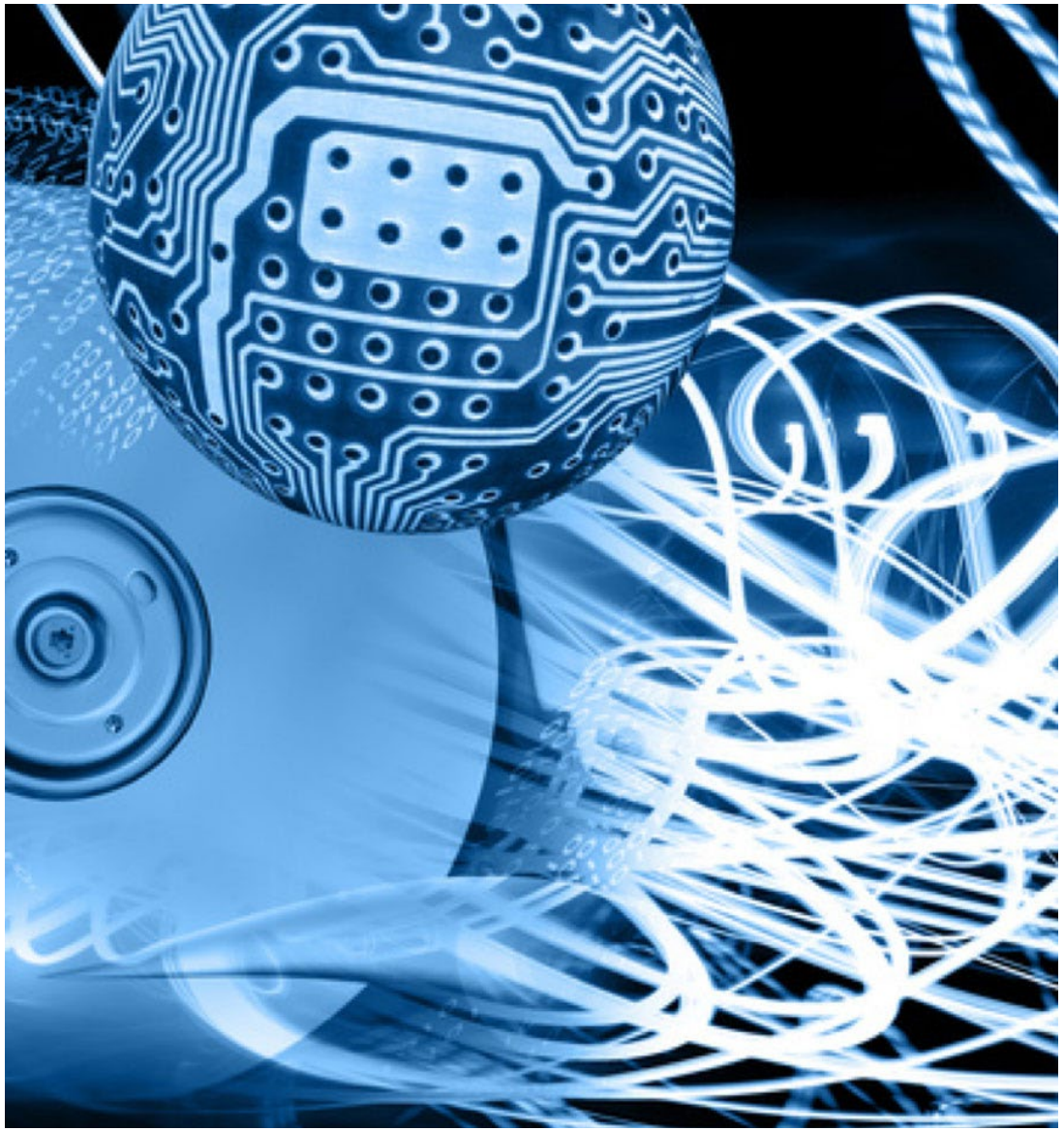
Mesures à prendre pour l'entreprise

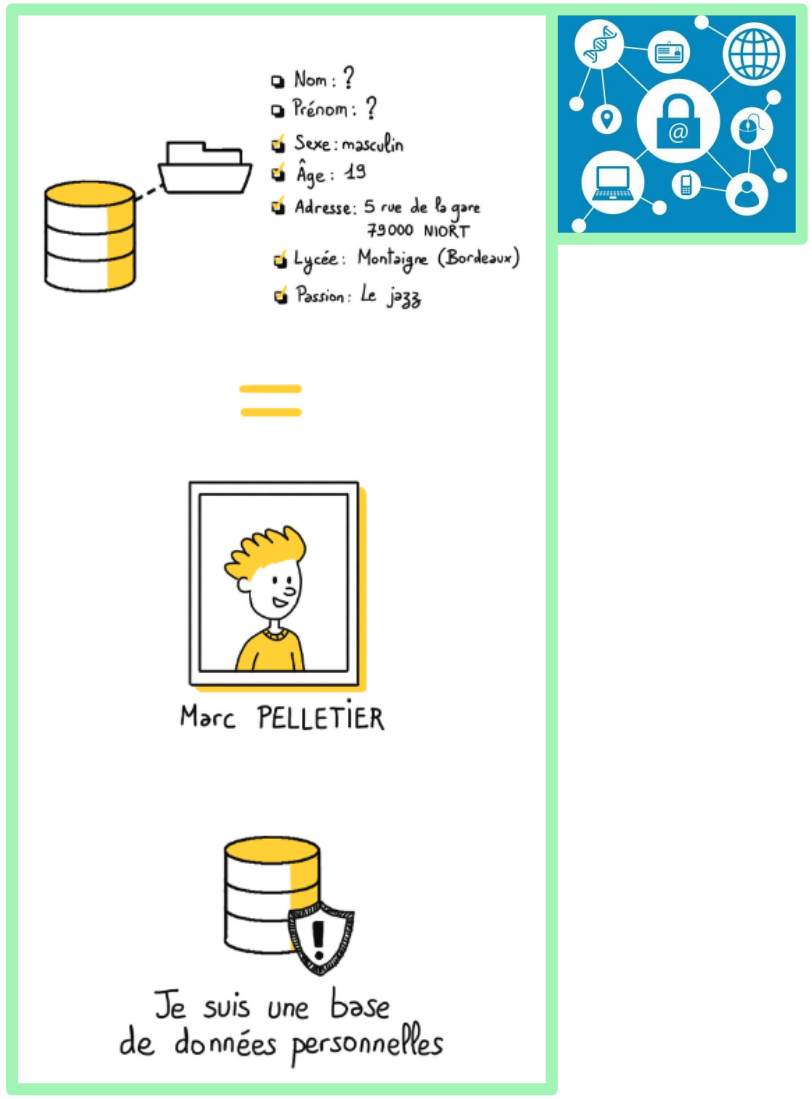
Axel DAGNAUD
Noah DE GUNST
Quentin RICROS
Victor CHASSÉ

1 General Data Protection Regulation (GDPR)

Les choses à savoir

1. **Qu’est-ce qu’une donnée personnelle ?**
