Formation CNPD:
Introduction à la protection des données

Les obligations du responsable du traitement et du sous-traitant

Esch-sur-Alzette

11 juin 2018

Arnaud Habran

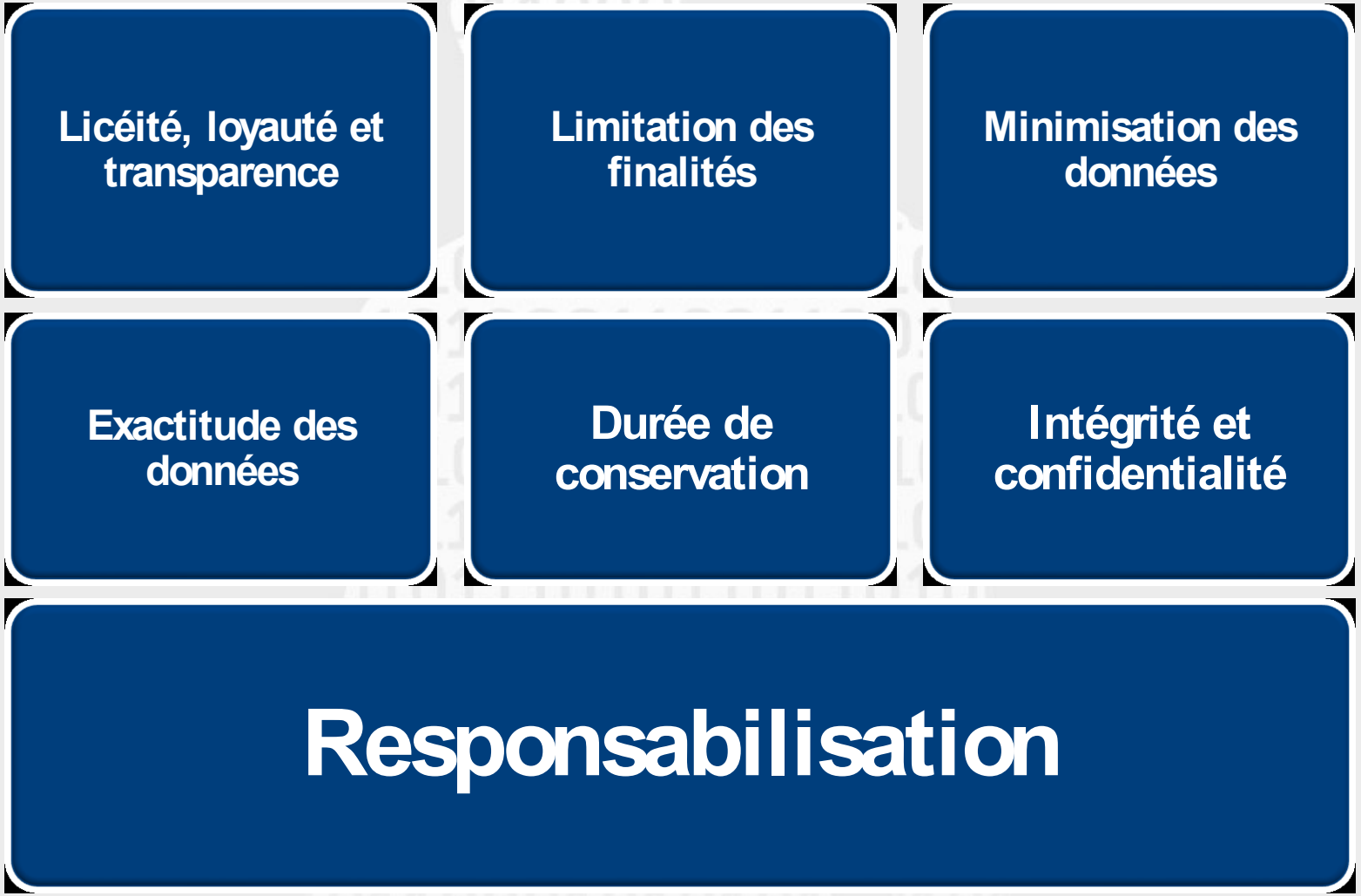
Service juridique

Programme

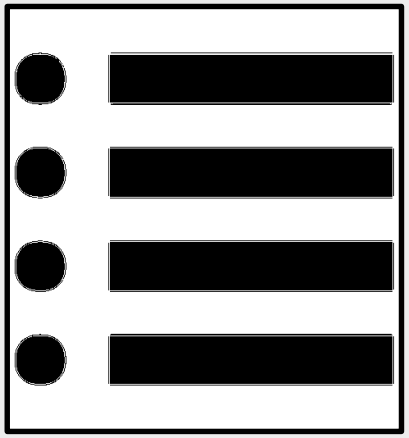
1. Introduction
2. Les notions élémentaires
3. Les droits des personnes concernées
4. **Les obligations du responsable du traitement et du sous-traitant**
5. Le rôle de la CNPD


Obligations du responsable du traitement
Principes de qualité des données
Registre des activités
Sécurité et notification de violation de données
Analyse d'impact
Délégué à la protection des données
Sous-traitance
Transferts vers des pays tiers
Droits des personnes concernées
Gouvernance interne

1. Principes de qualité des données



2. Registre des activités de traitement



Un document/fichier qui reprend la description de l'ensemble de vos traitements

RGPD: Registre qui, pour chaque activité de traitement, comporte notamment les informations suivantes:

a) le nom et les coordonnées du responsable du traitement (…)
b) les finalités du traitement;
c) une description des catégories de personnes concernées et des catégories de données à caractère personnel;
d) les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées (…)
e) le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale(…)
f) dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données;
g) dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles (…)

Exemples:

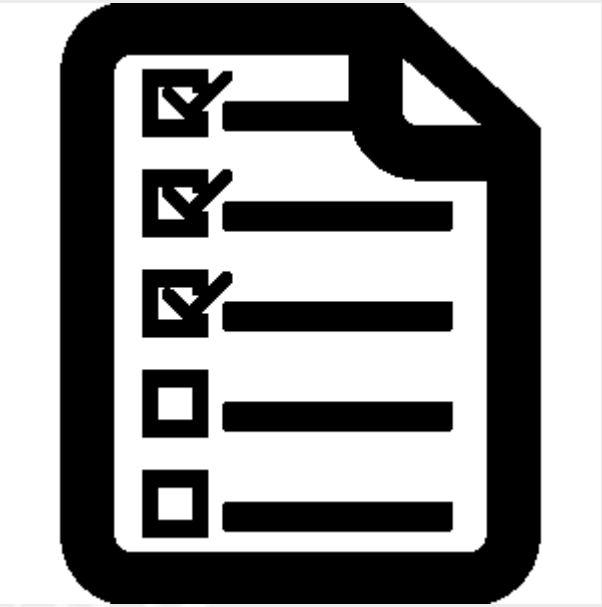
- « Compliance Support Tool » de la CNPD qui **permet aussi de générer un registre**
- Autres outils: CPVP (Commission belge), CNIL (Commission française)

Réutilisation: Le règlement n'est pas prescriptif quant à la forme du registre. Alors que les exemples ci-dessus peuvent vous aider à construire un registre nous vous recommandons de produire un registre qui est cohérent avec votre organisation – en terme de forme et vocabulaire utilisé.

2. Registre des activités de traitement

Checklist simplifiée

Objectif: Fournir une **aide pragmatique** afin d'évaluer de manière simple votre niveau de **maturité par rapport à un traitement de données**



La checklist proposée se concentre sur les principes de la protection des données du RGPD (art. 5). Sans être exhaustive elle peut cependant constituer un outil pragmatique. Ainsi elle peut constituer un élément de début – pour les question plus approfondies nous proposons de se référer aux chapitres respectifs du RGPD.

2. Registre des activités de traitement

Checklist simplifiée

Fiche signalétique

Rôles et responsabilités

- Analysez si vous êtes l'entreprise qui décide ce qui est fait avec les données ou si vous êtes exécutant

Données traitées

- Enumérer les types de données traitées (p.ex. noms, adresses, certificats de maladie, comptables,….)

