CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

Délibération n° 2017-249 du 14 septembre 2017 portant avis sur un projet d'arrêté relatif aux modalités de signalement et de traitement des incidents graves de sécurité des systèmes d'information

(demande d'avis n° 17016219)

La Commission nationale de l'informatique et des libertés,

Saisie par le ministère des solidarités et de la santé d'une demande d'avis concernant un projet d'arrêté relatif aux modalités de signalement et de traitement des incidents graves de sécurité des systèmes d'information ;

Vu la convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ;

Vu la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données ;

Vu le code de la santé publique, notamment ses articles L. 1110-4-1, L. 1111-8-2 et D. 1111-16-3 ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, notamment ses articles 11-2°-d) ;

Vu le décret n° 2005-1309 du 20 octobre 2005 modifié pris pour l'application de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

Vu le décret n° 2016-1214 du 12 septembre 2016 relatif aux conditions selon lesquelles sont signalés les incidents graves de sécurité des systèmes d'information ;

Vu l'arrêté du 27 février 2017 relatif au traitement automatisé de données à caractère personnel dénommé « portail de signalement des évènements sanitaires indésirables » ;

Sur la proposition de Mme Valérie PEUGEOT, commissaire, et après avoir entendu les observations de Mme Nacima BELKACEM, commissaire du Gouvernement,

Émet l'avis suivant :

La Commission a été saisie par la ministre des solidarités et de la santé d'une demande d'avis concernant un projet d'arrêté relatif aux modalités de signalement et de traitement des incidents graves de sécurité des systèmes d'information.

L'article 110 de la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, codifié à l'article L. 1111-8-2 du code de la santé publique (CSP), fait obligation aux établissements de santé et les organismes et services exerçant des activités de prévention, de diagnostic ou de soins, de déclarer les *« incidents graves de sécurité des systèmes d'information »*.

Ce projet d'arrêté (ci-après le « projet ») est pris en application de l'article D. 1111-16- 3 du CSP créé par le décret n° 2016-1214 du 12 septembre 2016 relatif aux conditions selon lesquelles sont signalés les incidents graves de sécurité des systèmes d'information.

Il vise à préciser les modalités de signalement et de traitement des incidents graves et notamment le traitement de données à caractère personnel mis en œuvre dans ce cadre par l'ASIP santé.

Afin d'apporter un appui et un accompagnement aux structures de santé concernées par la déclaration de ces incidents, le ministère de la santé met en place un dispositif pour traiter leur signalement, en lien avec les ARS, l'ASIP Santé et les services du haut fonctionnaire de défense et de sécurité des ministères chargés des affaires sociales.

La déclaration d'un incident grave de sécurité est effectuée par les établissements concernés sur le portail de signalement des évènements sanitaires indésirables prévu par l'arrêté du 27 février 2017 précité.

Les déclarations sont récupérées, d'une part, par l'ARS territorialement compétente et, d'autre part, par l'ASIP santé.

L'ASIP santé informe la structure concernée de la prise en compte de sa déclaration, analyse celle-ci et qualifie les incidents signalés lorsqu'ils constituent des incidents significatifs, pour le compte de l'ARS compétente. Cette dernière est alors tenue informée de la qualification de l'incident.

Enfin, l'ASIP santé informe les agences ou autorités compétentes de l'Etat, conformément à l'article D. 1111-16- 3 du CSP.

Le circuit de déclaration décrit dans le projet d'arrêté est la déclinaison opérationnelle de celui initialement prévu par les textes et n'a pas pour objet de remettre en cause les responsabilités définies dans le décret.

Sur le responsable de traitement et les formalités préalables :

Les déclarations d'incident graves reçues sur le portail sont transmises à l'ARS compétente et à l'ASIP santé.

Les ARS sont donc destinataires, dès l'origine, des déclarations qui les concernent.

Ainsi, la Commission constate qu'il existe deux traitements distincts de données à caractère personnel : le traitement mis en œuvre par l'ASIP santé et mentionné à l'article D. 1111-16-3 du CSP d'une part, celui mis en œuvre par l'ARS territorialement compétente d'autre part.

Ces traitements doivent faire l'objet des formalités préalables prévues par la loi et présenter des garanties similaires en matière de protection des données.

Concernant les formalités devant être effectuées par l'ASIP Santé, la Commission relève que l'article 4 du projet prévoit que le traitement de données à caractère personnel qu'elle met en œuvre est « *autorisé par le présent arrêté* » ; la Commission étant saisie sur le fondement de l'article 11-2°-d) de la loi, le traitement mis en œuvre par l'ASIP Santé devra faire l'objet d'une déclaration normale ou être inscrit dans le registre du correspondant informatique et libertés, conformément à l'article 22 de cette même loi. Chaque ARS devra, elle aussi, effectuer une telle déclaration.