2. **Qu'est-ce qu'une donnée sensible ?**
3. **Qu'est-ce que le DPO**
4. **Responsable de traitement et sous-traitants**





1) Qu'est-ce qu'une donnée personnelle ?

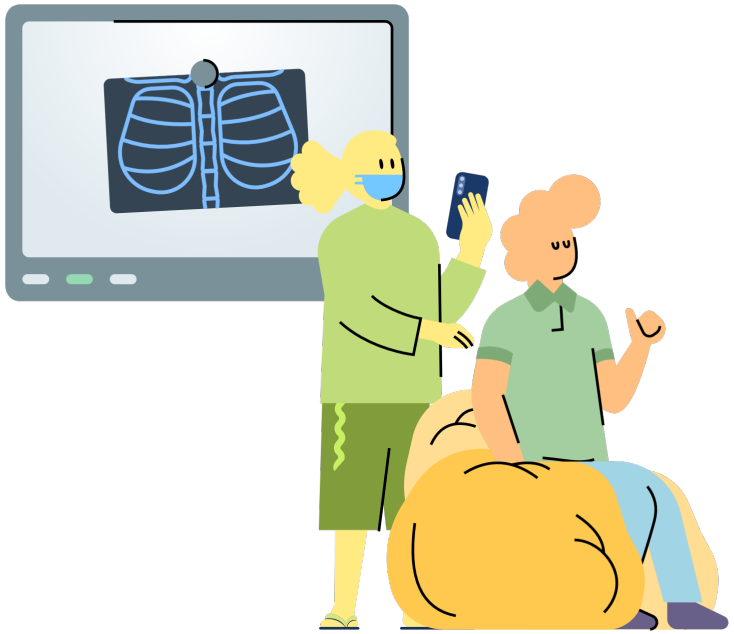
Elle identifie une personne de manière directe ou indirecte

