape 7/7 : Documenter la conformité

Documentation sur vos traitements de données personnelles:

- Le registre des traitements (pour les RT) ou des catégories d'activités de traitements (pour les ST)
- Les DPIA (analyses d'impact)
- L'encadrement des transferts de données hors de l'UE
- Le registre des violations de données

L'information des personnes:

- Les mentions d'information
- Les modèles de recueil du consentement des PC
- Les procédures mises en place pour l'exercice des droits des PC

Autre documentation:

- Les procédures internes en cas de violations de données
- Les preuves que les PC ont donné leur consentement lorsque le traitement de leurs données repose sur cette base juridique

Etape 7/7 : Documenter la conformité

Ne pas oublier de documenter la gestion des flux de données:

- Les documents de vérification de la conformité des utilisateurs externes de vos données;
- Contrats avec les tiers pour réutiliser les données;
- Contrats avec les sous-traitants.

Commission nationale pour la protection des données

Merci pour votre attention!



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