Insee
Mesurer pour comprendre
Direction générale

CONCOURS INTERNE SPÉCIAL DE CONTRÔLEUR DE L'INSTITUT NATIONAL DE LA STATISTIQUE ET DES ÉTUDES ÉCONOMIQUES

ANNÉE 2020

ÉPREUVE DE RÉPONSES A DES QUESTIONS PORTANT SUR UN OU PLUSIEURS TEXTES A CARACTÈRE ADMINISTRATIF

Décembre 2019
(Durée : 3 heures, coefficient: 4)
Le sujet comporte 35 pages (y compris celle-ci)

Textes à étudier :

1 – Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles (10 pages)

2 – Directive 2016/681 du Parlement européen et du Conseil, du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière. (8 pages)

3 – Mémento à l'usage du directeur d'établissement de santé - Connaître vos risques pour mieux y faire face - Cybersécurité - édition 2017. (5 pages)

4 – Ce qu'il faut savoir sur l'analyse d'impact relative à la protection des données (AIPD) - 19 février 2018 ; Site de la CNIL – www.cnil.fr. (4 pages)

5 – Devenir délégué à la protection des données - 23 mai 2017 – www.cnil.fr. (5 pages)

Questions :

Vous pouvez répondre aux questions dans l'ordre que vous souhaitez en précisant à chaque fois le numéro de la question. Il sera tenu compte de la présentation, de la qualité de la rédaction et de l'orthographe.

Partie A (12 points sur 20)

Vous préciserez le numéro du document servant de référence à la rédaction de votre réponse et, chaque fois que nécessaire, le ou les article(s) des textes.

Q1 : Qu'est-ce que le G29, l'instance qui a clarifié le rôle du délégué à la protection des données ?

Q2 : Quels sont les deux piliers sur lesquels repose une analyse d'impact relative à la protection des données (AIPD)?

Q3 : D'après la loi, à partir de quel âge un mineur peut-il donner seul son consentement à un traitement de données à caractère personnel en ce qui concerne l'offre directe de services de la société de l'information ?

Q4 : Dans quelles conditions Europol peut-il présenter une demande électronique d'accès aux données PNR ?

Q5 : Quel article encadre l'hébergement de données de santé à caractère personnel ?

Q6 : Comment est estimé un risque sur la vie privée dans une AIPD ?

Q7 : Quel est le nom de l'autorité compétente en matière de prévention et de détection des infractions terroristes et des formes graves de criminalités, ainsi que d'enquêtes et de poursuites en matière d'utilisation des données des dossiers passagers ?

Q8 : Quels sont les deux certificats délivrés aux entités hébergeant des données de santé depuis 2018 ?

Q9 : Citer deux exemples de fonctions susceptibles de donner lieu à un conflit d'intérêt si le délégué à la protection des données les occupaient ?

Q10 : Citez trois exemples de programmes nationaux qui illustrent la transition numérique dans le secteur de la santé.

Q11 : Dans quel cas un organisme doit-il obligatoirement désigner un délégué à la protection des données ?

Q12 : D'après la loi, quelles sont les données à caractère personnel qu'il est interdit de traiter ?

Q13 : Si le traitement de données personnelles répond à une obligation légale ou est nécessaire à l'exercice d'une mission de service public, une AIPD est nécessaire sauf à remplir certaines conditions, lesquelles ?

Q14 : En matière de données personnelles lorsqu'un responsable d'un traitement ne respecte pas ses obligations (celles résultant du règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016), citer précisément trois des mesures susceptibles d'être prononcées, d'après la loi, par le Président de la CNIL ?

Q15 : Afin de dépersonnaliser les données PNR, quels éléments en sont masqués ?

Q16 : D'après la loi, quel est le rôle du comité d'audit du système national des données de santé ?

Q17 : Dans le texte sur l'analyse d'impact relative à la protection des données comment définir les termes suivants (soulignés dans le texte numéro 4) : soudoyé, finalité, vraisemblance, résiduel.

Partie B (8 points sur 20)

Selon vous, comment chaque individu peut-il se prémunir des impacts des nouvelles technologies du numérique sur le respect de la vie privée ?

Vous rédigerez une réponse structurée en une trentaine de lignes maximum.

