TP1 Comment mettre en place ces 6 mesures ?

La désignation d’un délégué à la protection des données

1. **Qui peut être délégué ?**

Le **DPO (Délégué à la Protection des Données)** peut être :

- **Un salarié interne** à l’organisme (ex. juriste, responsable conformité, RSSI, etc.),
- **Ou une personne externe** (consultant, cabinet spécialisé, groupement mutualisé).

Le DPO doit :

- Posséder **une expertise juridique, technique et organisationnelle** en matière de protection des données,
- Être **indépendant**,
- **Ne pas avoir de conflit d’intérêts** (il ne doit pas être juge et partie, ex. responsable IT ou RH sans précaution).

2. **Quels sont les rôles du délégué ?**

Le DPO est le **chef d’orchestre de la conformité RGPD**. Ses principales missions sont définies à l’article 39 du RGPD :

Mission principale	Description
Informer et conseiller	Le responsable du traitement, les sous-traitants et les employés.
Contrôler la conformité	Vérifier la mise en œuvre du RGPD et des politiques internes.
Sensibiliser et former	Organiser des sessions de formation auprès du personnel.
Conseiller sur les AIPD (analyses d’impact)	Aider à identifier et évaluer les risques sur la vie privée.
Coopérer avec la CNIL	Être le point de contact privilégié de l’autorité de contrôle.
Tenir un registre et documenter la conformité	Maintenir à jour la cartographie et les registres de traitement.

> Le DPO est à la fois **conseiller**, **vigie** et **interface** entre l’organisation, les personnes concernées et la CNIL.

3. **Est-il toujours obligatoire d’élire un délégué ? Existe-t-il des cas particuliers ?**

Non, pas toujours. Le **DPO est obligatoire** uniquement dans les cas suivants (article 37 du RGPD) :

Cas	Exemple
Autorité publique ou organisme public	Collectivités, écoles, hôpitaux, administrations
Activité principale = surveillance régulière et systématique à grande échelle	Réseaux sociaux, géolocalisation, caméras, marketing comportemental
Traitement à grande échelle de données sensibles ou judiciaires	Données de santé, opinions politiques, casiers judiciaires

Pour les autres structures (TPE/PME, associations), il est **fortement recommandé** mais non obligatoire.

4. **Comment devenir délégué à la protection des données ?**

Aucune formation obligatoire n’est imposée par la loi, mais le DPO doit avoir :

- Une **bonne maîtrise du RGPD et de la loi Informatique et Libertés**,
- Des **compétences juridiques**, informatiques et organisationnelles,
- Une **capacité à dialoguer avec les différents services**.

> Il est possible de suivre des **formations spécialisées certifiantes**, reconnues par la CNIL.

5. **Quelles sont les étapes de désignation d’un DPO ?**

1. **Décision interne** de nommer un DPO (et définition de son périmètre d’action).
2. **Rédaction d’un acte de désignation** (contrat ou lettre de mission).
3. **Déclaration officielle à la CNIL** via le formulaire en ligne (service.cnil.fr/dpo).
4. **Communication interne** : informer les salariés, les partenaires, les clients.
5. **Mise en place des outils** (registre, plan de conformité, procédures internes).

> Le DPO peut couvrir **plusieurs entités** d’un même groupe ou d’un groupement (mutualisation possible).

6. **Comment se passe la fin de mission d’un DPO ?**

La fin de mission intervient en cas de :

- Fin de contrat / mission,

- Changement de poste ou départ,
- Remplacement par un autre DPO.

L'organisme doit :

- **Informer la CNIL** du changement,
- **Garantir la continuité** de la fonction (désignation d'un remplaçant),
- **Assurer la transmission des dossiers** et de la documentation RGPD.

---

7. **Quel est le statut du DPO ?**

Le DPO a un **statut particulier d'indépendance** (articles 38 et 39 du RGPD) :

- Il **ne reçoit aucune instruction** concernant l'exercice de ses missions.
- Il **ne peut pas être sanctionné ou licencié** pour avoir exercé son rôle.
- Il **rend compte directement à la direction** ou au plus haut niveau hiérarchique.
- Il doit **disposer des moyens nécessaires** (temps, budget, accès à l'information).

> Ce statut est essentiel pour garantir son **impartialité et son efficacité**.

---

8. **Chaque organisme doit-il avoir un délégué différent ?**

Pas forcément.

- Un **DPO peut être commun à plusieurs organismes** (ex. un DPO mutualisé pour plusieurs mairies, ou pour les sociétés d'un même groupe).
- À condition que :
  - le DPO soit **facilement joignable** pour chaque entité,
  - et qu'il dispose **des moyens nécessaires** pour accomplir sa mission.