Par ailleurs, la Commission prend acte de l'engagement du ministère de modifier l'article 4 du projet afin de remplacer le terme « *autorisé* » par « *créé* ».

Sur les finalités :

La Commission n'a pas d'observations à formuler sur ce point.

Sur la nature des données :

La Commission n'a pas d'observations à formuler sur ce point.

Sur les destinataires des données :

La Commission n'a pas d'observations à formuler sur ce point.

Sur l'information et les droits des personnes :

L'article 8 du projet prévoit que l'ASIP santé et les ARS compétentes procèdent à l'information des personnes concernées, conformément à l'article 32 de la loi « informatique et libertés ».

Le dossier produit à l'appui du projet précise que l'ASIP santé informe les déclarants via le portail de son rôle ainsi que des finalités du traitement, au travers des mentions légales du site et des conditions générales d'utilisation (CGU). L'utilisateur devra systématiquement accepter les CGU avant de pouvoir déclarer.

La Commission souhaite rappeler que l'information délivrée dans le cadre du traitement objet de la présente saisine doit être distincte de l'information délivrée par l'ASIP santé dans le cadre du traitement de données relatif à la gestion du portail de signalement des évènements sanitaires indésirables.

Par ailleurs, l'article précité précise que le droit d'opposition prévu à l'article 38 de la loi « informatique et libertés » ne s'applique pas au présent traitement.

Si le signalement des incidents de sécurité constitue une obligation légale justifiant ainsi l'exclusion de l'exercice du droit d'opposition, la mise en œuvre d'un service d'information et d'accompagnement est, quant à elle, facultative. Le droit d'opposition doit donc pouvoir s'exercer.

La Commission prend acte de l'engagement du ministère de modifier le projet afin de préciser que l'exclusion du droit d'opposition ne porte que sur les traitements de données à caractère personnel strictement nécessaires à la réalisation de l'obligation légale de signalement et de traitement des incidents graves de sécurité des systèmes d'information.

Sur les durées de conservation :

L'article 7 du projet prévoit que les données collectées dans le cadre du traitement des incidents graves de sécurité sont conservées pendant la durée nécessaire à la gestion de l'incident de sécurité avant de faire l'objet d'un archivage.

La Commission relève que, d'une part, la durée durant laquelle ces données sont archivées et, d'autre part, les personnes habilitées à y accéder ne sont pas précisées par le projet.

Elle recommande que les ARS définissent des durées d'archivage uniformisées dans la mesure où les traitements mis en œuvre par ces dernières sont similaires.

La Commission souhaite également rappeler que les données archivées ne devront être accessibles que par un nombre limité de personnes habilitées à y accéder en raison de leurs fonctions.

Sur les mesures de sécurité :

La Commission relève que les articles 5 et 6 du projet prévoient que l'ASIP santé et les ARS sont responsables de la mise en œuvre des mesures de sécurité destinées à garantir la confidentialité et l'intégrité des données à caractère personnel de leurs traitements respectifs.

Cependant, elle relève que seul l'article 5 concernant l'ASIP santé mentionne des mesures particulières et que le dossier produit à l'appui du projet décrit uniquement les mesures de sécurité qui sont envisagées par l'ASIP santé.

Considérant les risques que le traitement d'informations sur des incidents et failles de sécurité peut faire peser sur tous les systèmes d'information traitant des données personnelles, la Commission considère que certaines mesures de sécurité devraient être mises en œuvre par les traitements de l'ASIP santé comme par ceux des ARS. Elle recommande d'ajouter à l'arrêté un article rédigé comme suit :

« [Sécurité des données]

Afin de garantir la sécurité des données des traitements visés par le présent arrêté, des mesures de sécurité doivent être définies au regard d'une analyse des risques ; elles doivent être matérialisées dans une politique de sécurité et faire l'objet de contrôles et de révisions régulières au vu des évolutions des traitements, de leurs usages et de leur environnement. »

Ces mesures de sécurité peuvent ainsi comprendre :

- *des moyens d'authentification et de gestion des habilitations encadrant l'accès aux données et aux locaux par les personnes habilitées ;*
- *des mécanismes de chiffrement préservant la confidentialité des flux de données, ainsi que, de préférence, celle des bases de données et des sauvegardes ;*
- *une journalisation et un contrôle des traces permettent de détecter des comportements anormaux et de lever des alertes ;*
- *des procédures de sécurité sont définies et appliquées pour les échanges d'informations effectués par courriel, papier et téléphone ;*
- *des clauses spécifiques dans les contrats de sous-traitance encadrent la sécurité des données. »*

Sur la modification de l'arrêté « portail de signalement des évènements sanitaires indésirables » :

La Commission n'a pas d'observations à formuler sur ce point.

Pour la Présidente,
Le Vice-Président Délégué

Marie-France MAZARS