Séances d'information

Règlement général sur la protection des données

La conformité au nouveau règlement: comment se préparer?

CNPD
COMMISSION NATIONALE POUR LA PROTECTION DES DONNÉES

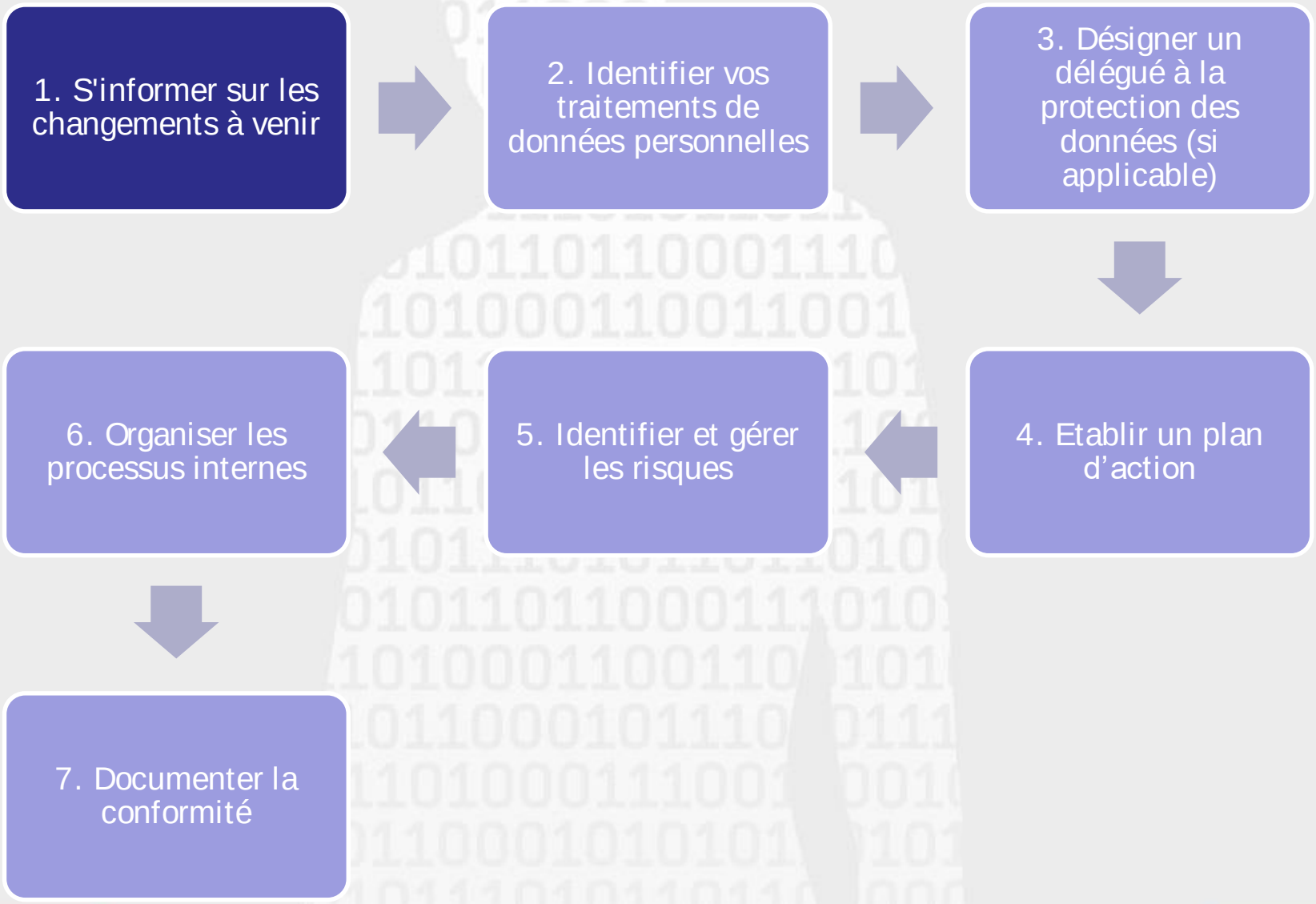
18 octobre 2017

Esch-sur-Alzette (Belval)

Christophe Buschmann

Guillaume Byk

7 étapes pour préparer sa conformité



1. S'informer sur les changements à venir 1/11

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

I

(Actes législatifs)

RÈGLEMENTS

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)

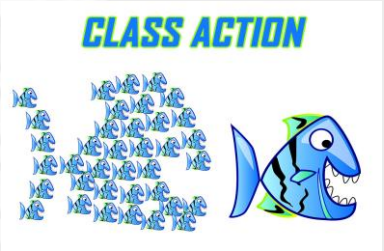
(Texte présentant de l'intérêt pour l'EEE)

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

RGPD – LES CHANGEMENTS CLÉS

1. S'informer sur les changements à venir 2/11

- **a) 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.



1. S'informer sur les changements à venir 3/11

- **b) 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);

Risk based approach!

  - **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.

1. S'informer sur les changements à venir 4/11

- **c) Nouveaux concepts:**

- 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

1. S'informer sur les changements à venir 5/11

- **d) Champ d'application territorial plus large:**
  - soit un RT ou un ST sont établi 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;

1. S'informer sur les changements à venir 6/11

- **e) 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.

1. S'informer sur les changements à venir 7/11

- **f) 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.