---

9. **Quels sont les moyens d'action du délégué ?**

Le DPO doit disposer :

- D'un **accès direct** aux responsables et aux informations internes,
- De la **possibilité d'auditer** les services et les traitements,
- Du **temps nécessaire** à l'exercice de sa mission,
- De **ressources humaines et techniques** suffisantes,
- Du **soutien de la direction**,
- Et de la **liberté d'expression** auprès de la CNIL et des personnes concernées.

---

10. **Existe-t-il des certifications de compétences pour les DPO ?**

Oui La **CNIL a mis en place un référentiel de certification** pour les compétences du DPO (2018). Cette certification n'est **pas obligatoire**, mais **hautement valorisée**.

Elle atteste que le DPO :

- connaît le cadre juridique,
- sait piloter la conformité,
- peut sensibiliser, conseiller et contrôler efficacement.

---

11. **Quels organismes sont agréés pour dispenser ces formations ?**

La **CNIL n'organise pas elle-même les formations**, mais elle **agrée des organismes certificateurs**. Ces organismes peuvent **délivrer la certification officielle "Compétences du DPO"**.

Quelques exemples d'organismes agréés (liste officielle sur le site de la CNIL) :

- **AFNOR Certification**,
- **Bureau Veritas Certification**,
- **CNPP Cert.**,
- **LSTI**,
- **DEKRA Certification**,
- **ISQ-OPQF** (pour la qualité de la formation).

> Les organismes de formation (ex. CNFPT, EFE, CNAM, ICPF, DPO Consulting, etc.) s'appuient souvent sur ces certificateurs agréés.

Cartographier vos traitements de données personnelles

1. Les recensements précis à effectuer

Le recensement consiste à **identifier et décrire tous les traitements de données personnelles** réalisés dans l'organisme. Cela suppose de **collecter des informations précises** sur :

- Les **activités métiers** qui manipulent des données personnelles.
- Les **données collectées** (type, origine, finalité).
- Les **personnes concernées** (clients, salariés, usagers, partenaires…).
- Les **supports utilisés** (logiciels, formulaires, bases de données…).
- Les **destinataires** des données (internes, sous-traitants, partenaires).
- Les **durées de conservation**.
- Les **mesures de sécurité** mises en place.

Le DPO recense cela via des **entretiens, questionnaires, audits ou observations**.

---

2. Les différents traitements pouvant être effectués

Un *traitement* est **toute opération sur une donnée personnelle**, automatisée ou non. Exemples de traitements :

Domaine	Exemple de traitement
Ressources humaines	Gestion du personnel, paie, recrutement, formation
Commercial / Marketing	Gestion clients, prospection, fidélisation
Sécurité	Vidéosurveillance, contrôle d’accès
Informatique	Gestion des comptes utilisateurs, sauvegardes
Administratif	Gestion des courriers, comptabilité
Communication	Gestion du site web, réseaux sociaux

> Même une simple **collecte ou conservation** de données constitue déjà un *traitement*.

---

3. Les différentes catégories de données personnelles

Le RGPD distingue plusieurs **catégories de données** :

Catégorie	Exemples	Particularités
Données d’identification	nom, prénom, adresse, n° téléphone, email	Données classiques
Données de contact professionnel	poste, service, email pro	Utilisées pour échanges pro
Données économiques	RIB, revenus, factures	Sensibles en cas de fuite
Données de connexion	IP, logs, cookies	Traitées souvent sur les sites web
Données sensibles (art. 9 RGPD)	santé, opinions, religion, syndicat, biométrie, orientation sexuelle	Interdiction sauf exceptions
Données judiciaires	infractions, condamnations	Très encadrées
Données de localisation	GPS, badge, smartphone	Nécessitent une base légale forte

---

4. Les objectifs de la cartographie

La **cartographie des traitements** vise à :

1. **Connaître précisément** les données traitées par l’organisme.
2. **Prouver la conformité RGPD** (principe d’« accountability »).
3. **Identifier les risques** pour les personnes concernées.
4. **Mettre en place les mesures de sécurité adaptées**.
5. **Construire et tenir à jour le registre des traitements** (obligatoire selon l’article 30 du RGPD).
6. **Sensibiliser les services** à la protection des données.

---

5. Les acteurs qui rentrent en jeu

Acteur	Rôle dans la cartographie
DPO	Pilote le projet, valide les fiches, conseille
Direction	Donne les moyens et la légitimité
Responsables de traitement	Définissent les finalités et moyens des traitements
Chefs de service / métiers	Décrivent leurs pratiques concrètes
DSI / RSI	Fournit les éléments techniques et mesures de sécurité
Sous-traitants	Fournissent des informations sur leurs propres traitements
CNIL (indirectement)	Peut contrôler la cohérence du registre

6. Les flux de données qui rentrent en jeu

Lors du recensement, il faut **cartographier les flux** :

- **Flux internes** : entre services (ex. RH → comptabilité).
- **Flux externes** : vers des partenaires, prestataires ou autorités (ex. banque, URSSAF, CNIL).
- **Flux internationaux** : transferts hors UE (nécessitent encadrement juridique spécifique).
- **Flux entrants** : collecte des données (formulaire, email, capteurs…).
- **Flux sortants** : diffusion ou suppression des données.