Texte 1

Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles

L'Assemblée nationale et le Sénat ont délibéré,
L'Assemblée nationale a adopté
Vu la décision du Conseil constitutionnel n° 2018-765 DC du 12 juin 2018 ;
Le Président de la République promulgue la loi dont la teneur suit :

Titre Ier : DISPOSITIONS D'ADAPTATION COMMUNES AU RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL DU 27 AVRIL 2016 ET À LA DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL DU 27 AVRIL 2016

Chapitre Ier : Dispositions relatives à la Commission nationale de l'informatique et des libertés

Article 1

L'article 11 de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés est ainsi modifié :

1° Au début du premier alinéa, est ajoutée la mention : « I.-» ;

2° Après la première phrase du même premier alinéa, est insérée une phrase ainsi rédigée : « Elle est l'autorité de contrôle nationale au sens et pour l'application du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité » ;

3° Le 1° est complété par les mots : « et peut, à cette fin, apporter une information adaptée aux collectivités territoriales, à leurs groupements et aux petites et moyennes entreprises » ;

4° Le 2° est ainsi modifié :

a) Le premier alinéa est complété par les mots : « et aux autres dispositions relatives à la protection des données personnelles prévues par les textes législatifs et réglementaires, le droit de l'Union européenne et les engagements internationaux de la France » ;

b) Au a, les mots : « autorise les traitements mentionnés à l'article 25, » et, à la fin, les mots : « et reçoit les déclarations relatives aux autres traitements » sont supprimés ;

c) Après le même a, il est inséré un a bis ainsi rédigé :

« a bis) Elle établit et publie des lignes directrices, recommandations ou référentiels destinés à faciliter la mise en conformité des traitements de données à caractère personnel avec les textes relatifs à la protection des données à caractère personnel et à procéder à l'évaluation préalable des risques par les responsables de traitement et leurs sous-traitants. Elle prend en compte la situation des personnes dépourvues de compétences numériques. Elle encourage l'élaboration de codes de conduite définissant les obligations qui incombent aux responsables de traitement et à leurs sous-traitants, compte tenu du risque inhérent aux traitements de données à caractère personnel pour les droits et libertés des personnes physiques, notamment des mineurs, et des besoins spécifiques des collectivités territoriales, de leurs groupements et des micro-entreprises, petites entreprises et moyennes entreprises ; elle homologue et publie les méthodologies de référence destinées à favoriser la conformité des traitements de données de santé à caractère personnel ; »

d) Le b est ainsi rédigé :

« b) En concertation avec les organismes publics et privés représentatifs des acteurs concernés, elle établit et publie des règlements types en vue d'assurer la sécurité des systèmes de traitement de données à caractère personnel et de régir les traitements de données biométriques, génétiques et de santé. A ce titre,

sauf pour les traitements mis en œuvre pour le compte de l'Etat agissant dans l'exercice de ses prérogatives de puissance publique, elle peut prescrire des mesures, notamment techniques et organisationnelles, supplémentaires pour le traitement des données biométriques, génétiques et de santé en application du 4 de l'article 9 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité et des garanties complémentaires en matière de traitement de données à caractère personnel relatives aux condamnations pénales et aux infractions conformément à l'article 10 du même règlement ; »

e) Après le f, il est inséré un f bis ainsi rédigé :

« f bis) Elle peut décider de certifier des personnes, des produits, des systèmes de données ou des procédures aux fins de reconnaître qu'ils se conforment au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité et à la présente loi. Elle prend en considération, à cette fin, les besoins spécifiques des collectivités territoriales, de leurs groupements et des micro-entreprises, petites entreprises et moyennes entreprises. Elle agrée, aux mêmes fins, des organismes certificateurs, sur la base, le cas échéant, de leur accréditation par l'organisme national d'accréditation mentionné au b du 1 de l'article 43 du même règlement ou décide, conjointement avec cet organisme, que ce dernier procède à leur agrément, dans des conditions précisées par décret en Conseil d'Etat pris après avis de la Commission nationale de l'informatique et des libertés. La commission élabore ou approuve les critères des référentiels de certification et d'agrément ; »

f) Au g, après le mot : « certification », sont insérés les mots : «, par des tiers agréés ou accrédités selon les modalités mentionnées au f bis du présent 2°, » ;

g) A la fin du h, les mots : « d'accès concernant les traitements mentionnés aux articles 41 et 42 » sont remplacés par les mots : « ou saisines prévues aux articles 41,42 et 70-22 » ;

h) Sont ajoutés des i et j ainsi rédigés :

« i) Elle peut établir une liste des traitements susceptibles de créer un risque élevé devant faire l'objet d'une consultation préalable conformément à l'article 70-4 ;

« j) Elle mène des actions de sensibilisation auprès des médiateurs de la consommation et des médiateurs publics, au sens de l'article L. 611-1 du code de la consommation, en vue de la bonne application de la présente loi ; »

5° Après la première phrase du a du 4°, est insérée une phrase ainsi rédigée :

« Elle peut également être consultée par le Président de l'Assemblée nationale, par le Président du Sénat ou par les commissions compétentes de l'Assemblée nationale et du Sénat ainsi qu'à la demande d'un président de groupe parlementaire sur toute proposition de loi relative à la protection des données à caractère personnel ou au traitement de telles données. » ;

6° Après le même 4°, il est inséré un 5° ainsi rédigé :

« 5° Elle peut présenter des observations devant toute juridiction à l'occasion d'un litige relatif à l'application de la présente loi et des dispositions relatives à la protection des données personnelles prévues par les textes législatifs et règlementaires, le droit de l'Union européenne, y compris le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, et les engagements internationaux de la France. » ;

7° Au début du vingt-sixième alinéa, est ajoutée la mention : « II.-» ;

8° L'avant-dernier alinéa est supprimé.