Personnes concernées

- Enumérer les types personnes sur lesquelles porte le traitement (p.ex. clients, salariés, prospects, potentiels recrutés,…)

Finalité du traitement

- Décrire l'objectif que le traitement permet d'atteindre (p.ex. paiement des salaires, envoie de factures, prospection de potentiels clients,…)

Suppression

- Décrire quand les données seront effacées ou la durée de conservation

Flux de données

- Analysez si vous recevez ou transmettez les données à une autre organisation, y compris hors l'Union européenne

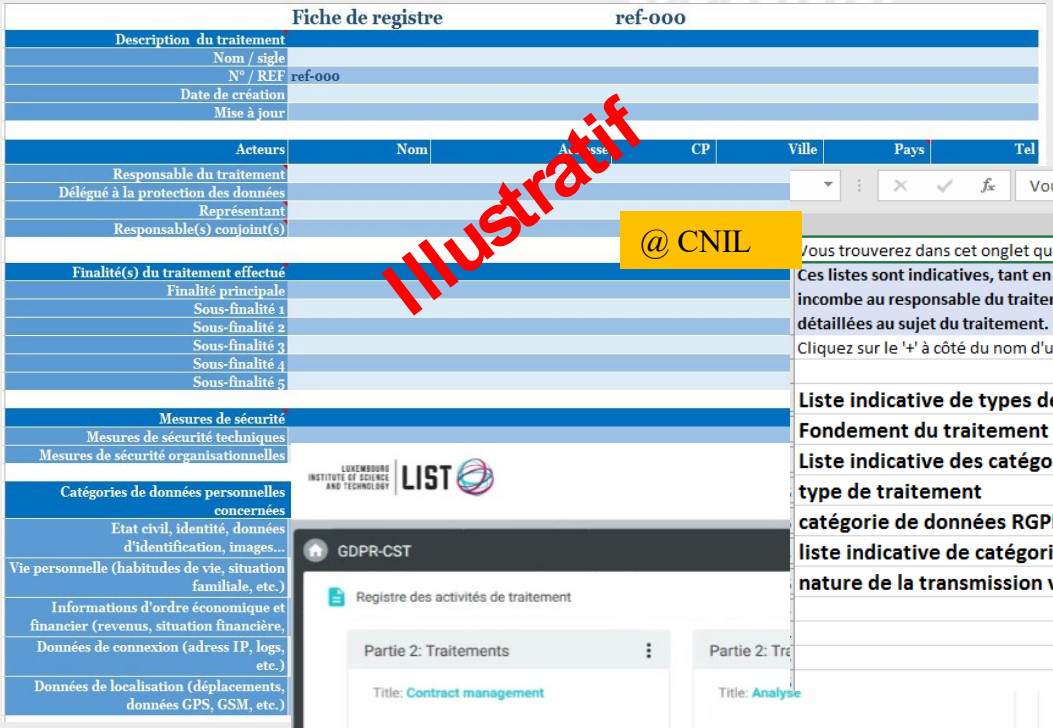
Cette fiche signalétique est inspirée des informations qui doivent figurer dans un « registre des activités de traitement » tel que défini dans l'article 30 du RGPD.

Questionnaire

	Questions	Remarque
1	Est-ce que j'ai le droit d'effectuer ce traitement?	**Principe: licéité**
2	Est-ce que les personnes concernées sont au courant du traitement?	**Principe: transparence**
3	Est-ce que je sais avec précision pourquoi je collecte ces données? / Est-ce que j'utilise ces données pour faire autre chose?	**Principe: limitation des finalités**
4	Est-ce que toutes les données sont nécessaires – pas seulement utiles?	**Principe: minimisation**
5	Est-ce que les données sont correctes et à jour?	**Principe: exactitude**
6	Est-ce que je dois supprimer les données à la fin du traitement – ou est-ce qu'il y a une nécessité (pas une utilité) de les garder?	**Principe: durée de conservation limitée**
7	Est-ce que les données sont sécurisées?	**Principe: sécurité**

Le questionnaire est inspiré des « principes relatifs au traitement de données à caractère personnel » tel que défini dans l'article 5 du RGPD.