L'objectif est de **visualiser le "chemin" des données** de leur collecte jusqu'à leur suppression.

7. Le QQOCQP : la méthode d'analyse

Le **QQOCQP** (Qui ? Quoi ? Où ? Quand ? Comment ? Pourquoi ?) est un outil pratique pour décrire chaque traitement :

Élément	Question à poser	Exemple
Qui ?	Qui collecte / accède / décide ?	Service RH
Quoi ?	Quelles données sont collectées ?	Nom, CV, diplômes
Où ?	Où sont-elles stockées ?	Serveur interne ou cloud
Quand ?	Pendant combien de temps ?	2 ans après candidature
Comment ?	Par quel moyen ?	Formulaire en ligne
Pourquoi ?	Quelle finalité ?	Recruter un salarié

8. À quoi ressemble un registre de base ?

Le **registre des traitements** est souvent tenu sous forme de tableau Excel ou d'outil dédié. Voici un **exemple de structure simplifiée**

N°	Activité / traitement	Finalité	Base légale	Catégories de données	Personnes concernées	Destinataires	Durée de conservation	Sécurité	Trans hors
1	Gestion du personnel	Administration RH	Contrat / Obligation légale	Identité, paie, santé	Salariés	Comptable, organismes sociaux	5 ans	Accès restreint, mots de passe	Non
2	Gestion des clients	Exécution contrat	Contrat / Consentement	Coordonnées, factures	Clients	Service client, comptable	10 ans	Chiffrement, sauvegarde	Oui (serve US)

Prioriser les actions à mener

1. Les actions à mettre en place pour se conformer aux obligations

Une fois les traitements recensés, il faut engager un **plan de conformité RGPD**. Voici les principales actions à mener :

🔹 A. Gouvernance & organisation

- Désigner officiellement un **DPO** (si nécessaire) et définir son périmètre.
- Mettre en place une **politique de protection des données** interne.
- Définir des **rôles et responsabilités clairs** (responsable de traitement, sous-traitant, etc.).
- Former et sensibiliser les collaborateurs.

🔹 B. Documentation

- **Tenir à jour le registre des traitements** (art. 30 RGPD).
- Documenter les **bases légales** de chaque traitement (consentement, contrat, obligation légale…).
- Conserver les **preuves du consentement** lorsque c'est requis.
- Tenir un **registre des violations de données**.
- Mettre en place une **procédure de gestion des droits** (accès, rectification, effacement…).

🔹 C. Sécurité et gestion des risques

- Réaliser des **analyses d'impact (AIPD)** sur les traitements à risque.
- Mettre en œuvre des **mesures de sécurité techniques et organisationnelles** (authentification forte, chiffrement, sauvegardes…).
- Évaluer régulièrement les sous-traitants et leurs garanties RGPD.

🔹 D. Transparence et information

- Mettre à jour les **mentions d'information / politiques de confidentialité**.
- S'assurer de la **clarté et accessibilité** des documents pour les personnes concernées.
- Prévoir une **procédure de réponse aux demandes des personnes** (sous 1 mois max).

🔹 E. Supervision et amélioration continue

- Évaluer périodiquement la conformité.

- Suivre les évolutions réglementaires et les recommandations CNIL.
- Mettre à jour la documentation en cas de nouveau traitement.

2. **Les éléments de priorisation**

Le DPO doit prioriser les actions selon le **niveau de risque** et la **maturité de l'organisation** :

Critère de priorité	Exemple
Risque élevé pour les personnes	Données de santé, géolocalisation, données d'enfants
Volume important de données	Bases clients ou employés importantes
Multiplicité des traitements sensibles	Vidéosurveillance, biométrie
Absence de base légale claire	Collecte sans consentement
Sous-traitance à l'étranger	Transferts hors UE
Manque de sécurité manifeste	Mot de passe faible, pas de chiffrement

Priorité haute : traitements sensibles + absence de base légale + transferts non encadrés. **Priorité moyenne** : manques documentaires, information incomplète. **Priorité basse** : ajustements esthétiques ou non urgents.

3. **Les points d'attention sur lesquels travailler**

Quelques **zones sensibles** souvent relevées par la CNIL :

- Collecte excessive de données (« minimisation » non respectée).
- Absence de purge automatique des données périmées.
- Manque de preuve du consentement.
- Sécurité insuffisante (mots de passe, sauvegardes non chiffrées).
- Mentions légales trop vagues ou absentes.
- Sous-traitants non audités ni encadrés contractuellement.
- Absence de procédure en cas de violation de données.