Article 2

Le I de l'article 13 de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi modifié :

1° Au 6°, le mot : « ou » est remplacé par le mot : « et » ;

2° Au 7°, après le mot : « numérique », sont insérés les mots : « et des questions touchant aux libertés individuelles ».

Article 3

L'article 15 de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi modifié :

1° Après le premier alinéa, il est inséré un alinéa ainsi rédigé :

« L'ordre du jour de la commission réunie en formation plénière est rendu public. » ;

2° Sont ajoutés trois alinéas ainsi rédigés :

«-au 4 de l'article 34 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, pour les décisions donnant acte du respect des conditions mentionnées au 3 du même article 34 ;

«-aux a et h du 3 de l'article 58 du même règlement.

« Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés, fixe les conditions et limites dans lesquelles le président de la commission et le vice-président délégué peuvent déléguer leur signature. »

……...

Article 7

I.-Le chapitre VII de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi modifié :

1° L'intitulé est ainsi rédigé : « Mesures et sanctions prises par la formation restreinte de la Commission nationale de l'informatique et des libertés » ;

2° Les articles 45 à 48 sont ainsi rédigés :

« Art. 45.-I.-Le président de la Commission nationale de l'informatique et des libertés peut avertir un responsable de traitement ou son sous-traitant du fait que les opérations de traitement envisagées sont susceptibles de violer les dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité ou de la présente loi.

« II.-Lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut, si le manquement constaté est susceptible de faire l'objet d'une mise en conformité, prononcer à son égard une mise en demeure, dans le délai qu'il fixe :

« 1° De satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits ;

« 2° De mettre les opérations de traitement en conformité avec les dispositions applicables ;

« 3° A l'exception des traitements qui intéressent la sûreté de l'Etat ou la défense, de communiquer à la personne concernée une violation de données à caractère personnel ;

« 4° De rectifier ou d'effacer des données à caractère personnel, ou de limiter le traitement de ces données.

« Dans le cas prévu au 4° du présent II, le président peut, dans les mêmes conditions, mettre en demeure le responsable de traitement ou son sous-traitant de notifier aux destinataires des données les mesures qu'il a prises.

« Le délai de mise en conformité peut être fixé à vingt-quatre heures en cas d'extrême urgence.

« Le président prononce, le cas échéant, la clôture de la procédure de mise en demeure.

« Le président peut demander au bureau de rendre publique la mise en demeure. Dans ce cas, la décision de clôture de la procédure de mise en demeure fait l'objet de la même publicité.

« III.-Lorsque le responsable de traitement ou son sous-traitant ne respecte pas les obligations résultant du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité ou de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut également, le cas échéant après lui avoir adressé l'avertissement prévu au I du présent article ou, le cas échéant en complément d'une mise en demeure prévue au II, saisir la formation restreinte de la commission en vue du prononcé, après procédure contradictoire, de l'une ou de plusieurs des mesures suivantes :

« 1° Un rappel à l'ordre ;

« 2° Une injonction de mettre en conformité le traitement avec les obligations résultant de la présente loi ou du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité ou de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits, qui peut être assortie, sauf dans des cas où le traitement est mis en œuvre par l'Etat, d'une astreinte dont le montant ne peut excéder 100 000 € par jour de retard à compter de la date fixée par la formation restreinte ;

« 3° A l'exception des traitements qui intéressent la sûreté de l'Etat ou la défense ou de ceux relevant du chapitre XIII de la présente loi lorsqu'ils sont mis en œuvre pour le compte de l'Etat, la limitation temporaire ou définitive du traitement, son interdiction ou le retrait d'une autorisation accordée en application du même règlement ou de la présente loi ;

« 4° Le retrait d'une certification ou l'injonction, à l'organisme certificateur concerné, de refuser une certification ou de retirer la certification accordée ;

« 5° La suspension des flux de données adressées à un destinataire situé dans un pays tiers ou à une organisation internationale ;

« 6° La suspension partielle ou totale de la décision d'approbation des règles d'entreprise contraignantes ;

« 7° A l'exception des cas où le traitement est mis en œuvre par l'Etat, une amende administrative ne pouvant excéder 10 millions d'euros ou, s'agissant d'une entreprise, 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu. Dans les hypothèses mentionnées aux 5 et 6 de l'article 83 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, ces plafonds sont portés, respectivement, à 20 millions d'euros et 4 % dudit chiffre d'affaires. La formation restreinte prend en compte, dans la détermination du montant de l'amende, les critères précisés au même article 83.