Directement :

- Nom
- Prénom
- Date de naissance
- Adresse
- Numéro de passeport

Indirectement :

- Numéro de client
- Numéro de téléphone
- Données biométriques (empreintes digitales)
- Données de comportement en ligne (historique de navigation, cookies)
- Données de santé
- Voix



2) Qu'est-ce qu'une donnée sensible ?

Donnée qui touche à la vie personnelle ou privé et qui peuvent amener la discrimination des individus

Liste :

- Données de santé
- Origine raciale ou ethnique
- Opinions politiques
- Convictions religieuses ou philosophiques
- Appartenance syndicale
- Données génétiques
- Données biométriques
- Vie sexuelle

3) Le DPO ou DPD

DPO (Data Protection Officer)

DPD (Délégué à la Protection des Données)

« Avec une fonction située au cœur de la conformité au règlement européen sur la protection des données (RGPD), le délégué à la protection des données (DPO) conseille et accompagne les organismes qui le désignent. »
(source : CNIL)

4) Responsable de traitement et sous-traitants

Responsable de Traitement:

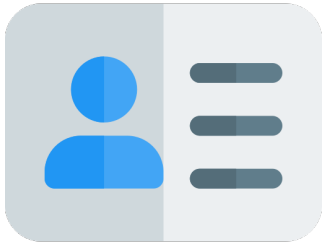
- Collecte et gère les données personnelles
- Responsable de la conformité au RGPD
- Notifie les violations de données
- Coupable si violation du RGPD

Sous-traitants:

- Traite les données pour le compte du Responsable de Traitement
- Doivent suivre les instructions du Responsable de Traitement
- Contrats nécessaires pour assurer la conformité et définir leurs responsabilités

Mise en place concrète du RGPD

Données relatives à l'identité



Coordonnées des employés

- Nom, prénom, photographie, date de naissance, nationalité, type de permis de conduire…

-> Ces données sont autorisées car nécessaires au fonctionnement de l'entreprise

Données dont la finalité est à expliciter

- Nombre d'enfants
- Profession des parents ou conjoints
- Situation matrimoniale
- Enfants à charges
- Nature

-> Il faut donner la finalité du traitement des données

Données relatives à la situation professionnelle

- Lieu de travail
- Numéro d'identification interne
- Date d'entrée dans l'entreprise
- Ancienneté (pour les augmentations)
- Emploi occupé et coefficient hiérarchique (pour les fiches de paye)
- Section comptable (pour la gestion de l'entreprise)
- Nature du contrat de travail
- Taux d'invalidité
- Reconnaissance de la qualité de travailleur handicapé (RQTH)

-> Ces données sont impératives au fonctionnement de l'entreprise

Les employés étrangers et les personnes à contacter

- Pour les employés étrangers, soit l'autorisation de travail, soit le titre de séjour suffit. Selon le principe de proportionnalité du RGPD, la structure ne nécessite qu'un des deux documents.
- Les coordonnées des personnes à prévenir en cas d'urgence sont importantes en cas d'accident de travail par exemple.

Gestion de la carrière des employés

Le recrutement

- Date et conditions de recrutement **->** limiter la durée de conservation pour les employés et les candidats (2 ans max)
- Désiderata de l'employé **->** assure l'évolution des employés
- Sanctions disciplinaires -> encadre les employés

Données dont la finalité est à expliciter

- Simulation de carrière -> éviter la discrimination des employés

Evaluation professionnelle de l'employé

Les données à garder

- Dates des entretiens d'évaluation
- Identité de l'évaluateur
- Compétences de l'employé
- Objectifs, résultats et appréciations

Les Données à supprimer

- Appartenance à un syndicat -> donnée sensible selon la CNIL
- Nombre de jours de grève -> donnée sensible selon la CNIL