4. **Les points d'attention particuliers**

Certaines **situations spécifiques** nécessitent une vigilance accrue :

Situation	Point d'attention particulier
Traitement de données sensibles	AIPD obligatoire, mesures renforcées
Transfert hors UE (ex : USA)	Encadrement juridique (clauses, Data Privacy Framework, BCR)
Mineurs	Consentement des parents, langage clair
Vidéosurveillance / contrôle d'accès	Information visible, durée limitée
Prospection commerciale	Consentement préalable (email/SMS)
RH / recrutement	Données limitées, conservation courte

5. **Les particularités de la sous-traitance**

La **sous-traitance** est un aspect clé du RGPD. Le **responsable du traitement** reste **juridiquement responsable**, mais doit encadrer la relation.

🔹 Obligations principales :

Obligation	Détail
Contrat écrit	Doit encadrer les traitements confiés (article 28 RGPD)
Clauses obligatoires	Objet, durée, finalités, sécurité, confidentialité, assistance au RT
Choix du sous-traitant	Doit offrir **des garanties suffisantes** de conformité
Autorisation préalable	Pour tout **sous-traitant ultérieur**
Coopération	Le sous-traitant aide à la gestion des droits, AIPD, violations
Notification des violations	Il doit **alerter le responsable du traitement sans délai**
Audit possible	Le responsable doit pouvoir contrôler le sous-traitant

> Exemple : hébergeur, prestataire de paie, cabinet comptable, éditeur SaaS, société de sécurité.

En résumé

Thème	Objectif principal	Actions clés

Thème	Objectif principal	Actions clés
Conformité	Respect du RGPD	Registre, base légale, sécurité
Priorisation	Gérer le risque	Traiter les traitements sensibles d'abord
Points d'attention	Éviter les non-conformités fréquentes	Sécurité, consentement, information
Sous-traitance	Encadrement contractuel	Clauses, contrôle, notification

Gérer les risques

1. **Qu'est-ce qu'un risque ?**

En matière de protection des données, un **risque** est la **possibilité qu'un événement affecte négativement les droits et libertés des personnes concernées**.

Autrement dit, ce n'est pas le risque pour l'entreprise, mais pour **l'individu** (le citoyen, le client, le salarié…).

🔹 Exemples de risques :

- Vol ou fuite de données personnelles (atteinte à la confidentialité).
- Erreur de saisie entraînant une mauvaise décision (atteinte à l'exactitude).
- Perte de données (atteinte à la disponibilité).
- Profilage abusif (atteinte à la vie privée ou aux libertés).

Objectif : **évaluer la probabilité** et **la gravité** de ces risques pour décider des mesures de protection adaptées.

2. **Qu'est-ce qu'une analyse d'impact (AIPD) ?**

Une **AIPD** (ou **PIA – Privacy Impact Assessment**) est une **étude de gestion des risques RGPD**. Elle consiste à :

1. **Décrire le traitement de données prévu**.
2. **Évaluer la nécessité et la proportionnalité** du traitement.
3. **Identifier les risques** sur les droits et libertés des personnes.
4. **Déterminer les mesures** permettant de réduire ces risques à un niveau acceptable.

L'AIPD est **obligatoire** pour les traitements **susceptibles d'engendrer un risque élevé** (article 35 du RGPD).

3. **Les piliers d'une AIPD**

Une AIPD repose sur **3 grands piliers** :

Pilier	Objectif	Exemple
Légitimité et proportionnalité du traitement	Vérifier que le traitement est justifié, limité et conforme au RGPD	Base légale, finalité claire, minimisation
Identification et évaluation des risques	Mesurer les impacts potentiels sur la vie privée des personnes	Vol de données, surveillance, erreur automatisée
Mesures de maîtrise des risques	Déterminer comment réduire ces risques	Chiffrement, anonymisation, limitation d'accès, formation

> L'AIPD est à la fois **juridique**, **technique** et **organisationnelle**.

4. **Quand réaliser une AIPD ?**

Une AIPD doit être réalisée **avant la mise en œuvre d'un traitement**, lorsque celui-ci présente un **risque élevé** pour les droits et libertés des personnes.

🔹 Exemples de traitements nécessitant une AIPD :

- Traitement de **données sensibles** (santé, biométrie…).
- **Surveillance systématique** d'une zone publique.
- **Profilage automatisé** ayant un effet juridique.
- **Croisement massif de données** provenant de sources différentes.
- **Traitements à grande échelle**.
- **Utilisation de nouvelles technologies** (IA, objets connectés…).

La **CNIL publie une liste officielle** de traitements pour lesquels une AIPD est obligatoire.

