Veille juridique protection des données
Juin & Juillet 2026

Veille n°8 : Juin & Juillet 2026
Ségolène Salomez – Déléguée à la Protection des Données
Pour toute question : segolene.salomez@institutimagine.org

DIVERS

CEPD, adoption d'un modèle commun de notification des violations de données, 10 juin 2026 :

edpb_template_2026_data_breach_notification_v1.0_en.docx

Pour aider les entreprises et les autorités à mieux respecter le **RGPD** (le règlement européen sur la protection des données), le **Comité européen de la protection des données (CEPD)** a créé un **modèle standard** pour signaler les fuites de données.

À quoi sert ce modèle ?

- Il permet aux organisations de **structurer et simplifier** leurs déclarations en cas de fuite de données.
- Il s'assure que toutes les informations nécessaires (comme celles demandées par l'**article 33 du RGPD**) sont présentes.
- Il facilite le travail des autorités, qui peuvent ainsi **évaluer plus rapidement** les incidents.
  Grâce à des **options prédéfinies** et des **conseils pratiques**, ce modèle permet de gagner du temps et d'éviter les erreurs

Impact pour Imagine : Ce modèle va standardiser et accélérer notre procédure de gestion de crise en cas de fuite de données (ex: perte de fichiers génomiques, ransomware). En tant que structure de recherche gérant des données de santé sensibles, l'adoption de ce template permettra de respecter plus facilement le délai strict de 72h imposé par l'article 33 du RGPD lors de la notification à la CNIL.

CNIL, revoir le webinaire – Pixels de suivi dans les courriers : présentation des recommandations de la CNIL, 15 juin 2026 :

Qu'est-ce que la CNIL désigne par le terme de « pixel de suivi » ? Comment s'assurer que leur utilisation respecte la règlementation ?

Suite à la publication de ses recommandations, la CNIL présente le cadre applicable afin d'aider les acteurs à mieux comprendre leurs obligations et assurer le respect des droits des personnes.

Lien vers le webinaire

Q&A CNIL sur les recommandations

Impact pour Imagine : Si l'Institut utilise des outils de mailing (newsletters scientifiques, invitations à des colloques, campagnes de fundraising) intégrant des pixels de suivi pour mesurer les taux d'ouverture, une mise en conformité immédiate est requise. L'utilisation

de ces traceurs sans consentement préalable explicite est désormais clairement sanctionnée. Nous devons auditer nos outils d'emailing, désactiver les pixels par défaut ou mettre en place un mécanisme de recueil de consentement spécifique avant tout chargement d'image tierce, sous peine de risques réputationnels et financiers. Pour les bases de données déjà constituées, nous devons envoyer un email aux personnes afin de les informer & leur laisser la possibilité de s'opposer.

CNIL, 23 nouvelles sanctions prononcées depuis janvier au titre de la procédure simplifiée, 06 juillet 2026 :

La CNIL a mis en place une procédure simplifiée pour sanctionner les organisations qui ne respectent pas les règles de protection des données. Contrairement à la procédure classique, ici, une seule personne (le président ou un membre de la formation restreinte de la CNIL) décide de la sanction.

Les limites de cette procédure :

- Le montant maximal de l'amende est de 20 000 €.
- Le nom de l'organisme sanctionné n'est pas rendu public.

À savoir :

Toutes les amendes prononcées par la CNIL, qu'elles concernent des entreprises privées ou des administrations, sont recouvrées par l'État et versées au budget national.

Bilan depuis janvier 2026 :

La CNIL a déjà prononcé 23 sanctions dans le cadre de cette procédure, pour un total de 133 750 € d'amendes. Ces sanctions concernent principalement trois types de manquements :

1. **La vidéosurveillance abusive des salariés**

Certaines entreprises surveillent leurs employés sans respecter leur vie privée.

2. **Les manquements aux règles sur les cookies**

Certains sites déposent des cookies publicitaires (qui nécessitent le consentement de l'utilisateur) avant même que l'internaute n'ait agi. Également, il est souvent plus facile d'accepter tous les cookies que de les refuser. Par exemple, une bannière propose un bouton "Tout accepter" en un clic, mais pour refuser, il faut :

- Cliquer sur "Personnaliser"
- Puis accéder à une interface pour désactiver chaque cookie un par un.