1. S'informer sur les changements à venir 8/11

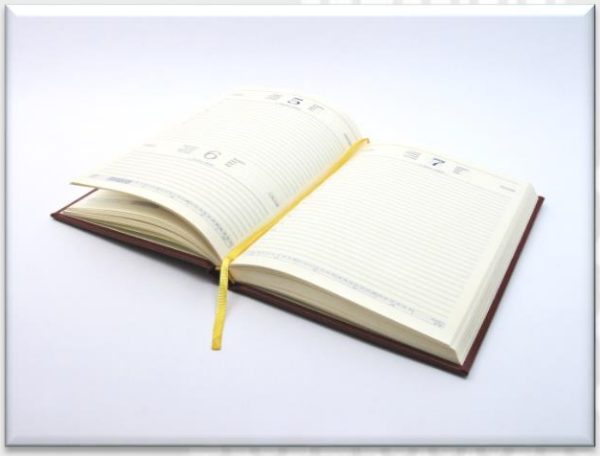
Impératif d'informer les personnes clés et les décideurs

+

ne pas oublier de sensibiliser les collaborateurs

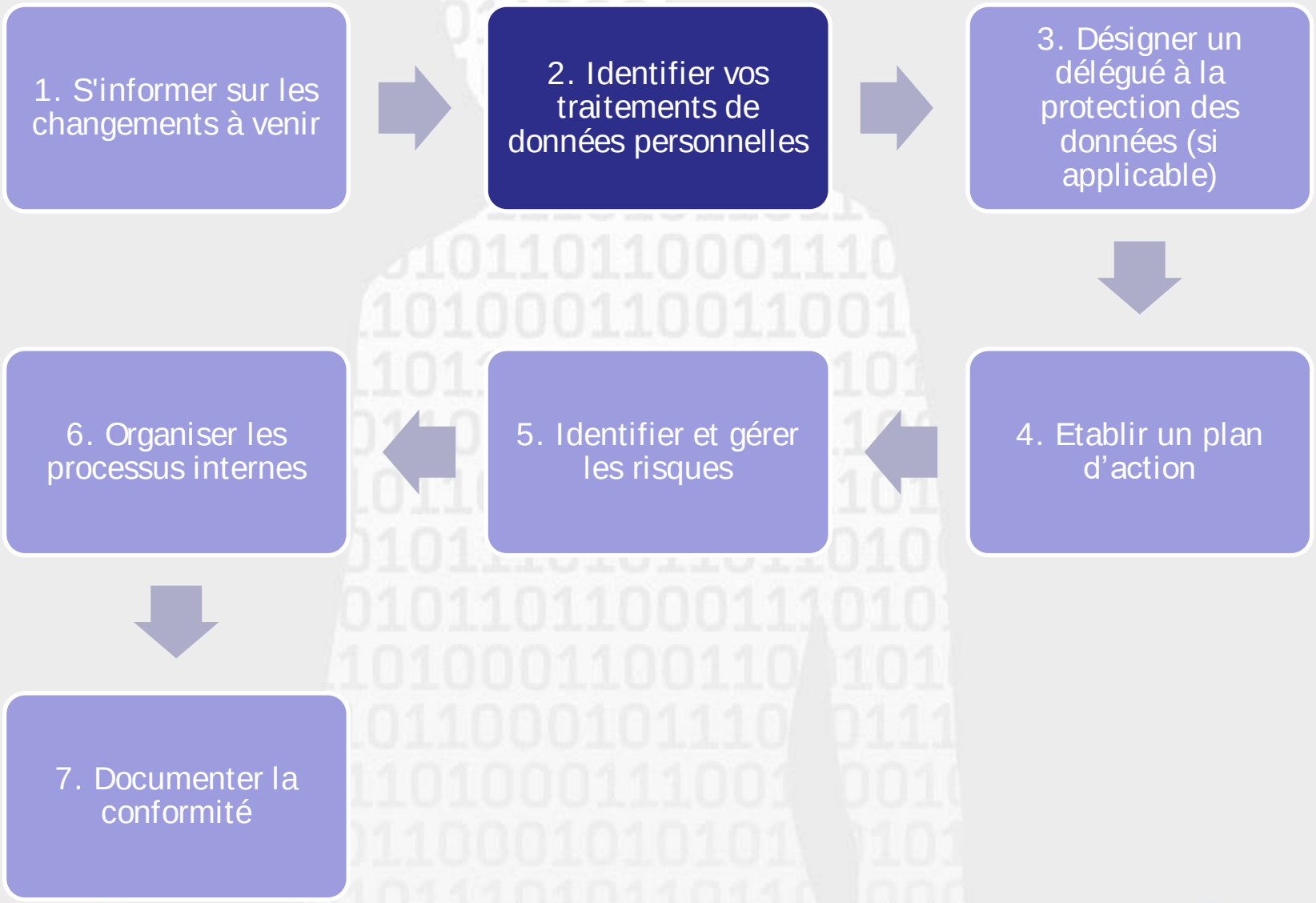
Evaluer correctement les conséquences

1. S’informer sur les changements à venir 9/11



Date butoir:
25 mai 2018

7 étapes pour préparer sa conformité



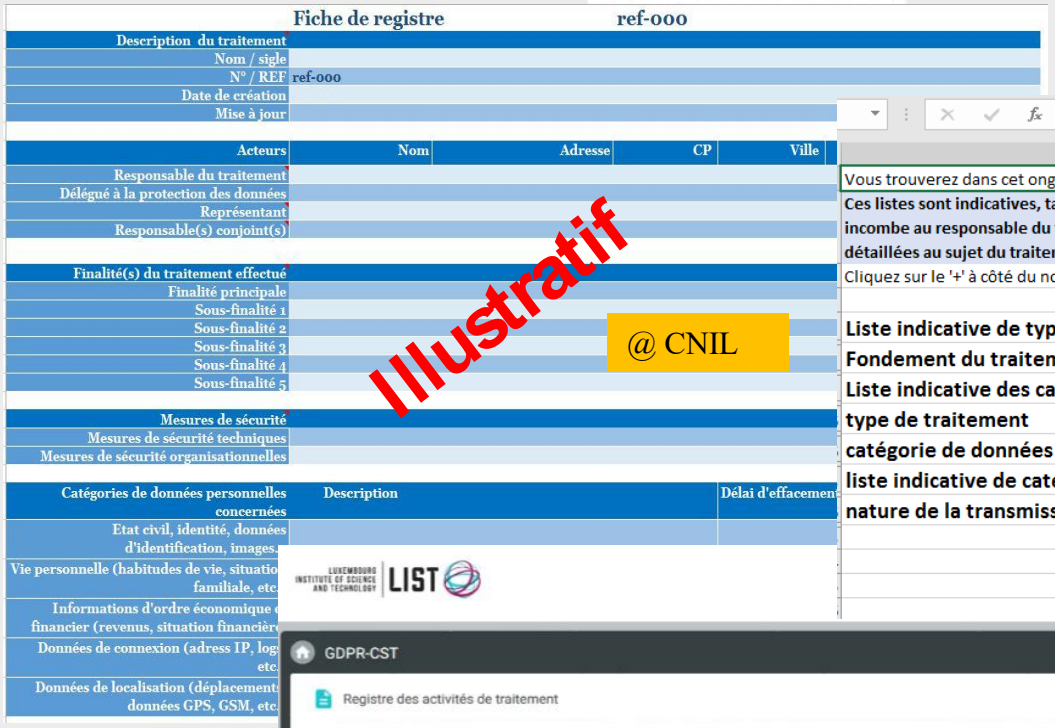
2. Identifier vos traitements de données personnelles 1/3