Suivi administratif des visites médicales

Les données à garder

- Dates des visites **->** uniquement si c'est une visite au médecin de travail
- Aptitude au poste de travail **->** L'entreprise étant industrielle, l'employé ne doit pas avoir d'allergies aux produits utilisés par exemple

Données à supprimer

- Les pathologies des employés **->** donnée sensible

Il est important de savoir que la structure ne doit en aucun cas avoir accès aux données médicales mais uniquement l'avis du médecin

Définition du Registre des Activités de Traitement

Il répertorie toutes les activités de traitement des données à caractère personnel effectuées par une organisation

Contenu :

- Les traitements non occasionnels (exemple : gestion de la paie, gestion des clients/prospects et des fournisseurs, etc.)
- Les traitements susceptibles de comporter un risque pour les droits et libertés des personnes (exemple : systèmes de géolocalisation, de vidéosurveillance, etc.)
- Les traitements qui portent sur des données sensibles
- Le caractère des données traitées (nom, adresse...)

Si l'entreprise dépasse les 250 employés dans le futur, d'autres traitements doivent être mentionnés

Exemple de fiche de registre

Description du traitement	
Nom du traitement	Gestion de la paie
N° / RÉF	1 - Exemple
Date de création du traitement	26/05/2018
Mise à jour du traitement	13/05/2019

Acteurs	Nom	Adresse	Code Postal	Ville	Pays	Téléphone	Adresse mél
Responsable du traitement	Louise DUPONT	1 rue Rivoli	75001	Paris	France	01 xx xx xx xx	exemple1@ets.com
Délégué à la protection des données	Martin HENRI	1 rue Rivoli	75001	Paris	France	01 xx xx xx xx	exemple2@ets.com
Société du DPO (si celui-ci est externe)	N/A						

Finalité(s) du traitement effectué	
Finalité principale	Gestion de la paie
Sous-finalité 1	Calcul des rémunérations
Sous-finalité 2	Calcul du montant des versements adressés aux organismes sociaux
Sous-finalité 3	Ordre de virement à la banque

Catégories de données personnelles concernées	Description	Durée de conservation
État civil, identité, données d'identification, images...	Noms, prénoms, adresses	5 ans à compter du versement de la paie
Informations d'ordre économique et financier (revenus, situation financière, situation fiscale, etc.)	RIB	5 ans à compter du versement de la paie
Numéro de Sécurité Sociale (ou NIR)	Numéros de sécurité sociale des salariés	5 ans à compter du versement de la paie

Une fois les traitements listés, il faut saisir les différentes informations dans une fiche de registre qui permet à la CNIL de contrôler la conformité des traitements par rapport au RGPD.

Consentement et transparence

Obtention du consentement

Mettre en place un processus pour recueillir le consentement explicite des employés concernant le traitement de leurs données personnelles. Cela peut se faire en intégrant une case à cocher dans les formulaires d'embauche ou de gestion des données.

Politique de confidentialité

Rédiger une politique de confidentialité accessible et compréhensible qui détaille quelles données sont collectées (par exemple, nom, prénom, date de naissance, données professionnelles), dans quel but (gestion des ressources humaines, évaluation professionnelle, gestion médicale), combien de temps elles sont conservées, et les droits des employés en matière de protection des données.

Conservation des Données

- Durée nécessaire à la réalisation de l'objectif du traitement
- Les services opérationnels, comme les ressources humaines, auront un accès direct aux données.

Par exemple, dans une entreprise, les données d'un candidat non retenu seront conservées pendant 2 ans maximum

- Données conservées pour des raisons administratives ou légales.
- Accès limité, autorisation requise pour consultations spécifiques.

Par exemple, les données de facturation doivent être conservées dix ans en application du Code de commerce, même si la personne concernée n'est plus cliente

- Certaines informations sont archivées de manière permanente en raison de leur valeur.
- Accès limité, autorisation requise pour consultations spécifiques.

Par exemple, les documents historiques d'entreprise (création, contrats majeurs, décisions stratégiques)

Conclusion : Pour chaque type de données, fixez des délais de conservation adaptés à leur utilité, par exemple, les données de facturation peuvent être conservées pendant un certain temps après la fin de l'emploi, tandis que d'autres données moins cruciales peuvent être supprimées plus tôt pour rester en conformité avec la loi.

