

AVIS DE LA CNIL SUR LE PROJET DE DECRET RELATIF AUX SYSTEMES D'INFORMATION

[> Lien vers le rapport de la CNIL](#)

La Commission nationale de l'informatique et des libertés (CNIL) a rendu, mercredi 13 mai 2020, son avis sur le projet de décret relatif aux systèmes d'information créés par l'article 6 du projet de loi prorogeant l'état d'urgence sanitaire.

La CNIL était saisie pour émettre ses observations et recommandations sur **les modalités d'application d'un système d'information permettant la collecte de données personnelles** afin de lutter contre l'épidémie de Covid.

L'AVIS DE LA CNIL

1. L'avis global de la CNIL

- Les finalités poursuivies par le système d'information (SI) apparaissent **déterminées, explicitées et légitimes**, conformément à l'article 5 du RGPD ;
- Nécessité de **réévaluer périodiquement les traitements de données à caractère personnel** au vu de l'évolution de l'épidémie et des connaissances scientifiques ;
- Transmission nécessaire dans leur version définitive **des analyses d'impact relatives à la protection des données (AIPD)** ainsi que, le cas échéant, leurs mises à jour ;
- Le refus des médecins, des patients ou des personnes « contacts » de participer aux enquêtes sanitaires **ne doivent pas entraîner de conséquences de quelque ordre que ce soit** ;
- Recommande **l'indépendance des systèmes d'information** créés par la loi par rapport à d'autres traitements pour que la fin de leur mise en œuvre soit effective dans les délais prévus ;
- Nécessité **d'encadrer strictement les finalités du SI** et d'une sanction pénale pour tout usage des données qui ne s'inscrirait pas dans celles-ci.

2. Sur les catégories de données personnelles

- Nécessité de la pertinence des données au regard des finalités du traitement **au nom du principe de minimisation des données**. Les listes de catégories de données doivent être exhaustives et ne pourront excéder celles prévues par la loi ;
- Nécessité de **préciser certaines catégories de données** : donnée de « rang de naissance », « données relatives au médecin à l'origine de l'inscription dans le traitement », données relatives à la profession qui comprennent « notamment » la qualité de professionnel de santé ;
- Nécessité d'une **protection particulière des données à caractère personnel concernant la santé** qui sont collectées ;
- Nécessité de **certaines mesures fonctionnelles dans le paramétrage du traitement** : exclure les zones « commentaires » ou « zones blocs notes » susceptibles de contenir des données non pertinentes. Lorsqu'un choix multiple est nécessaire, il doit être proposé au moyen de menus déroulants proposant des informations et appréciations objectives ;
- Nécessiter **de former et sensibiliser régulièrement les intervenants** du SI.

3. Sur les personnes pouvant consulter, enregistrer ou être destinataire des données

- Des **précisions supplémentaires doivent figurer dans le décret** : des limitations d'accès paramétrées dans le système d'information et ses règles d'usages ; les finalités au titre desquelles chaque catégorie d'accédant accède au système d'information et les données correspondantes ;
- Mise en place de mesures pour que **les personnes habilitées ne puissent accéder aux données relatives aux personnes concernées que lorsqu'elles en ont besoin**, et pour certaines personnes habilitées, uniquement en présence des personnes concernées ;
- Mise en place de **formations par les organismes pour leurs agents**, qui seront autorisés à consulter ou enregistrer des données : protection des données à caractère personnel, respect du secret professionnel et risques de sanctions pénales encourues en cas de détournement ;
- Formulation, par ces agents, **d'un engagement de respecter ces principes, préalablement à l'habilitation** ;
- **Limitation dans le temps et révision des habilitations délivrées**, notamment pour intégrer les éventuels départs d'agents ou changements d'affectation ;
- **Précision de la liste des organismes auxquels les données sensibles pourraient être transmises**. Elles devront présenter les garanties requises par le RGPD en matière de traitement des données.

4. Sur les droits des personnes

- Invite le gouvernement à **minimiser les cas d'exclusion du droit d'opposition** ;
- Nécessité de mettre en œuvre **un mécanisme d'archivage intermédiaire des données** afin, notamment, que les « cas contact » puissent être rapidement retirés de la base active ;
- Nécessité **d'une parfaite information** qui devra être donnée aux personnes concernées quant au traitement de leurs données à caractère personnel, en cas de collecte directe ou indirecte ;
- **Ouverture de l'accès des personnes au détail des opérations effectuées sur leurs données**, sauf les données qui permettraient l'identification des personnes ayant réalisé ces opérations ;

5. Sur les mesures de sécurité

- **Mise en place d'un socle minimal de mesures de sécurité** afin de garantir un niveau de sécurité à l'état de l'art du secteur de la santé ;
- **Garantir la maîtrise de l'authentification des personnes et de la traçabilité des actions des utilisateurs** ;
- Utilisation, par l'ensemble des personnes habilitées à accéder aux données traitées, d'un **mécanisme d'authentification fort comportant plusieurs facteurs d'authentification** ;
- Mise en place d'un **mécanisme de surveillance et de scellement des traces**, afin de garantir que d'éventuelles opérations illégitimes soient non seulement tracées mais effectivement détectées.

6. Sur les destinataires des données

- Nécessité de définir, pour les organismes concernés, **une politique d'habilitation de leurs agents très stricte** afin que seuls ceux qui en ont besoin accèdent à SI-DEP ;
- **Revue régulière des habilitations délivrées**, notamment pour intégrer les éventuels départs ou changement d'affectation des agents ;
- **Sensibilisation et formation de chaque organisme** dont les agents ou personnels seront autorisés à consulter ou enregistrer des données, à leurs obligations : protection des données à caractère personnel, respect du secret professionnel, risques de sanctions pénales encourues en cas de détournement du traitement ;
- **Nécessité d'une information claire et complète** apportée sur les dispositifs de traçage des accès mis en place, permettant un contrôle régulier de l'utilisation des données contenues dans le traitement ;
- **Nécessité de justifier** pour chaque catégorie de données dont le traitement est envisagé, **du besoin d'en connaître de chaque catégorie de destinataires**.