5. **Les 9 critères de définition du risque (selon la CNIL)**

La CNIL (et le G29, devenu CEPD) a défini **9 critères** permettant d'évaluer si un traitement présente un **risque élevé**. Si **au moins 2 critères** sont remplis, une AIPD est généralement requise.

N°	Critère	Exemple
1	Évaluation/scoring	Profilage de clients, notation de crédit

N°	Critère	Exemple
2	Décision automatisée ayant effet juridique	Refus automatique de prêt, recrutement automatisé
3	Surveillance systématique	Vidéosurveillance, tracking en ligne
4	Données sensibles ou hautement personnelles	Santé, opinions, religion, biométrie
5	Données traitées à grande échelle	Base clients nationale
6	Croisement ou combinaison de données	Fusion de bases RH et santé
7	Personnes vulnérables	Mineurs, patients, personnes âgées
8	Utilisation innovante ou technologique	IA, reconnaissance faciale
9	Exclusion d'un droit, d'un service ou d'un contrat	Refus d'emploi, d'assurance, d'accès

6. **Les personnes qui participent à l'élaboration d'une AIPD**

L'AIPD est un **travail collectif**, piloté par le **DPO** mais impliquant plusieurs acteurs :

Acteur	Rôle
Responsable du traitement	Décide du traitement, valide l'AIPD
DPO	Conseille, supervise, valide la méthodologie
Chef de projet / métier	Fournit la description du traitement
DSI / RSSI	Apporte les éléments techniques et de sécurité
Juridique / conformité	Vérifie la base légale et les clauses contractuelles
Sous-traitants	Décrivent leurs mesures de protection
Représentants du personnel / utilisateurs (si pertinent)	Donnent un retour sur les impacts concrets

> En cas de doute persistant sur la gravité du risque, le DPO peut consulter la **CNIL** avant le lancement du traitement.

7. **Qu'est-ce que le PIA ? Comment fonctionne-t-il ?**

Le **PIA** (*Privacy Impact Assessment*) est à la fois :

- le **nom anglais de l'AIPD**,
- et le **nom de l'outil logiciel gratuit** développé par la **CNIL** pour réaliser ces analyses.

🔹 Fonctionnement du logiciel **PIA CNIL** :

- Téléchargeable sur pia.cnil.fr.
- Permet de **structurer pas à pas** l'AIPD :
  1. Définition du contexte et du traitement.
  2. Évaluation de la légitimité et de la proportionnalité.
  3. Identification des risques.
  4. Évaluation du niveau de gravité et de probabilité.
  5. Proposition de mesures de réduction.
- Génère un **rapport complet au format PDF** conforme au RGPD.
- Peut être utilisé **en local ou en réseau** (multi-utilisateurs).

> C'est l'outil recommandé par la CNIL, très utile pour **standardiser et prouver la conformité**.

En résumé

Thème	Contenu clé
Risque	Possibilité d'atteinte aux droits des personnes
AIPD	Étude d'évaluation et de maîtrise des risques
Piliers	Légitimité – Risque – Mesures de maîtrise
Quand ?	Avant tout traitement à risque élevé
9 critères CNIL	Profilage, automatisation, surveillance, sensible, etc.
Acteurs	DPO, responsable, DSI, juridique, sous-traitants
Outil PIA	Logiciel CNIL pour piloter et documenter les AIPD

Organiser les processus internes, violations de données et demandes d'accès

1. **Qu'est-ce qu'un processus ?**

Un **processus** est une **suite d'activités coordonnées** visant à atteindre un objectif précis. Dans le contexte du RGPD, un processus décrit **comment les données sont collectées, traitées, conservées et sécurisées** tout au long de leur cycle de vie.

> Exemple : le processus de recrutement → collecte des CV → tri → entretien → décision → suppression.

2. **Quels processus doivent être mis en place lors de la collecte ?**

Lors de la collecte de données personnelles, l'organisme doit prévoir :

Étape	Processus à mettre en place
Avant la collecte	Vérification de la **base légale** (consentement, contrat, obligation légale…).
Au moment de la collecte	Information claire de la personne (mentions légales).
Après la collecte	Enregistrement dans le **registre des traitements**, **sécurisation** des données, limitation de la durée de conservation.
Gestion des droits	Procédure de **réponse aux demandes** (accès, rectification, suppression…).

i 3. **Quelles sont les informations à fournir lors de la collecte ?**

L'article **13 du RGPD** impose d'informer la personne **au moment de la collecte** :

Information à fournir	Exemple
Identité et coordonnées du responsable de traitement	« Société X – DPO : dpo@societe.com »
Finalités du traitement	« Gestion de votre commande »
Base légale	« Exécution d'un contrat »
Destinataires	« Service client, prestataire de livraison »
Durée de conservation	« 3 ans après le dernier contact »
Droits des personnes	Accès, rectification, suppression, opposition, portabilité
Droit d'introduire une réclamation	CNIL – www.cnil.fr
Caractère obligatoire ou facultatif des données	Ex. champ obligatoire = traitement impossible sinon
Existence de transferts hors UE	et leurs garanties éventuelles

> Ces mentions doivent être **claires, compréhensibles et facilement accessibles**.