Voir recommandations CNIL : https://www.cnil.fr/fr/les-durees-de-conservation-des-donnees

Nomination du DPO

Vérifier la nécessité de nommer un DPO

*L'entreprise comptant une **centaine** de salariés, on vérifiera en fonction de la nature des opérations de celle-ci*

La nomination du DPO est obligatoire :

- si l'entreprise traitent de données sensibles à grande échelle
- si l'entreprise a une activité qui exige un suivi régulier et systématique à grande échelle des personnes concernées

Voir la désignation du DPO émis par la CNIL (https://www.cnil.fr/fr/designation-dpo)

Statut, compétences et moyens du DPO

Compétences requises

- Connaître les fondements du RGPD
- Être au fait des réglementations spécifiques du secteur industriel
- Pouvoir garantir la sécurité des systèmes d'informations

Moyens suffisants

- Disposer d'un temps suffisant pour exercer ses missions
- Bénéficier de moyens matériels et humains adéquats
- Accéder aux informations utiles
- Être associé en amont aux projets impliquant des données personnelles
- Être facilement joignable

Agir en toute indépendance

- Pouvoir rendre compte de son action au plus haut niveau de la direction de l'entreprise
- Pas être en conflit d'intérêt avec sa fonction de DPO et une potentielle autre fonction
- Pas être sanctionné pour l'exercice de ses missions
- Pas recevoir d'instruction dans le cadre de l'exercice de ses missions

Comment protéger les données

- ✓ **Chiffrer les données** : Le chiffrement garantit que les données ne sont accessibles que par des **personnes autorisées**. En cybersécurité, le chiffrement désigne la conversion des données depuis un format lisible dans un **format codé**. Les données chiffrées ne **peuvent être lues** ou traitées qu'après leur **déchiffrement.**
- ✓ **Formez le personnel** du service des ressources humaines aux bonnes pratiques de sécurité, telles que la **création de mots de passe forts**, l'utilisation d'authentification à deux facteurs, et la protection contre les logiciels malveillants.
- ✓ Ne laissez pas votre personnel connecter des **espaces de stockage amovibles** sans en connaître l'origine
- ✓ Incitez votre personnel de **changer de mot passe régulièrement**

Comment générer un mot de passe fort 💪

2 Le mot de passe

JsuédSdD&j'a18a

Est associé à la phrase :

> Je suis un éléve de Sciences des Données & j'ai 18 ans

Pour retrouver votre mot de passe :

1. Mémoriser la phrase choisie avec les majuscules, les nombres et la ponctuation.
2. Prendre les premières lettres de chaque mot, garder les nombres et la ponctuation.

Source : https://www.cnil.fr/fr/generer-un-mot-de-passe-solide

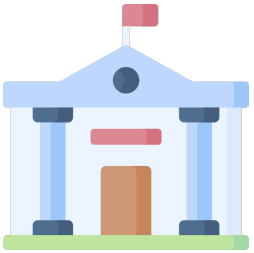
Que faire en cas de violation de données

✓ **Élaborer un plan de gestion des violations** de données qui détaille comment les violations seront signalées aux autorités de contrôle, comment les employés seront informés, et quelles **mesures correctives** seront prises pour prévenir de futures violations.

Les violations doivent être enregistrées dans un registre et contenir les informations suivantes:

- la nature de la violation
- les catégories et le nombre approximatif des personnes concernées
- les catégories et le nombre approximatif d'enregistrements concernés
- les conséquences probables de la violation
- les mesures prises pour remédier à la violation et, le cas échéant, pour limiter les conséquences négatives de la violation ;
- le cas échéant, la justification de l’absence de notification auprès de la CNIL ou d’information aux personnes concernées.

Que faire en cas de violation de données



Une notification doit être transmise à la CNIL dans les meilleurs délais à la suite de la constatation d'une violation présentant un risque pour les droits et libertés des personnes.