« Le projet de mesure est, le cas échéant, soumis aux autres autorités de contrôle concernées selon les modalités définies à l'article 60 du même règlement.

« Art. 46.-I.-Lorsque le non-respect des dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité ou de la présente loi entraîne une violation des droits et libertés mentionnés à l'article 1er de la présente loi et que le président de la commission considère qu'il est urgent d'intervenir, il saisit la formation restreinte, qui peut, dans le cadre d'une procédure d'urgence contradictoire définie par décret en Conseil d'Etat, adopter l'une des mesures suivantes :

« 1° L'interruption provisoire de la mise en œuvre du traitement, y compris d'un transfert de données hors de l'Union européenne, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui intéressent la sûreté de l'Etat ou la défense ou de ceux relevant du chapitre XIII lorsqu'ils sont mis en œuvre pour le compte de l'Etat ;

« 2° La limitation du traitement de certaines des données à caractère personnel traitées, pour une durée maximale de trois mois, si le traitement n'est pas au nombre de ceux qui intéressent la sûreté de l'Etat ou la défense ou de ceux relevant du même chapitre XIII lorsqu'ils sont mis en œuvre pour le compte de l'Etat ;

« 3° La suspension provisoire de la certification délivrée au responsable de traitement ou à son sous-traitant ;

« 4° La suspension provisoire de l'agrément délivré à un organisme de certification ou un organisme chargé du respect d'un code de conduite ;

« 5° La suspension provisoire de l'autorisation délivrée sur le fondement du III de l'article 54 de la présente loi ;

« 6° L'injonction de mettre en conformité le traitement avec les obligations résultant du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité ou de la présente loi ou de satisfaire aux demandes présentées par la personne concernée en vue d'exercer ses droits, qui peut être assortie, sauf dans le cas où le traitement est mis en œuvre par l'Etat, d'une astreinte dont le montant ne peut excéder 100 000 € par jour de retard à compter de la date fixée par la formation restreinte ;

« 7° Un rappel à l'ordre ;

« 8° L'information du Premier ministre pour qu'il prenne, le cas échéant, les mesures permettant de faire cesser la violation constatée, si le traitement en cause est au nombre de ceux qui intéressent la sûreté de l'Etat ou la défense ou de ceux relevant du chapitre XIII de la présente loi lorsqu'ils sont mis en œuvre pour le compte de l'Etat. Le Premier ministre fait alors connaître à la formation restreinte les suites qu'il a données à cette information au plus tard quinze jours après l'avoir reçue.

« II.-En cas de circonstances exceptionnelles prévues au 1 de l'article 66 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, lorsque la formation restreinte adopte les mesures provisoires prévues aux 1° à 4° du I du présent article, elle informe sans délai de la teneur des mesures prises et de leurs motifs les autres autorités de contrôle concernées, le comité européen de la protection des données et la Commission européenne.

« Lorsque la formation restreinte a pris de telles mesures et qu'elle estime que des mesures définitives doivent être prises, elle met en œuvre les dispositions du 2 de l'article 66 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité.

« III.-Pour les traitements relevant du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, lorsqu'une autorité de contrôle compétente en application du même règlement n'a pas pris de mesure appropriée dans une situation où il est urgent d'intervenir afin de protéger les droits et libertés des personnes concernées, la formation restreinte, saisie par le président de la commission, peut demander au comité européen de la protection des données un avis d'urgence ou une décision contraignante d'urgence dans les conditions et selon les modalités prévues aux 3 et 4 de l'article 66 dudit règlement.

« IV.-En cas d'atteinte grave et immédiate aux droits et libertés mentionnés à l'article 1er de la présente loi, le président de la commission peut en outre demander, par la voie du référé, à la juridiction compétente d'ordonner, le cas échéant sous astreinte, toute mesure nécessaire à la sauvegarde de ces droits et libertés.

« Art. 47.-Les mesures prévues au III de l'article 45 et aux 1° à 7° du I de l'article 46 sont prononcées sur la base d'un rapport établi par l'un des membres de la Commission nationale de l'informatique et des libertés, désigné par le président de celle-ci parmi les membres n'appartenant pas à la formation restreinte. Ce rapport est notifié au responsable de traitement ou à son sous-traitant, qui peut déposer des observations et se faire représenter ou assister. Le rapporteur peut présenter des observations orales à la formation restreinte mais ne prend pas part à ses délibérations. La formation restreinte peut entendre toute personne dont l'audition lui paraît susceptible de contribuer utilement à son information, y compris, à la demande du secrétaire général de la commission, les agents des services de celle-ci.