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).



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	Description	Délai d'effacement
Etat civil, identité, données d'identification, images		
Vie personnelle (habitudes de vie, situation familiale, etc		
Informations d'ordre économique financier (revenus, situation financière		
Données de connexion (adress IP, log etc		
Données de localisation (déplacement données GPS, GSM, etc		

Illustratif

@ CNIL

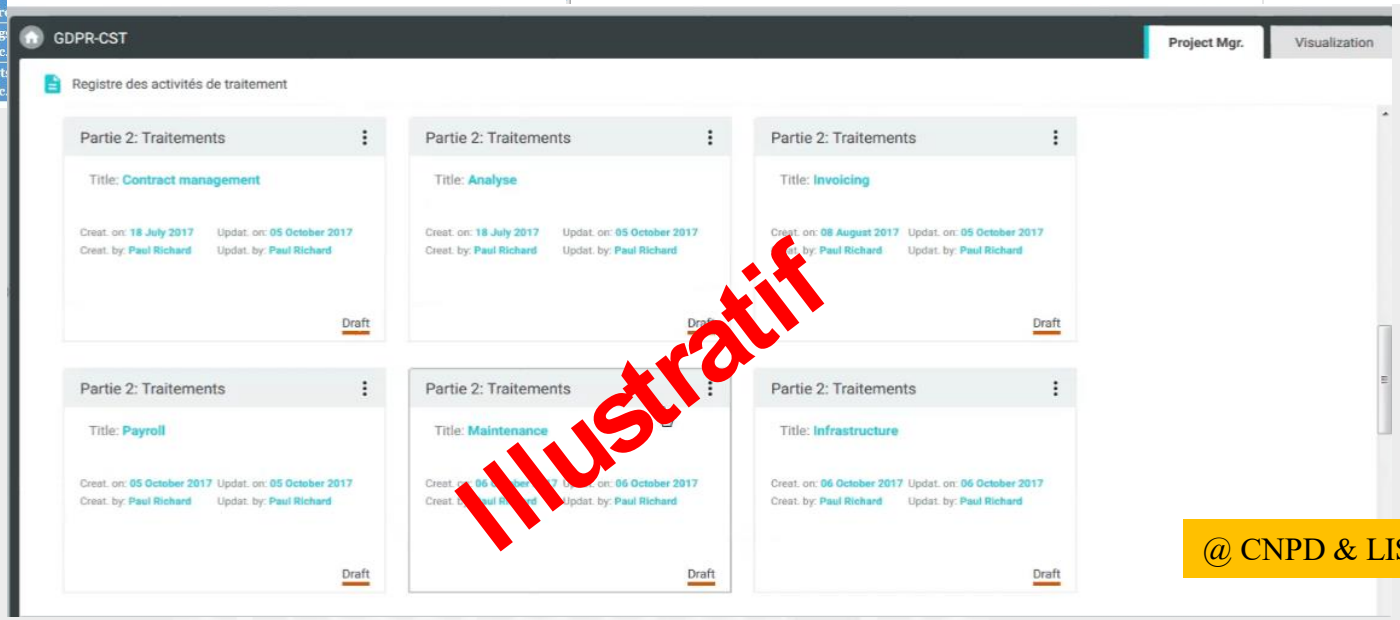
LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | LIST

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

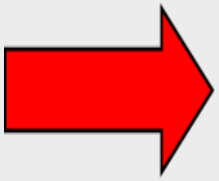


Illustratif

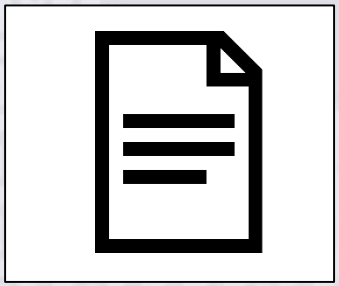
@ CNPD & LIST

2. Identifier vos traitements de données personnelles 3/3

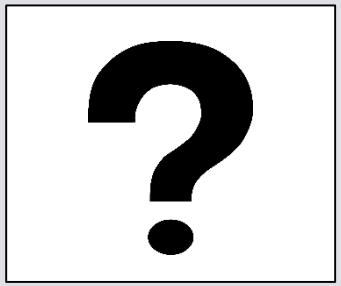
Les questions essentielles:



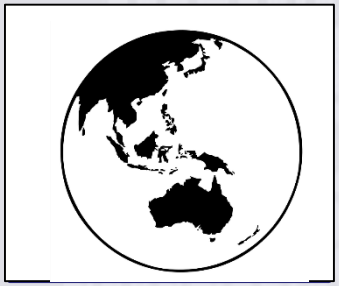
QUI
est en charge du traitement ?



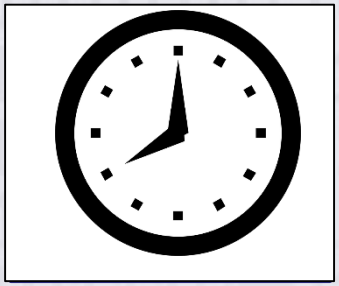
QU'EST-ce qui est traité?