2. Registre – quelques exemples



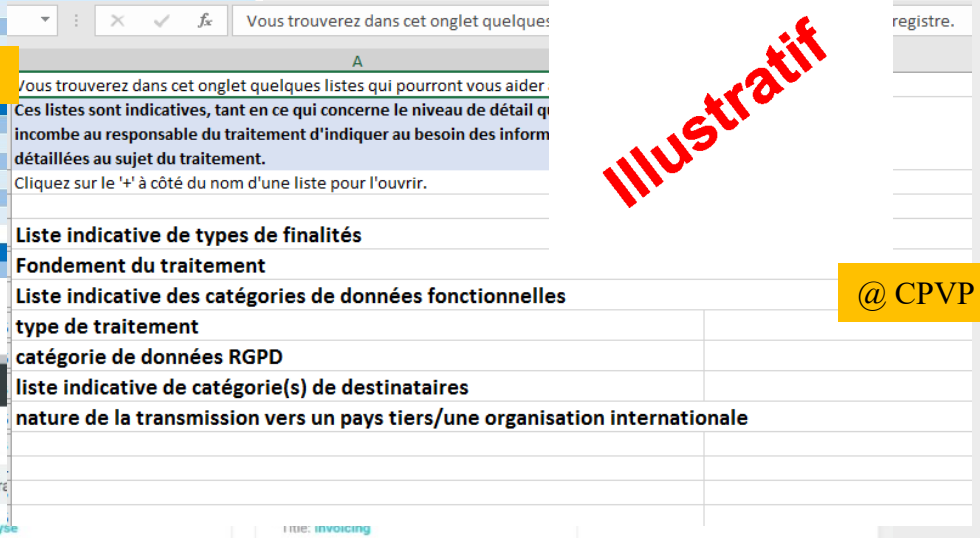
Fiche de registre	ref-000
Description du traitement	
Nom / sigle	
N° / REF	ref-000
Date de création	
Mise à jour	

Acteurs	Nom	Adresse	CP	Ville	Pays	Tel
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,
Données de connexion (adress IP, logs, etc.)
Données de localisation (déplacements, données GPS, GSM, etc.)