« La formation restreinte peut rendre publiques les mesures qu'elle prend. Elle peut également ordonner leur insertion dans des publications, journaux et supports qu'elle désigne, aux frais des personnes sanctionnées.

« Sans préjudice des obligations d'information qui incombent au responsable de traitement ou à son sous-traitant en application de l'article 34 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, la formation restreinte peut ordonner que ce responsable ou ce sous-traitant informe individuellement, à ses frais, chacune des personnes concernées de la violation relevée des dispositions de la présente loi ou du règlement précité ainsi que, le cas échéant, de la mesure prononcée.

« Lorsque la formation restreinte a prononcé une sanction pécuniaire devenue définitive avant que le juge pénal ait statué définitivement sur les mêmes faits ou des faits connexes, celui-ci peut ordonner que l'amende administrative s'impute sur l'amende pénale qu'il prononce.

« L'astreinte est liquidée par la formation restreinte, qui en fixe le montant définitif.

« Les sanctions pécuniaires et les astreintes sont recouvrées comme les créances de l'Etat étrangères à l'impôt et au domaine.

« Art. 48.-Lorsqu'un organisme de certification ou un organisme chargé du respect d'un code de conduite a manqué à ses obligations ou n'a pas respecté les dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité ou celles de la présente loi, le président de la Commission nationale de l'informatique et des libertés peut, le cas échéant après mise en demeure, saisir la formation restreinte de la commission, qui peut prononcer, dans les mêmes conditions que celles prévues aux articles 45 à 47, le retrait de l'agrément qui a été délivré à cet organisme. »

II.-A.-Au deuxième alinéa de l'article 226-16 du code pénal, la référence : « I » est remplacée par la référence : « III ».

B.-Le deuxième alinéa de l'article 226-16 du code pénal demeure applicable, dans sa rédaction antérieure à la présente loi, aux faits commis avant l'entrée en vigueur de celle-ci.

Chapitre II : Dispositions relatives à certaines catégories de données

Article 8

L'article 8 de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi modifié :

1° Le I est ainsi rédigé :

« I.-Il est interdit de traiter des données à caractère personnel qui révèlent la prétendue origine raciale ou l'origine ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale d'une personne physique ou de traiter des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique. » ;

2° Le II est ainsi modifié :

a) A la fin du 7°, les mots : « et dans les conditions prévues à l'article 25 de la présente loi » sont supprimés ;

b) Le 8° est ainsi rédigé :

« 8° Les traitements comportant des données concernant la santé justifiés par l'intérêt public et conformes aux dispositions du chapitre IX de la présente loi ; »

c) Sont ajoutés des 9° à 11° ainsi rédigés :

« 9° Les traitements conformes aux règlements types mentionnés au b du 2° du I de l'article 11 mis en œuvre par les employeurs ou les administrations qui portent sur des données biométriques strictement

nécessaires au contrôle de l'accès aux lieux de travail ainsi qu'aux appareils et aux applications utilisés dans le cadre des missions confiées aux salariés, aux agents, aux stagiaires ou aux prestataires ;

« 10° Les traitements portant sur la réutilisation des informations publiques figurant dans les jugements et décisions mentionnés, respectivement, à l'article L. 10 du code de justice administrative et à l'article L. 111-13 du code de l'organisation judiciaire, sous réserve que ces traitements n'aient ni pour objet ni pour effet de permettre la réidentification des personnes concernées ;

« 11° Les traitements nécessaires à la recherche publique au sens de l'article L. 112-1 du code de la recherche, mis en œuvre dans les conditions prévues au 2 de l'article 9 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, après avis motivé et publié de la Commission nationale de l'informatique et des libertés rendu selon les modalités prévues à l'article 28 de la présente loi. » ;

3° Le III est ainsi rédigé :

« III.-N'entrent pas dans le champ de l'interdiction prévue au I les données à caractère personnel mentionnées au même I qui sont appelées à faire l'objet, à bref délai, d'un procédé d'anonymisation préalablement reconnu conforme aux dispositions de la présente loi par la Commission nationale de l'informatique et des libertés. » ;

4° Le IV est ainsi rédigé :

« IV.-De même, ne sont pas soumis à l'interdiction prévue au I les traitements, automatisés ou non, justifiés par l'intérêt public et autorisés dans les conditions prévues au II de l'article 26. »

Titre II : MARGES DE MANŒUVRE PERMISES PAR LE RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL DU 27 AVRIL 2016 RELATIF À LA PROTECTION DES PERSONNES PHYSIQUES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL ET À LA LIBRE CIRCULATION DE CES DONNÉES, ET ABROGEANT LA DIRECTIVE 95/46/CE

Article 9

L'article 2 de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi modifié :

1° Au premier alinéa, après les mots : « traitements automatisés », sont insérés les mots : « en tout ou partie » ;

2° L'avant-dernier alinéa est complété par les mots : «, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ».