Or, la loi est claire : si un site permet d'accepter tous les cookies en un clic, il doit aussi permettre de tous les refuser en un clic. Les organismes qui ne respectent pas cette règle risquent une amende.

3. **Le non-respect des droits des utilisateurs et le défaut de coopération avec la CNIL**

Sur les 23 sanctions, 8 concernent le non-respect des droits d'accès ou d'effacement (par exemple, une entreprise qui ne répond pas à une demande de suppression de données personnelles). Parmi elles, 4 sont liées à un défaut de coopération avec la CNIL : certaines sociétés (y compris des avocats ou des médecins) n'ont pas répondu aux demandes de la CNIL pendant l'enquête.

Résultat : elles ont écopé d'une amende, parfois assortie d'une injonction (obligation de se mettre en conformité sous peine de payer une somme supplémentaire). Ne pas répondre à la CNIL est illégal.

CEPD, anonymisation et moissonnage pour l'IA générative, traitement de données au moyen de technologies de la chaîne de blocs : adoption de la version finale des lignes directrices, 7 juillet 2026 :

Comprendre les données anonymes :

Les nouvelles lignes directrices du CEPD clarifient la notion de données anonymes, en tenant également compte de l'arrêt de la Cour de justice de l'Union européenne dans l'affaire C-413/23 P, CEPD/CRU, du 4 septembre 2025, et d'autres arrêts de la CJUE.

Les données sont anonymes si elles ne concernent pas une personne physique identifiée ou identifiable. La question de savoir si tel est le cas peut varier d'une entité à l'autre.

Les informations peuvent concerner une personne en raison de leur contenu, de leur finalité ou de leurs effets. L'existence d'un tel lien peut ne pas être immédiatement évidente et pourrait nécessiter une analyse plus approfondie.

Une personne est considérée comme « identifiée ou identifiable » si elle peut être distinguée des autres dans un contexte spécifique en utilisant des moyens raisonnablement susceptibles d'être utilisés d'une manière qui permet de les traiter différemment. La question de savoir si les moyens sont raisonnablement susceptibles d'être utilisés dépendra du point de vue de l'entité concernée et devrait être appréciée à la lumière de tous les facteurs objectifs.

Les lignes directrices fournissent également un cadre pratique permettant aux organisations de déterminer si l'anonymisation est un succès. Le cadre peut être appliqué de deux manières : soit en évaluant les différences de capacités entre ceux qui pourraient identifier l'individu (« approche contextuelle »), soit, par souci de simplicité, en

ne tenant pas compte de ces différences (« approche simplifiée »), si un responsable du traitement choisit de le faire. L'approche contextuelle reflète toutes les nuances de la norme juridique relative à l'anonymisation. L'approche simplifiée peut aller au-delà de la norme juridique et peut amener un responsable du traitement anonymisant à traiter les données comme si elles n'étaient pas anonymes, même si ce serait effectivement le cas pour certaines entités concernées, mais cette approche peut être plus pratique et fournir une plus grande confiance dans le fait que les données sont réellement anonymes.

Le cadre utilise **3 critères** pour tester si les données sont anonymes :

1. **pas d'individualisation des enregistrements :** il ne doit pas être possible d'isoler un individu dans le jeu de données
2. **pas de corrélation** : il ne doit pas être possible de relier entre eux des ensembles de données distincts concernant un même individu
3. **pas d'inférence :** il ne doit pas être possible de déduire, de façon quasi certaine, de nouvelles informations sur un individu.

Si les trois critères sont remplis, les données peuvent être considérées comme anonymes en toute sécurité. Si l'un de ces critères n'est pas satisfait, une analyse plus approfondie devrait être effectuée pour déterminer si les données peuvent être considérées comme anonymes.

- Lignes directrices sur l'anonymisation (PDF, en anglais)

Clarifier les implications du moissonnage sur la protection des données pour le développement de l'IA :

Le moissonnage (ou *web scraping*) est une technique automatisée qui permet de collecter massivement des données sur internet, souvent sans que les personnes concernées le sachent. Cette pratique peut poser des risques pour la protection des données personnelles, surtout quand elle alimente le développement de l'intelligence artificielle (IA).

L'IA générative (comme les outils qui créent du texte, des images ou de la voix) a besoin d'énormes quantités de données pour fonctionner. Mais attention : si ces données contiennent des informations personnelles, le RGPD (le règlement européen sur la protection des données) s'applique.