Illustratif

@ CNIL

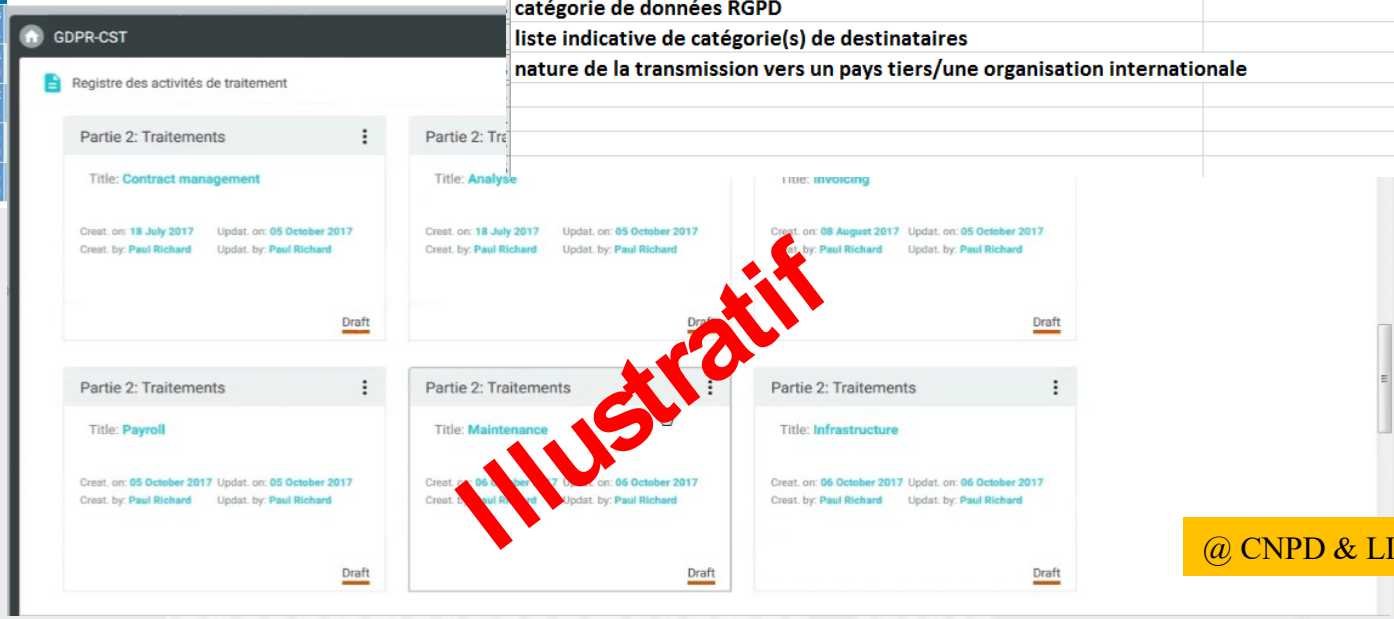


Vous trouverez dans cet onglet quelques listes qui pourront vous aider
Ces listes sont indicatives, tant en ce qui concerne le niveau de détail q
incombe au responsable du traitement d'indiquer au besoin des inform
détaillées au sujet du traitement.
Cliquez sur le '+' à côté du nom d'une liste pour l'ouvrir.