…….

Article 16

I.-Le chapitre IX de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi rédigé :

« Chapitre IX

« Traitements de données à caractère personnel dans le domaine de la santé

« Section 1

« Dispositions générales

« Art. 53.-Outre aux dispositions du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, les traitements contenant des données concernant la santé des personnes sont soumis aux dispositions du présent chapitre, à l'exception des catégories de traitements suivantes :

« 1° Les traitements relevant des 1° à 6° du II de l'article 8 ;

« 2° Les traitements permettant d'effectuer des études à partir des données recueillies en application du 6° du même II lorsque ces études sont réalisées par les personnels assurant ce suivi et destinées à leur usage exclusif ;

« 3° Les traitements mis en œuvre aux fins d'assurer le service des prestations ou le contrôle par les organismes chargés de la gestion d'un régime de base d'assurance maladie ainsi que la prise en charge des prestations par les organismes d'assurance maladie complémentaire ;

« 4° Les traitements effectués au sein des établissements de santé par les médecins responsables de l'information médicale, dans les conditions prévues au deuxième alinéa de l'article L. 6113-7 du code de la santé publique ;

« 5° Les traitements effectués par les agences régionales de santé, par l'État et par la personne publique qu'il désigne en application du premier alinéa de l'article L. 6113-8 du même code, dans le cadre défini au même article L. 6113-8.

…..

« Art. 65.-Dans le respect des missions et des pouvoirs de la Commission nationale de l'informatique et des libertés et aux fins de renforcer la bonne application des règles de sécurité et de protection des données, un comité d'audit du système national des données de santé est institué. Ce comité d'audit définit une stratégie d'audit puis une programmation, dont il informe la commission. Il fait réaliser des audits sur l'ensemble des systèmes réunissant, organisant ou mettant à disposition tout ou partie des données du système national des données de santé à des fins de recherche, d'étude ou d'évaluation ainsi que sur les systèmes composant le système national des données de santé.

« Le comité d'audit comprend des représentants des services des ministères chargés de la santé, de la sécurité sociale et de la solidarité, de la Caisse nationale d'assurance maladie, responsable du traitement du système national des données de santé, des autres producteurs de données du système national des données de santé, de l'Institut national des données de santé, ainsi qu'une personne représentant les acteurs privés du domaine de la santé. Des personnalités qualifiées peuvent y être désignées. Le président de la Commission nationale de l'informatique et des libertés, ou son représentant, y assiste en tant qu'observateur.

« Les audits, dont le contenu est défini par le comité d'audit, sont réalisés par des prestataires sélectionnés selon des critères et modalités permettant de disposer de garanties attestant de leur compétence en matière d'audit de systèmes d'information et de leur indépendance à l'égard de l'entité auditée.

« Le prestataire retenu soumet au président du comité d'audit la liste des personnes en charge de chaque audit et les informations permettant de garantir leurs compétences et leur indépendance.

« Les missions d'audit s'exercent sur pièces et sur place. La procédure suivie inclut une phase contradictoire. La communication des données médicales individuelles ne peut se faire que sous l'autorité et en présence d'un médecin, s'agissant des informations qui figurent dans un traitement nécessaire aux fins de la médecine préventive, de la recherche médicale, des diagnostics médicaux, de l'administration de soins ou de traitements, ou de la gestion de service de santé.

« Pour chaque mission diligentée, des échanges ont lieu, si nécessaire, entre les personnes en charge des audits, le président du comité d'audit, le responsable du traitement mentionné au II de l'article L. 1461-1 du code de la santé publique et le président de la Commission nationale de l'informatique et des libertés.

« Si le comité d'audit a connaissance d'informations de nature à révéler des manquements graves en amont ou au cours d'un audit ou en cas d'opposition ou d'obstruction à l'audit, un signalement est adressé sans délai par le président du comité d'audit au président de la Commission nationale de l'informatique et des libertés.

« Chaque mission diligentée établit un rapport relevant notamment les anomalies constatées et les manquements aux règles applicables aux systèmes d'information audités.

« Si la mission constate, à l'issue de l'audit, de graves manquements, elle en informe sans délai le président du comité d'audit, qui informe sans délai le président de la Commission nationale de l'informatique et des libertés et le responsable du traitement mentionné au II de l'article L. 1461-1 du code de la santé publique.