Que dit le RGPD sur le moissonnage ?

Le Comité européen de la protection des données (CEPD) a publié des lignes directrices pour encadrer cette pratique. Voici les points clés :

1. Une base légale est obligatoire

Pour moissonner des données personnelles, il faut une raison valable (appelée *base juridique*), comme le consentement des personnes par exemple.

2. Respecter les principes du RGPD

- **Limitation de la finalité** : Les données ne doivent être utilisées que pour l'objectif annoncé (ex. : entraîner un modèle d'IA).
- **Transparence** : Les personnes doivent être informées que leurs données sont collectées **sauf exceptions.**
- **Minimisation des données** : Ne collecter que le strict nécessaire.
- **Précision** : Les données doivent être fiables et à jour. Le CEPD conseille d'utiliser des sources fiables, d'enregistrer la date de collecte et de vérifier les données avant de les utiliser pour entraîner une IA.

3. Attention aux données sensibles

Le RGPD interdit en principe le traitement des données sensibles (origine ethnique, santé, opinions politiques, etc.).

Exception possible : Si la collecte est accessoire (non intentionnelle) et que des mesures strictes sont mises en place pour éviter leur utilisation, une dérogation peut être envisagée.

Lignes directrices sur le moissonnage dans le contexte de l'IA générative (PDF, en anglais)

Lignes directrices sur les chaînes de blocs finalisées après consultation publique :

Les lignes directrices aident les organisations qui utilisent les technologies blockchain à se conformer au RGPD. Le CEPD explique le fonctionnement des chaînes de blocs, en évaluant les différentes architectures possibles et leurs implications pour le traitement des données à caractère personnel.

Conformément à l'objectif de la déclaration d'Helsinki de renforcer le dialogue avec les parties prenantes, le comité a également publié un rapport sur les résultats de la consultation publique spécifique, ainsi qu'une version des lignes directrices intitulée « Track changes ».

Impact pour Imagine :

- **Anonymisation :** Pour nos projets de partage de données de recherche ou de publication, (critères : pas d'individualisation, corrélation, inférence) l'approche

"simplifiée" suggérée par le CEPD pourrait nous inciter à traiter certaines données comme personnelles par prudence, impactant nos bases de données de recherche "anonymisées".

- **IA & Moissonnage :** Si l'Institut développe ou utilise des modèles d'IA générative entraînés sur des données web, la licéité du "scraping" est encadrée. L'utilisation de données de santé (catégorie spéciale) collectées accidentellement lors du moissonnage reste interdite sauf exception très stricte. Il faudra documenter rigoureusement la base légale (intérêt légitime) et mettre en place des filtres techniques robustes pour exclure les données sensibles avant entraînement.
- **Blockchain :** Si l'Institut explore la blockchain pour la traçabilité des consentements patients par exemple ces lignes directrices sont cruciales. Elles rappellent la tension entre l'immuabilité de la blockchain et le droit à l'effacement (RGPD). Toute nouvelle implémentation technologique devra privilégier des architectures où les données personnelles ne sont pas stockées "en clair" sur la chaîne pour rester conforme (ex: stockage des données identifiantes hors chaîne avec chiffrement sur la blockchain) .

CNIL, mise à jour des MR 001 et MR 003, ce qui change en 2026 – Revoir le webinaire, 31 juillet 2026 :

Les méthodologies de référence MR-001 et MR-003 évoluent.

Intégrant les besoins formulés par les acteurs, les nouvelles MR voient leur périmètre élargi : études menées à l'étranger, modalités d'information (y compris de manière dématérialisée), nature des données traitées, contrôle qualité à distance, destinataires des données, etc.

Sur la forme, les MR suivent un plan actualisé et de nouveaux documents ont fait leur apparition : annexes dédiées à la sécurité et au contrôle qualité, MR annotées, grilles de conformité, etc.

Revoir le webinaire.

Impact pour Imagine : Les Méthodologies de Référence (MR-001 pour les traitements internes, MR-003 pour la recherche) s'élargissent pour inclure explicitement les études menées à l'étranger et l'information dématérialisée.

Action requise : mettre à jour nos engagements de conformité pour couvrir nos collaborations internationales (transferts de données hors UE) et valider que nos formulaires de consentement/information patients (souvent dématérialisés aujourd'hui) respectent les nouveaux standards.