4. **Qu'est-ce qu'une violation de données à caractère personnel ?**

Une **violation de données** est une **atteinte à la sécurité** entraînant, de manière accidentelle ou illicite :

- la **destruction**,
- la **perte**,
- la **modification**,
- la **divulgation non autorisée**,
- ou l'**accès non autorisé** à des données personnelles.

> Exemple : piratage, vol d'ordinateur, envoi d'un mail à la mauvaise personne, suppression accidentelle d'une base.

5. **Que doit-il se passer en cas de violation de données ?**

Dès qu'une violation est détectée :

1. **Identifier et qualifier la violation** (quelles données ? combien de personnes ? quel impact ?).
2. **Contenir et corriger** la faille (isoler les serveurs, réinitialiser les accès…).
3. **Évaluer le risque** pour les personnes concernées.
4. **Notifier la CNIL** si le risque est élevé (dans les 72 h).
5. **Informer les personnes concernées** si le risque est grave.
6. **Documenter l'incident** dans le registre interne des violations.

6. **Qu'est-ce qu'une notification ?**

La **notification** est la **déclaration officielle** faite à la **CNIL** (ou à toute autorité de contrôle compétente) lorsqu'une violation de données personnelles survient.

Elle permet à l'autorité :

- d'évaluer la gravité de la violation,
- de vérifier la réaction de l'organisme,
- et de proposer ou d'imposer des mesures correctives.

7. **Quels sont les délais légaux de notification ?**

- **72 heures maximum** après avoir pris connaissance de la violation (article 33 RGPD).
- Si la notification dépasse ce délai, il faut **justifier le retard**.
- En cas de **risque élevé pour les personnes**, celles-ci doivent être **informées sans délai**.

8. **Les 5 étapes d'une notification**

1. **Détection** : identification de l'incident.
2. **Qualification** : évaluation du risque pour les personnes.
3. **Notification à la CNIL** (via le formulaire en ligne).
4. **Information des personnes concernées** (si risque élevé).
5. **Documentation interne** de la violation et des mesures prises.

9. **Que va faire la CNIL après votre notification ?**

La CNIL peut :

- Accuser réception de la notification.
- Demander des **informations complémentaires**.
- Donner des **recommandations** ou imposer des **mesures correctives**.
- Ouvrir une **enquête** si la gravité le justifie.
- En cas de manquement, prononcer des **sanctions administratives** (amendes, injonctions…).

10. **L'obligation de notifier à l'autorité de contrôle peut-elle être confiée au sous-traitant ?**

Non

- Le **responsable du traitement** reste **l'unique responsable légal** de la notification.
- Le **sous-traitant**, lui, a **l'obligation d'informer sans délai** le responsable **dès qu'il prend connaissance** d'une violation.

C'est ensuite au responsable de décider s'il faut notifier la CNIL ou informer les personnes concernées.

11. **Les pouvoirs de la CNIL en matière de violation de données**

La CNIL peut :

- **Contrôler** les organismes concernés.
- **Ordonner la mise en conformité**.
- **Suspendre les transferts de données**.
- **Prononcer des sanctions pécuniaires** (jusqu'à 20 M€ ou 4 % du CA mondial).
- **Publier** les sanctions (nomination publique).

12. **Quelle est la plateforme nationale d'assistance aux victimes d'actes de cybermalveillance ?**

Cybermalveillance.gouv.fr Plateforme officielle française d'aide aux particuliers, entreprises et collectivités victimes de piratage, vol de données, hameçonnage, etc. Elle propose :

- une **aide en ligne personnalisée**,
- des **partenaires locaux** pour intervenir,
- et des **conseils de prévention**.

13. **Qu'est-ce qu'une demande de droit d'accès ?**

Le **droit d'accès** (article 15 RGPD) permet à toute personne :

- de **savoir si des données personnelles la concernant sont traitées**,
- et d'en **obtenir une copie**, avec des informations sur :
  - la finalité du traitement,
  - les catégories de données,
  - les destinataires,
  - la durée de conservation,
  - la source des données,
  - l'existence de transferts internationaux.

14. **Les 4 étapes de la demande d'un droit d'accès**

1. **Réception** de la demande (par mail, courrier, formulaire…).
2. **Vérification de l'identité** du demandeur.

3. **Recherche et extraction** des données concernées.
4. **Réponse au demandeur** dans un **délai d'un mois** (prolongeable à 2 mois si complexe).