Si vous ne pouvez pas fournir toutes les informations requises dans les meilleurs delai car des investigations complémentaires sont nécessaires, vous pouvez procéder à une notification en deux temps :

- Une notification initiale dans un délai de 72 heures si possible à la suite de la constatation de la violation ;
- Si le délai de 72 heures est dépassé, vous devrez expliquer, lors de votre notification, les motifs du retard ;
- Enfin, une notification complémentaire dès lors que les informations complémentaires sont disponibles.

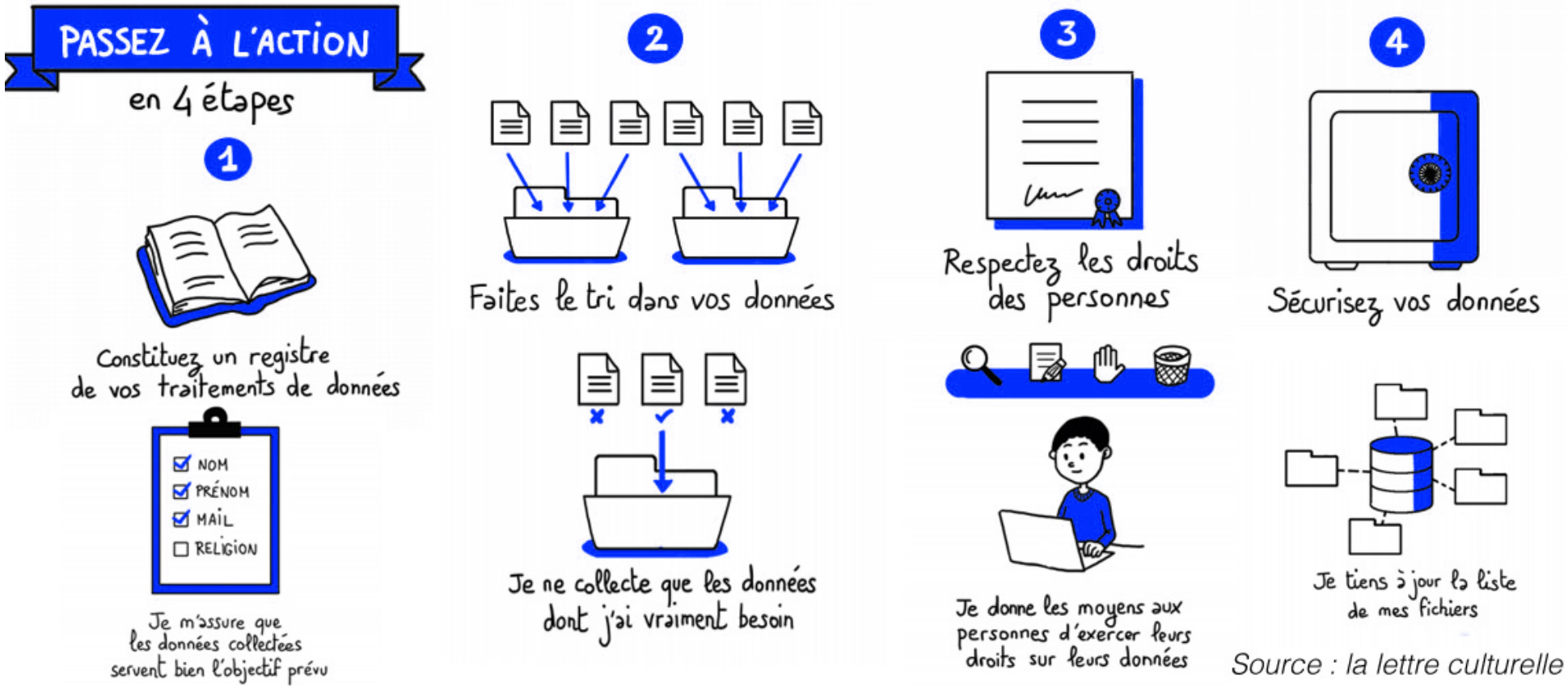
Travailler avec un sous-traitant

Les sous-traitants, comme les responsables de traitement, doivent respecter le RGPD

Ils doivent :

- Déterminer le **statut** des acteurs impliqués
- Établir un **contrat** clair
- **Documenter** l'activité de sous-traitance
- Proposer des outils **respectueux** des données personnelles
- **Garantir** la sécurité des données collectées

En résumé :



Source : *la lettre culturelle*