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



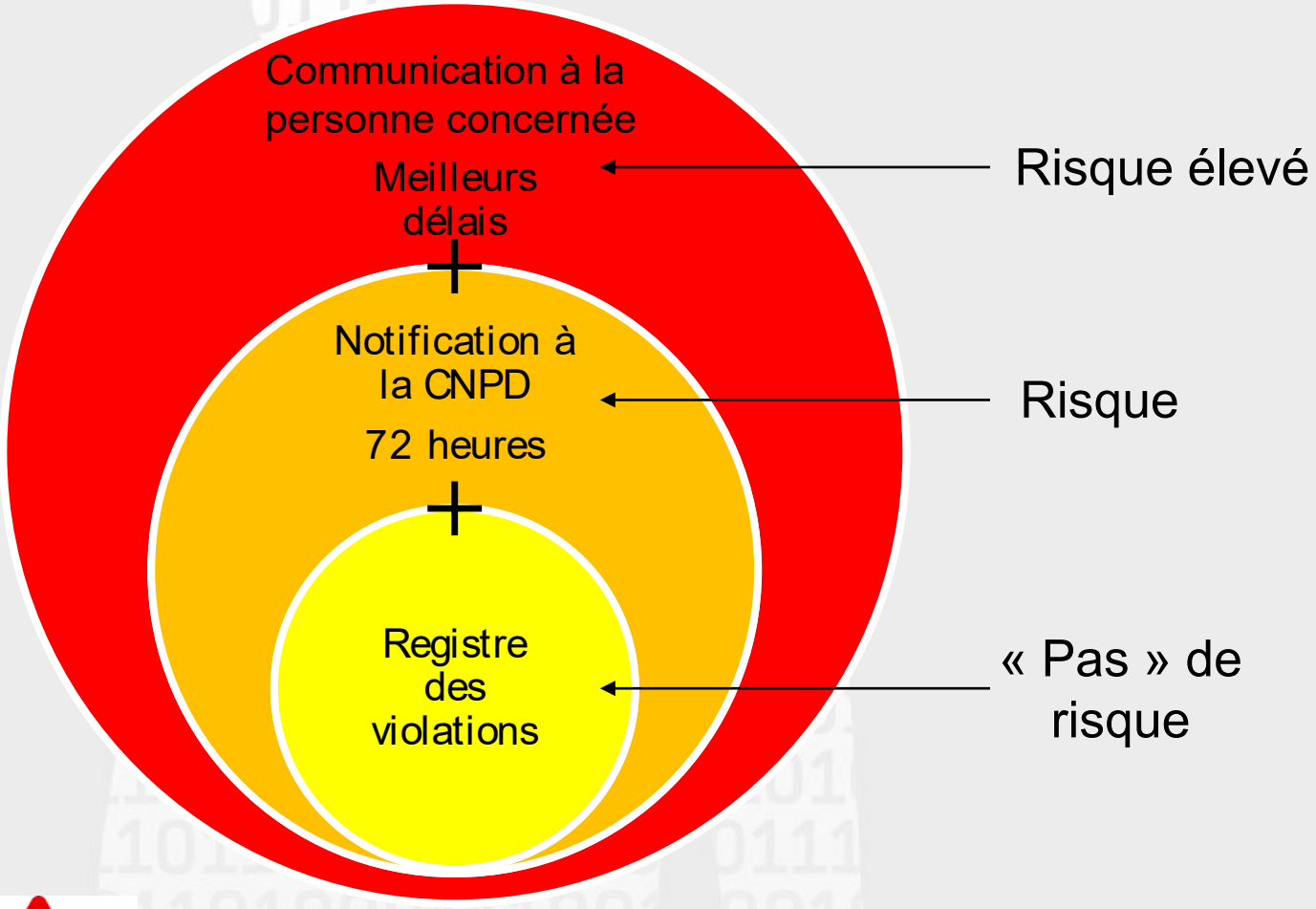
Illustratif

@ CNPD & LIST

3. Sécurité et notification de violations de données

- Mesures techniques et organisationelles selon :
  - “ l’état de l’art”
  - le risque pour les personnes concernées
- Mesures pour traiter les risques doivent être adaptées au contexte et aux spécificités du domaine concerné :
  - Analyse des risques en fonction de la nature des données, de prescriptions légales, de la complexité du système, etc.
- Mesures doivent être régulièrement mises à jour / adaptées :
  - Nouvelles menaces tous les jours
  - Nouvelles vulnérabilités découvertes
  - Changement du contexte de l'organisation → nouveaux risques

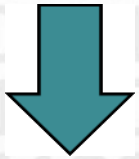
3. Sécurité et notification de violations de données



Obligation du sous-traitant de notifier au responsable du traitement toute violation de données dans les meilleurs délais après en avoir pris connaissance

4. Analyse d'impact

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***)

p.ex. service de location vélos avec géolocalisation

4. Analyse d'impact

Les critères suivants doivent être pris en compte pour déterminer la nécessité d'une analyse d'impact:

- Évaluation ou notation, y compris le profilage
- Décision individuelle automatisée avec effet juridique ou effet similaire significatif
- Surveillance systématique des personnes concernées
- Données sensibles ou données à caractère hautement personnel
- Données traitées à grande échelle
- Croisement ou combinaison d'ensembles de données
- Données concernant des personnes vulnérables
- Utilisation innovante ou application de nouvelles solutions technologiques ou organisationnelles
- Traitements qui empêchent les personnes concernées d'exercer un droit ou de bénéficier d'un service ou d'un contrat

5. Délégué à la protection des données

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.

5. Délégué à la protection des données

Pilote à bord!

Atout majeur pour: respecter les obligations du RGPD, dialoguer avec les autorités de contrôle, réduire les risques de contentieux

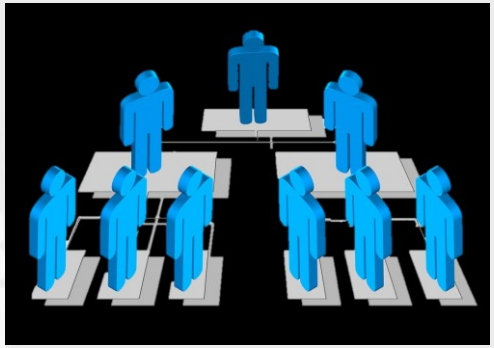
6. Sous-traitance

- Le responsable du traitement doit :
  - Choisir un sous-traitant adéquat et toujours garder le contrôle de la sous-traitance
  - Maîtriser la sous-traitance en cascade
  - Conclure avec chaque sous-traitant un **contrat écrit** prévoyant, entre autres, que:

- le sous-traitant ne traite les données que sur instruction documentée du responsable du traitement
- les obligations du responsable du traitement (p.ex. en matière de mesures de sécurité, confidentialité) incombent également au sous-traitant
- le sous-traitant doit assister le responsable du traitement (p.ex. droits des PC, violations de données)