---

15. **Peut-on refuser de répondre à une demande de droit d'accès ?**

Oui, **dans certains cas limités** :

- Demande **manifestement excessive ou répétitive**.
- Données impliquant des **droits de tiers** (protection d'autrui).
- Données couvertes par le **secret professionnel** ou **défense nationale**.
- Aucune donnée concernant la personne n'est détenue.

Le refus doit être **motivé par écrit** et **mentionner la possibilité de saisir la CNIL**.

---

16. **Qui peut exercer une demande de droit d'accès ?**

Toute **personne concernée** par un traitement de données :

- Un client, salarié, patient, usager, élève, etc.
- Un **représentant légal** (parent, tuteur) pour un mineur.
- Un **mandataire** (ex. avocat) dûment autorisé.

---

17. **Une justification d'identité doit-elle être obligatoirement demandée ?**

- Oui, **si le responsable du traitement a un doute raisonnable** sur l'identité du demandeur.
- Non, si la personne est déjà identifiée par des moyens fiables (ex. compte client sécurisé).

---

18. **Qu'est-ce qu'un "doute raisonnable" concernant la vérification d'identité ?**

C'est une **incertitude légitime** quant à l'identité réelle du demandeur. Exemples :

- Email reçu depuis une adresse inconnue.
- Absence d'éléments permettant de relier la demande à un compte connu.
- Demande portant sur des données sensibles.

Dans ce cas, l'organisme peut demander **une pièce d'identité**, uniquement pour vérifier l'identité.

---

19. **Quel est le coût d'une demande d'accès ?**

- **Gratuit** par principe.
- Sauf si la demande est **manifestement infondée ou excessive** : l'organisme peut alors exiger **des frais raisonnables** couvrant le coût administratif.

##📤 20. **Une fois la demande d'accès réalisée, de quelles manières les données peuvent-elles être communiquées ?**

- **Électroniquement** (format PDF, espace client, mail sécurisé).
- **Sur support papier** (copie imprimée).
- **Via un accès direct** à un espace sécurisé en ligne.

La réponse doit être **claire, compréhensible et complète**.

---

21. **Que faire lors d'une demande d'accès si la gestion des données personnelles est sous-traitée ?**

- Le **responsable du traitement** reste **seul responsable** de répondre à la demande.
- Le **sous-traitant** doit **coopérer** et **fournir les données nécessaires**, conformément au contrat RGPD (article 28).
- Le responsable consolide la réponse et la transmet à la personne concernée.

Documenter la conformité

1. **Qu'est-ce qu'un registre de traitement ?**

Le **registre des traitements** est un **document obligatoire** prévu à l'article **30 du RGPD**. Il recense **tous les traitements de données personnelles** effectués par un organisme (public ou privé).

Objectif :

- Avoir une **vue d'ensemble** des traitements,
- Identifier les **risques**,
- Permettre à la **CNIL** de vérifier la conformité,
- Servir de **base à la mise en conformité** (AIPD, sécurité, information, etc.).

> C'est un peu la « carte d'identité » de tous les traitements de données d'une organisation.

2. **Quels sont les éléments qui doivent apparaître dans ce registre ?**

Selon l'article 30 du RGPD, le registre doit contenir **au minimum** les informations suivantes 👇

Pour le **responsable du traitement** :

Élément	Description / Exemple
Nom et coordonnées du responsable	Société, organisme, DPO
Finalités du traitement	Ex. gestion du personnel, facturation, recrutement
Catégories de personnes concernées	Clients, salariés, usagers, élèves
Catégories de données traitées	Identité, contact, santé, données financières
Catégories de destinataires	Service RH, prestataire informatique, comptable
Transferts vers un pays tiers	Oui/Non + garanties (clauses types, BCR, etc.)
Durées de conservation	Exemple : 2 ans après la fin du contrat
Mesures de sécurité techniques et organisationnelles	Mots de passe forts, sauvegardes, contrôle d'accès
Base légale du traitement	Consentement, obligation légale, contrat, intérêt légitime…

Pour le **sous-traitant** :

Le registre doit comporter :

Élément	Description
Nom et coordonnées de chaque **responsable de traitement** pour lequel il agit	
Les **catégories de traitements réalisés**	
Les **transferts de données vers un pays tiers**	
Une **description des mesures de sécurité** mises en place	

3. **Quels sont les éléments qui doivent être documentés ?**

Le registre s'inscrit dans une démarche plus large de **documentation de la conformité RGPD**. Voici ce qui doit être **documenté** (et conservé à jour) :

Catégorie	Exemple de documents à conserver
Registre des traitements	Tous les traitements de données personnelles
Registre des violations	Historique des incidents et actions correctives
Mentions d'information	Textes fournis aux personnes (site web, formulaires…)
Consentements recueillis	Preuves du consentement (formulaires, logs, etc.)
Contrats de sous-traitance	Clauses RGPD article 28
Procédures internes	Sécurité, gestion des droits, conservation, suppression
Analyses d'impact (AIPD)	Évaluation des risques pour les traitements sensibles
Formations / sensibilisations	Preuves de formation du personnel
Politiques de confidentialité	Documents internes ou externes
Justifications de base légale	Contrat, texte législatif, intérêt légitime documenté

> Cette documentation permet de **démontrer la conformité** à la CNIL à tout moment (principe de *responsabilité proactive*).