« En cas d'urgence, le directeur général de la Caisse nationale d'assurance maladie peut suspendre temporairement l'accès au système national des données de santé avant le terme de l'audit s'il dispose d'éléments suffisamment préoccupants concernant des manquements graves aux règles précitées. Il doit en informer immédiatement le président du comité et le président de la commission. Le rétablissement de l'accèsne peut se faire qu'avec l'accord de ce dernier au regard des mesures correctives prises par l'entité auditée. Ces dispositions sont sans préjudice des prérogatives propres de la Commission nationale de l'informatique et des libertés.

« Le rapport définitif de chaque mission est transmis au comité d'audit, au président de la Commission nationale de l'informatique et des libertés et au responsable du traitement audité.

« Un décret en Conseil d'Etat, pris après avis de la Commission nationale de l'informatique et des libertés,

précise la composition du comité et définit ses règles de fonctionnement ainsi que les modalités de l'audit. »

Chapitre V : Dispositions particulières relatives aux droits des personnes concernées

Article 19

Au premier alinéa de l'article 7 de la loi n° 78-17 du 6 janvier 1978 précitée, après le mot : « concernée », sont insérés les mots : «, dans les conditions mentionnées au 11) de l'article 4 et à l'article 7 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, ».

Article 20

La section 1 du chapitre II de la loi n° 78-17 du 6 janvier 1978 précitée est complétée par un article 7-1 ainsi rédigé :

« Art. 7-1.-En application du 1 de l'article 8 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, un mineur peut consentir seul à un traitement de données à caractère personnel en ce qui concerne l'offre directe de services de la société de l'information à compter de l'âge de quinze ans.

« Lorsque le mineur est âgé de moins de quinze ans, le traitement n'est licite que si le consentement est donné conjointement par le mineur concerné et le ou les titulaires de l'autorité parentale à l'égard de ce mineur.

« Le responsable de traitement rédige en des termes clairs et simples, aisément compréhensibles par le mineur, les informations et communications relatives au traitement qui le concerne. »

Article 21

I.-L'article 10 de la loi n° 78-17 du 6 janvier 1978 précitée est ainsi rédigé :

« Art. 10.-Aucune décision de justice impliquant une appréciation sur le comportement d'une personne ne peut avoir pour fondement un traitement automatisé de données à caractère personnel destiné à évaluer certains aspects de la personnalité de cette personne.

« Aucune décision produisant des effets juridiques à l'égard d'une personne ou l'affectant de manière significative ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel, y compris le profilage, à l'exception :

« 1° Des cas mentionnés aux a et c du 2 de l'article 22 du règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 précité, sous les réserves mentionnées au 3 du même article 22 et à condition que les règles définissant le traitement ainsi que les principales caractéristiques de sa mise en œuvre soient

communiquées, à l'exception des secrets protégés par la loi, par le responsable de traitement à l'intéressé s'il en fait la demande ;

« 2° Des décisions administratives individuelles prises dans le respect de l'article L. 311-3-1 et du chapitre Ier du titre Ier du livre IV du code des relations entre le public et l'administration, à condition que le traitement ne porte pas sur des données mentionnées au I de l'article 8 de la présente loi. Ces décisions comportent, à peine de nullité, la mention explicite prévue à l'article L. 311-3-1 du code des relations entre le public et l'administration. Pour ces décisions, le responsable de traitement s'assure de la maîtrise du traitement algorithmique et de ses évolutions afin de pouvoir expliquer, en détail et sous une forme intelligible, à la personne concernée la manière dont le traitement a été mis en œuvre à son égard.

« Par dérogation au 2° du présent article, aucune décision par laquelle l'administration se prononce sur un recours administratif mentionné au titre Ier du livre IV du code des relations entre le public et l'administration ne peut être prise sur le seul fondement d'un traitement automatisé de données à caractère personnel. »

II.-Le comité éthique et scientifique mentionné à l'article L. 612-3 du code de l'éducation remet chaque année, à l'issue de la procédure nationale de préinscription et avant le 1er décembre, un rapport au Parlement portant sur le déroulement de cette procédure et sur les modalités d'examen des candidatures par les établissements d'enseignement supérieur. Le comité peut formuler à cette occasion toute proposition afin d'améliorer la transparence de cette procédure.

…….

Fait à Paris, le 20 juin 2018.