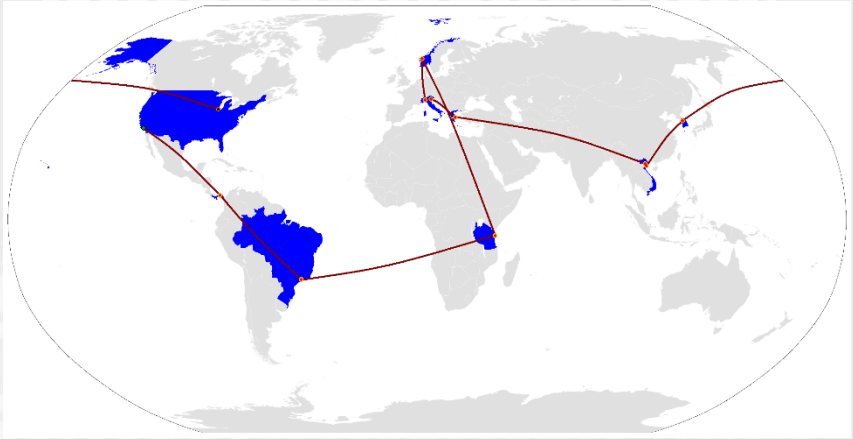
6. Sous-traitance

- Obligations des sous-traitants
  - Le sous-traitant ne traite les données que sur instruction documentée du responsable du traitement
    - Respect du contrat conclu avec le responsable du traitement
    - Si un sous-traitant détermine les finalités et les moyens du traitement, il devient le responsable du traitement
  - Sous-traitance en cascade
  - Mesures de sécurité
  - DPO
  - Registre
  - Transfert de données vers des pays tiers
  - Notification violations des données
  - Coopération avec la CNPD



7. Transferts pays tiers

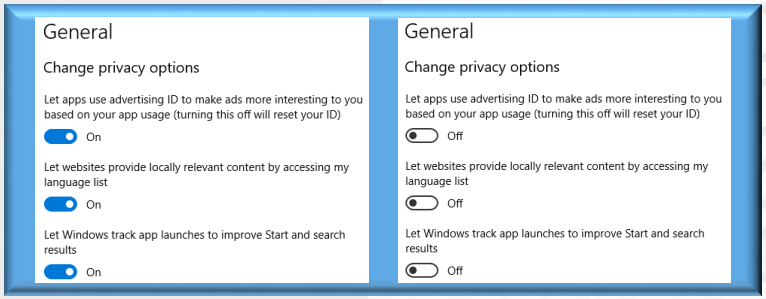
- Libre circulation des données au sein de l'UE/EEE
- Transferts de données vers des pays tiers (= en dehors de l'UE) uniquement possibles si:
  - Décision d'adéquation
  - Garanties appropriées (p.ex. BCR ou clauses contractuelles types, etc.)
  - Dérogations pour transferts spécifiques (p.ex. consentement, contrat, etc.)



8. Droits des personnes concernées

9. Gouvernance interne

- Créer une **culture globale** de la protection des données
- Implémenter la protection des données **dès la conception et par défaut**



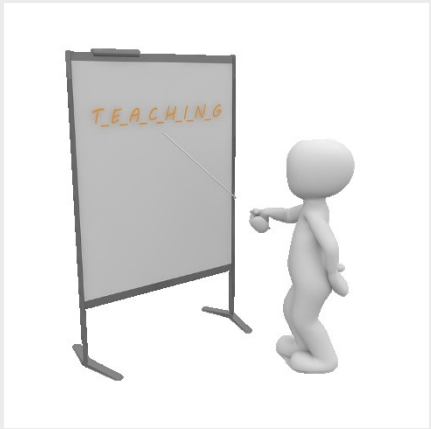
(*Privacy by design*)

(*Privacy by default*)

- **Anticiper** dès le départ les risques et problèmes
- Etre prêt à réagir en cas de **violations de données**
- Développer une gestion sécurisée de l'information **tout le long du cycle de vie** des traitements de données

9. Gouvernance interne

- **Sensibiliser** vos collaborateurs
- **Organiser** des procédures internes (ex. internal reporting)



- Mettre en place des procédure pour traiter les **réclamations** e les demandes des personne concernées quant à **l'exercic de leurs droits**
- **Informer les PC en tout transparence** sur l'ensemble d leurs droits

9. Gouvernance interne

- **Documenter la conformité**
  - Registre des traitements,
  - DPIA,
  - Encadrement des transferts de données hors de l'UE,
  - Registre des violations,
  - Contrats avec sous-traitants,
  - ...
- **Obligation de coopération avec la CNPD**