4. **Un registre concernant les violations de données doit-il être tenu ?**

Oui, absolument. L'article **33 §5 du RGPD** impose à **tous les responsables de traitement** de **documenter chaque violation de données personnelles**, qu'elle soit ou non notifiée à la CNIL.

Ce registre des violations doit contenir :

Élément	Description
Date et nature de la violation	Ex. perte d'un ordinateur, piratage de messagerie
Catégories et volume de données concernées	500 clients, données de santé
Conséquences de la violation	Risque d'usurpation d'identité, divulgation d'informations

Élément	Description
Mesures correctives prises	Réinitialisation, alerte CNIL, formation interne
Décision de notification	Oui/Non + justification
Date de notification	Si applicable (CNIL / personnes concernées)

> Ce registre doit être **tenu à jour**, même pour les incidents mineurs, et présenté à la CNIL sur demande.

Exemple simplifié d'un **registre de traitement de base**

N°	Traitement	Finalité	Base légale	Données collectées	Personnes concernées	Durée conservation	Destinataires	Sécurité
1	Gestion RH	Suivi du personnel	Contrat	Nom, prénom, salaire, congés	Salariés	5 ans après départ	Service paie, expert-comptable	Accès restreint, sauvegardes
2	Gestion clients	Facturation, SAV	Contrat	Nom, adresse, email	Clients	3 ans	Service client, prestataire IT	VPN, mots de passe, logs
3	Newsletter	Prospection	Consentement	Email	Clients/prospects	Jusqu'au retrait du consentement	Service marketing	Mail sécurisé, opt-out automatique

"QUID de la mort numérique" (personne décédée)

1. **Qu'est-ce que la mort numérique ?**

La **mort numérique** désigne la situation où **les comptes, données et traces en ligne d'une personne continuent d'exister après son décès** :

- Emails, réseaux sociaux, photos, vidéos, documents stockés sur le cloud, comptes bancaires en ligne, etc.
- Ces données restent **sous la responsabilité des fournisseurs de services et héritiers**, mais **ne sont plus protégées par le consentement du défunt**, car la personne n'est plus là pour exercer ses droits.

2. **Cadre légal en France**

a) Droit français sur les données post-mortem

- La **loi Informatique et Libertés** (article 40 de la loi n°78-17 modifiée) prévoit que :

  > « Les droits des personnes sur leurs données personnelles s'éteignent au décès, sauf disposition contraire du défunt ou par la loi. »

- En pratique :
  - Les **héritiers ou représentants légaux** peuvent demander la suppression ou la transmission des données du défunt.
  - Les fournisseurs peuvent imposer **leurs propres procédures** (ex. Facebook : « compte commémoratif »).

b) RGPD et personnes décédées

- Le RGPD **ne s'applique pas directement aux personnes décédées**, car il protège les personnes vivantes.
- Toutefois, certaines **pratiques internes des organismes** incluent la gestion des comptes post-mortem pour respecter le droit à la vie privée et la réputation numérique.

3. **Que peuvent faire les héritiers ou proches ?**

Action	Exemple
Demander la suppression	Supprimer le compte Facebook ou Google du défunt
Obtenir l'accès aux données	Certains services (Google Inactive Account Manager, Apple Legacy Contact) permettent de transmettre des données à un héritier désigné
Demander la conservation ou commémoration	Facebook permet de transformer un compte en compte « commémoratif »

> Chaque plateforme a ses **procédures propres** et exige généralement :

- Certificat de décès,
- Pièce d'identité du demandeur,
- Lien de parenté ou preuve d'héritage.

4. **Bonnes pratiques pour gérer la mort numérique**

1. **Prévoir une clause dans le testament** ou un document écrit indiquant la gestion de vos comptes et données numériques.
2. **Lister les comptes importants** et les mots de passe dans un coffre sécurisé ou un gestionnaire de mots de passe partagé avec un héritier de confiance.
3. **Utiliser les outils de planification numérique** proposés par certains services :
   - Google : *Inactive Account Manager*,
   - Apple : *Legacy Contact*,
   - Facebook : *Contact de confiance*.
4. **Supprimer les comptes inactifs** pour réduire la « trace numérique ».