POURQUOI cela est traité?



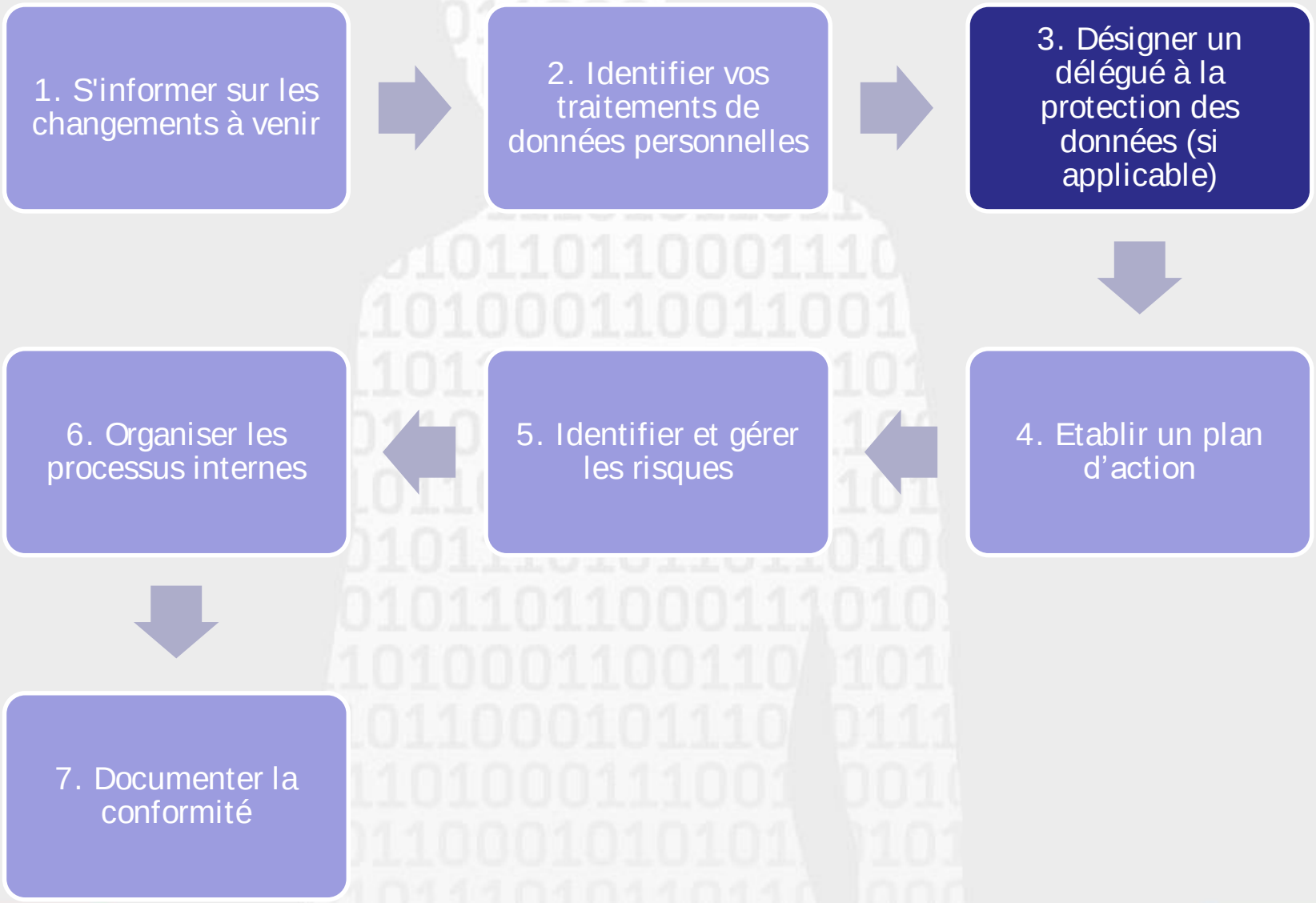
OÙ
est-ce que c'est traité?



JUSQU'À QUAND
cela est traité ?

COMMENT
c'est protégé?

7 étapes pour préparer sa conformité



3. Désigner un délégué à la protection des données (si applicable) 1/3

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)

3. Désigner un délégué à la protection des données (si applicable) 2/3

Rôle?

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

Atout majeur pour:

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

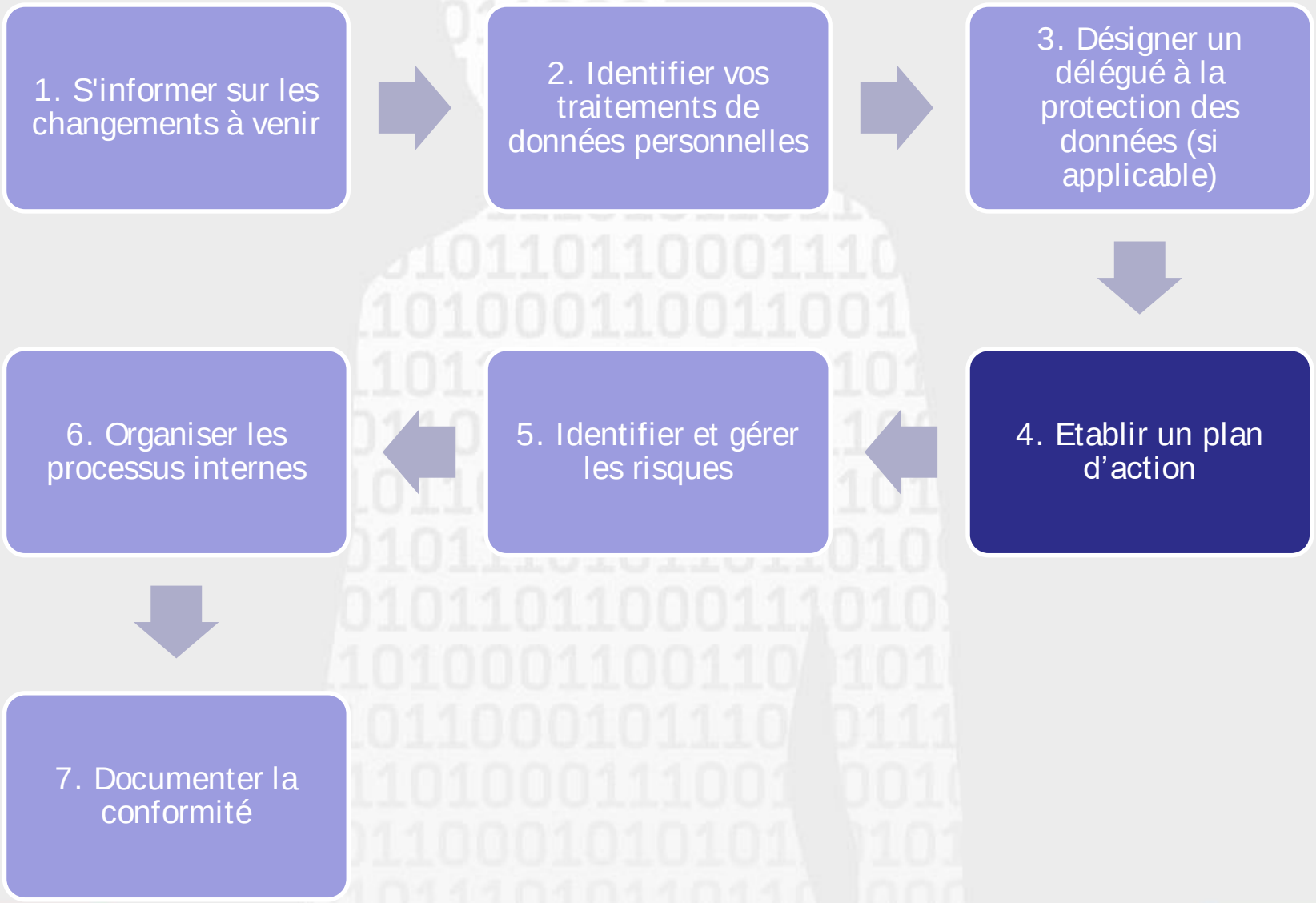
3. Désigner un délégué à la protection des données (si applicable) 3/3

Y a-t-il un pilote à bord?

Mieux vaut prévenir:

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

7 étapes pour préparer sa conformité



4. Etablir un plan d'action 1/3

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;

4. Etablir un plan d'action 2/3

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**.

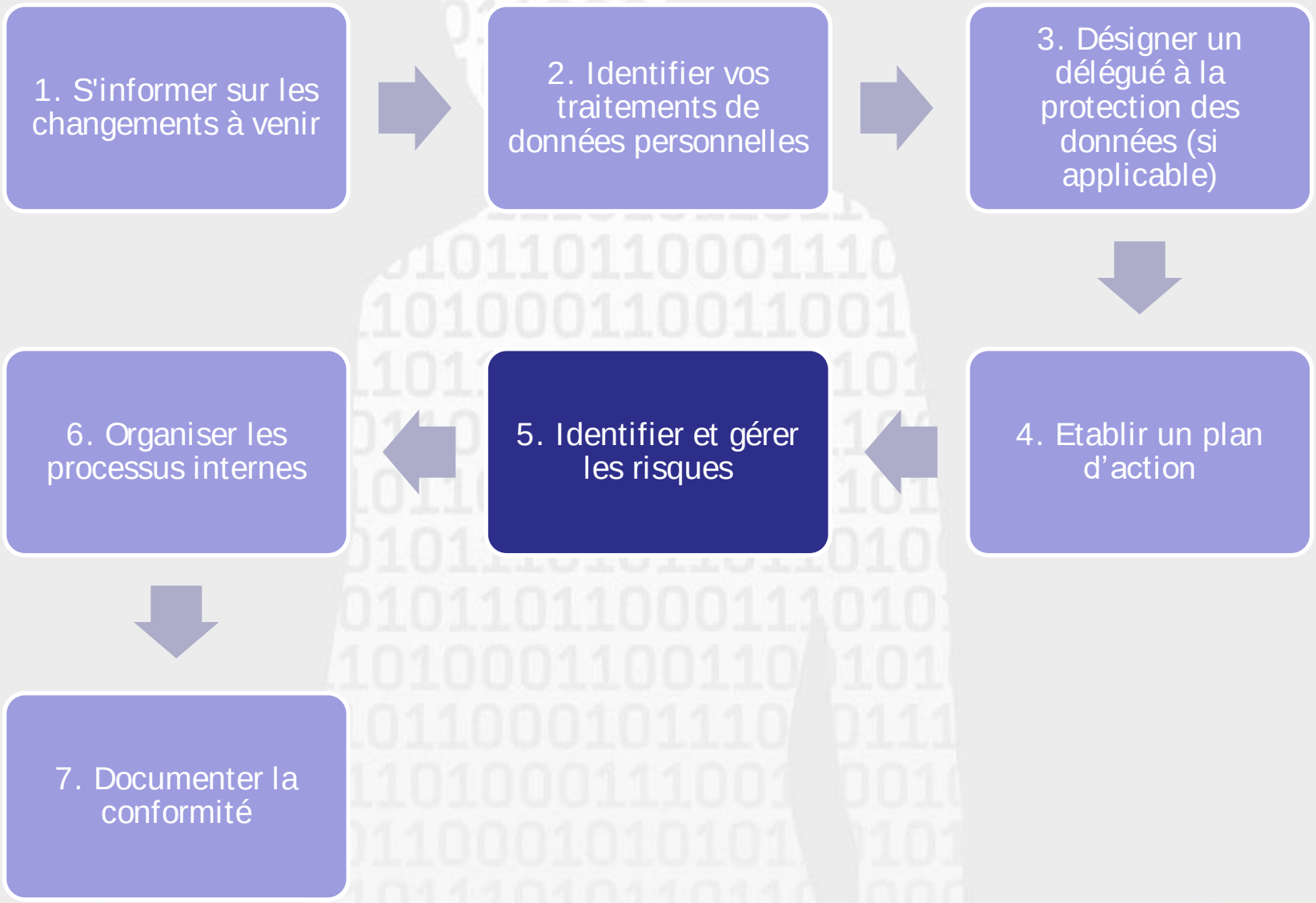
4. Etablir un plan d'action 3/3

Une vigilance particulière pour:

- **Données sensibles** (santé, opinions politiques, appartenance syndicale, infractions pénales…);

- **Certains traitements** de données (surveillance systématique à grande échelle, profilage …);
- Les transfers de données **hors UE.**

7 étapes pour préparer sa conformité



5. Identifier et gérer les risques

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

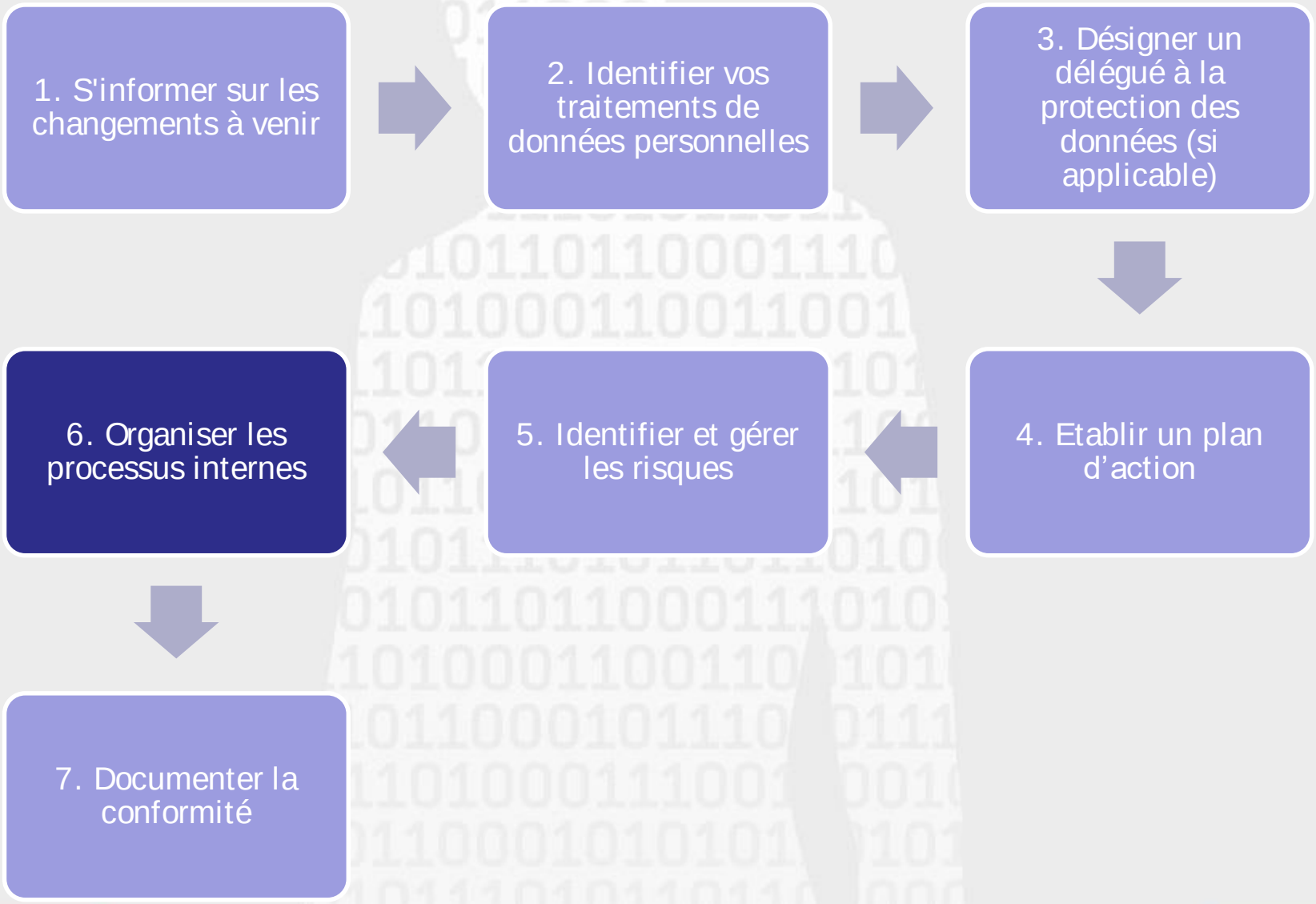
Le RT doit effectuer une

analyse d'impact

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

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

7 étapes pour préparer sa conformité



6. Organiser les processus internes 1/5

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?

