Registre, DPO et violations de données

> **Référentiel BTS** — **BC4 / C4.7**. Voir aussi **BC3 / C3.6** « Se prémunir et réagir face aux incidents numériques ».

> **L'essentiel :** trois obligations concrètes pèsent sur la structure — **tenir un registre** de ses traitements, **désigner un DPO** lorsque c'est requis, et **documenter puis notifier** les violations de données.

Objectif

À la fin de cette page, vous savez :

- dire ce que contient un registre des traitements et comment le construire ;
- savoir quand un **DPO** est obligatoire et ce qu'il fait ;
- qualifier une **violation de données** et déclencher la bonne réaction.

1. Le registre des traitements

C'est la pièce maîtresse de la « responsabilité » : le document qui permet de **prouver** qu'on sait ce qu'on fait des données. Il est demandé en premier en cas de contrôle de la CNIL.

Une ligne par traitement. Pour un cabinet d'orthoprothèse, la liste tient en une dizaine de lignes :

Traitement	Finalité	Personnes	Données	Destinataires	Durée
Dossier patient	Prise en soins, suivi de l'appareillage	Patients	Identité, INS, santé, mesures, modèles 3D, photos	Équipe, prescripteur	Voir politique d'archivage

Traitement	Finalité	Personnes	Données	Destinataires	Durée
Facturation / télétransmission	Facturer, être remboursé	Patients	Identité, NIR, droits, codes LPP	AMO, AMC, SCOR	Durée légale comptable
Rendez-vous	Organiser l'activité	Patients	Identité, coordonnées	Équipe	Durée du suivi
Gestion du personnel	Paie, contrats, planning	Salariés	Identité, contrat, paie	Comptable, URSSAF	Durées légales sociales
Fournisseurs / achats	Commandes, comptabilité	Contacts pro	Coordonnées professionnelles	Comptable	10 ans (pièces)
Recrutement	Sélectionner	Candidats	CV, lettre	Dirigeant	Quelques mois
Vidéosurveillance (si présente)	Sécurité des locaux	Patients, salariés, visiteurs	Images	Dirigeant, forces de l'ordre sur réquisition	Quelques semaines

À chaque ligne, on ajoute utilement : la **base légale**, les **mesures de sécurité**, et les éventuels **transferts hors Union européenne**.

Le registre **vit** : on le met à jour à chaque nouveau logiciel, nouveau prestataire, nouvel usage. Un registre écrit une fois en 2019 et jamais rouvert ne prouve rien.

2. Le délégué à la protection des données (DPO)

Obligatoire notamment lorsque l'activité principale conduit à un **traitement à grande échelle de données sensibles**. Pour un cabinet d'orthoprothèse de quelques personnes, la désignation n'est en général **pas obligatoire** — mais elle est **recommandée**, et une structure plus importante, un réseau ou un groupe d'établissements relèvera souvent de l'obligation.

Le DPO peut être **interne** ou **externe** (mutualisé entre plusieurs structures, ce qui est fréquent et économique). Il **informe et conseille**, **contrôle** le respect des règles, **coopère avec la CNIL** et sert de **point de contact** pour les personnes.

Il n'est **pas** le responsable de traitement : la responsabilité reste au dirigeant. Et il doit disposer des moyens et de l'indépendance nécessaires — on ne nomme pas DPO la personne qui décide des traitements.

Quand il n'y a pas de DPO, il faut malgré tout **désigner un référent** identifié dans l'équipe. Sinon, personne ne tient le registre et personne ne répond aux demandes.

3. L'analyse d'impact (AIPD)

Une **analyse d'impact relative à la protection des données** est requise lorsqu'un traitement est susceptible d'engendrer un **risque élevé** pour les personnes — ce qui vise notamment les traitements **à grande échelle** de données de santé.

Un cabinet de taille modeste n'y est généralement pas tenu pour son dossier patient courant, mais la question se pose sérieusement en cas de **nouveau dispositif** : plateforme de télésuivi, base de modèles 3D mutualisée, outil d'analyse de marche connecté, recherche. En cas de doute : la CNIL publie des listes de traitements nécessitant ou non une AIPD.

4. Les violations de données

Définition : une violation, c'est toute atteinte à la **confidentialité** (accès ou divulgation non autorisés), à l'**intégrité** (altération) ou à la **disponibilité** (perte, destruction) de données personnelles — **accidentelle ou illicite**.

Le mot important est **accidentelle** : il n'y a pas besoin d'un pirate.

Événement	Violation ?	Type
Compte rendu envoyé au mauvais patient	Oui	Confidentialité
Ordinateur portable non chiffré volé	Oui	Confidentialité
Rançongiciel chiffrant les dossiers	Oui	Disponibilité (+ confidentialité si exfiltration)
Classeur de dossiers papier perdu	Oui	Confidentialité
Serveur en panne, données intactes, restaurées en 2 h	Non (incident technique)	—
Salarié consultant un dossier sans motif	Oui	Confidentialité
Suppression accidentelle sans sauvegarde	Oui	Disponibilité

Ce qu'il faut faire

1. **Documenter toutes les violations** dans un **registre des violations** — y compris celles qu'on ne notifie pas. Ce registre doit pouvoir être présenté à la CNIL.
2. **Évaluer le risque** pour les personnes : nature des données (santé = risque élevé par défaut), nombre de personnes, facilité d'identification, conséquences possibles.

3. **Notifier la CNIL sous 72 h** dès lors que le risque n'est pas négligeable. En cas de retard, motiver. Une notification peut être complétée ensuite.
4. **Informer les personnes concernées sans délai** si le risque est **élevé** : leur dire ce qui s'est passé, quelles données, quelles conséquences possibles, ce qu'elles peuvent faire, et qui contacter.
5. **Prendre les mesures correctives**, et les consigner.

Le registre des violations note pour chaque événement : date de survenue et de découverte, nature, données et personnes touchées, conséquences, mesures prises, décision de notifier ou non **et sa justification**.

À retenir

- **Registre des traitements** : une ligne par traitement, mis à jour, présentable à tout moment.
- **DPO** : souvent non obligatoire en petit cabinet, toujours utile ; à défaut, un **référent désigné**.
- **AIPD** : pour les traitements à risque élevé — à examiner avant tout nouveau dispositif.
- **Violation** = confidentialité, intégrité **ou** disponibilité, y compris par accident.
- **Toutes** les violations se documentent ; celles à risque se notifient à la **CNIL sous 72 h** ; celles à risque **élevé** s'annoncent **aux patients**.

Revision #3
Created 2026-09-15 17:24:33 UTC by Antoine
Updated 2026-09-16 07:03:21 UTC by Antoine