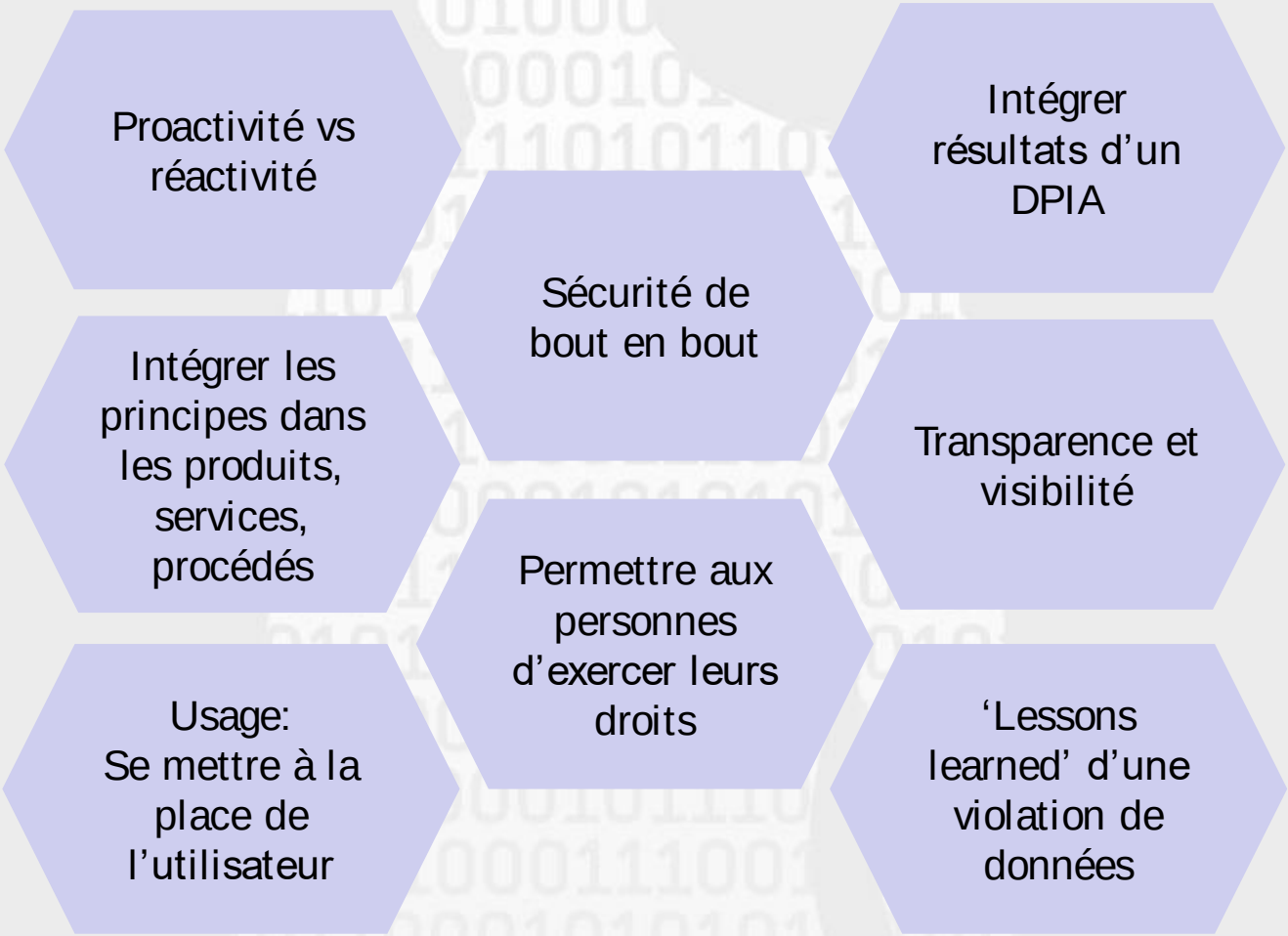
6. Organiser les processus internes 2/5

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**.

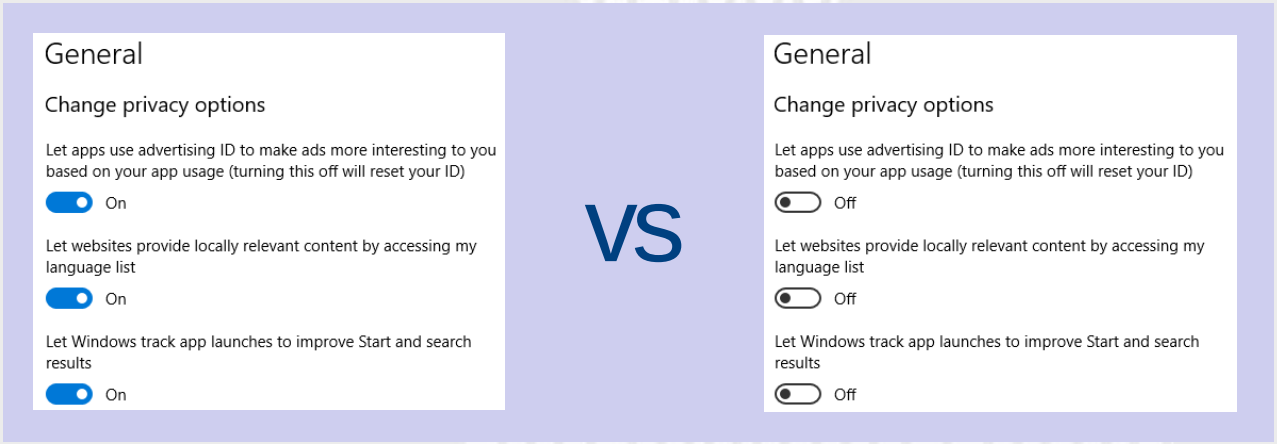
6. Organiser les processus internes 3/5

Protection des données dès la conception: Le 'Quoi'

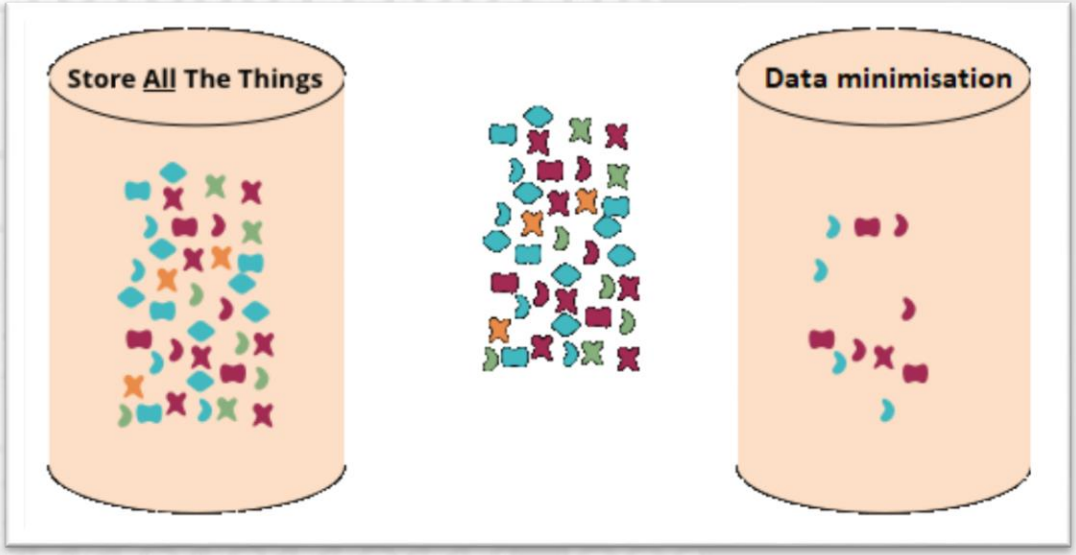


6. Organiser les processus internes 4/5

Protection des données dès la conception



Protection des données par défaut

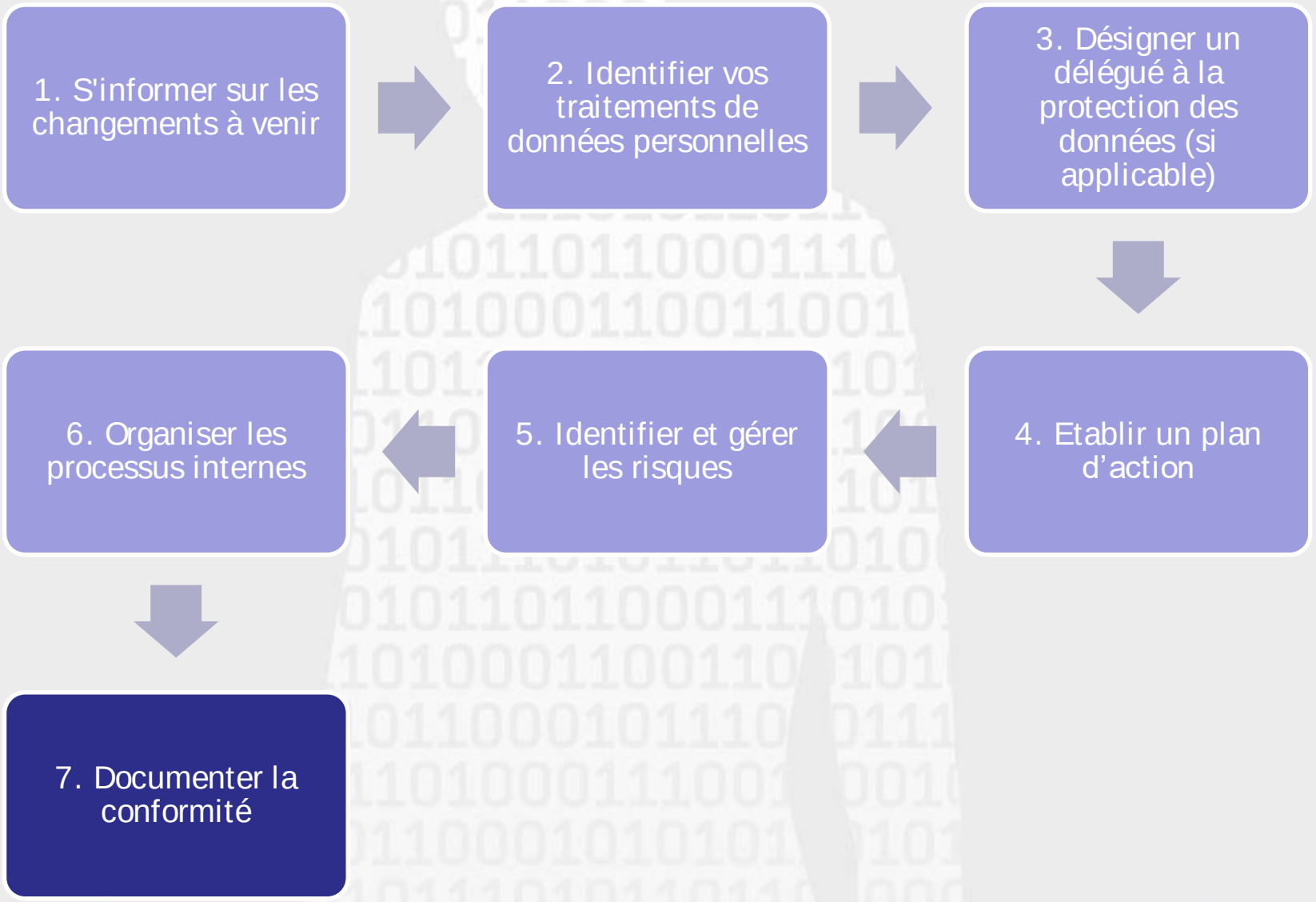


6. Organiser les processus internes 5/5

Objectifs principaux:

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

7 étapes pour préparer sa conformité



7. Documenter la conformité 1/3

Obligation de prouver votre conformité

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

7. Documenter la conformité 2/3

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 analyses d'impact relatives à la protection des données pour les traitements susceptibles d'engendrer des risques élevés pour les droits et libertés des personnes;
- L'encadrement des transferts de données hors de l'UE (notamment, les clauses contractuelles types, les BCR et certifications);
- Le registre qui documente toutes les violations de données (celui-ci renseigne les conséquences de la violation et les mesures prises pour y remédier).

L'information des personnes:

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

Les contrats et autre documentation:

- Les contrats avec les ST;
- Les procédures internes en cas de violations de données;
- Les preuves que les personnes concernées ont donné leur consentement lorsque le traitement de leurs données repose sur cette base juridique.

7. Documenter la conformité 3/3

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

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

Info

Pour vous aider dans la mise en œuvre de votre conformité, la CNPD procède:

- au développement d'un outil d'aide à la conformité (*Compliance Support Tool*);
- à la création de brochures;
- à l'actualisation de son site web.

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