Texte 2

Directive 2016/681 du parlement européen et du conseil du 27 avril 2016 relative à l'utilisation des données des dossiers passagers (PNR) pour la prévention et la détection des infractions terroristes et des formes graves de criminalité, ainsi que pour les enquêtes et les poursuites en la matière

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne, et notamment son article 82, paragraphe 1, point d), et son article 87, paragraphe 2, point a),

vu la proposition de la Commission européenne, après transmission du projet d'acte législatif aux parlements nationaux,

vu l'avis du Comité économique et social européen, après consultation du Comité des régions, statuant conformément à la procédure législative ordinaire, considérant ce qui suit:
[…]
ONT ADOPTE LA PRESENTE DIRECTIVE

CHAPITRE I
Dispositions générales

Article premier
Objet et champ d'application

1. La présente directive prévoit:

a) le transfert, par les transporteurs aériens, de données des dossiers des passagers (PNR) de vols extra-UE;

b) le traitement des données visées au point a), notamment leur collecte, leur utilisation et leur conservation par les États membres et leur échange entre les États membres.

2. Les données PNR recueillies conformément à la présente directive ne peuvent être traitées qu'à des fins de prévention et de détection des infractions terroristes et des formes graves de criminalité ainsi que d'enquêtes et de poursuites en la matière, comme prévu à l'article 6, paragraphe 2, points a), b) et c).

Article 2
Application de la présente directive aux vols intra-UE

1. Si un État membre décide d'appliquer la présente directive aux vols intra-UE, il le notifie à la Commission par écrit. Un État membre peut adresser ou révoquer une telle notification à tout moment. La Commission publie cette notification et la révocation éventuelle de celle-ci au Journal officiel de l'Union européenne.

2. Lorsqu'une notification visée au paragraphe 1 est adressée, toutes les dispositions de la présente directive s'appliquent aux vols intra-UE comme s'il s'agissait de vols extra-UE et aux données PNR des vols intra-UE comme s'il s'agissait de données PNR de vols extra-UE.

3. Un État membre peut décider d'appliquer la présente directive uniquement à certains vols intra-UE. Lorsqu'il prend une telle décision, l'État membre sélectionne les vols qu'il juge nécessaires afin de poursuivre les objectifs de la présente directive. L'État membre peut décider à tout moment de modifier la sélection des vols intra-UE.

[...]

CHAPITRE II
Responsabilités des États membres

Article 4
Unité d'informations passagers

1. Chaque État membre met en place ou désigne une autorité compétente en matière de prévention et de détection des infractions terroristes et des formes graves de criminalité, ainsi que d'enquêtes et de poursuites en la matière, ou crée ou désigne une antenne d'une telle autorité, en tant que son UIP.

2. L'UIP est chargée:

a) de la collecte des données PNR auprès des transporteurs aériens, de la conservation et du traitement de ces données, et du transfert de ces données ou du résultat de leur traitement aux autorités compétentes visées à l'article 7;

b) de l'échange à la fois des données PNR et du résultat de leur traitement avec les UIP d'autres États membres et avec Europol, conformément aux articles 9 et 10.

3. Les membres du personnel de l'UIP peuvent être des agents détachés par les autorités compétentes. Les États membres dotent les UIP des ressources adéquates pour l'accomplissement de leurs missions.

4. Deux États membres ou plus (ci-après dénommés «États membres participants») peuvent mettre en place ou désigner une autorité unique en tant qu'UIP. Cette UIP est établie dans l'un des États membres participants et est considérée comme l'UIP nationale de tous les États membres participants. Ces derniers conviennent conjointement des modalités de fonctionnement de l'UIP et respectent les exigences prévues dans la présente directive.

5. Chaque État membre notifie à la Commission la mise en place de son UIP dans un délai d'un mois à compter de cette mise en place et peut, à tout moment, modifier sa notification. La Commission publie cette notification et toute modification y afférente au Journal officiel de l'Union européenne.

Article 5
Délégué à la protection des données au sein de l'UIP

1. L'UIP nomme un délégué à la protection des données chargé de contrôler le traitement des données PNR et de mettre en œuvre les garanties pertinentes.

2. Les États membres dotent les délégués à la protection des données des moyens pour accomplir leurs missions et obligations, conformément au présent article, de manière effective et en toute indépendance.

3. Les États membres veillent à ce que la personne concernée ait le droit de s'adresser au délégué à la protection des données, en sa qualité de point de contact unique, pour toutes les questions relatives au traitement des données PNR la concernant.

Article 6
Traitement des données PNR

1. Les données PNR transférées par les transporteurs aériens sont recueillies par l'UIP de l'État membre concerné comme prévu à l'article 8. Lorsque les données PNR transférées par les transporteurs aériens comportent des données autres que celles énumérées à l'annexe I, l'UIP efface ces données immédiatement et de façon définitive dès leur réception.

2. L'UIP ne traite les données PNR qu'aux fins suivantes:

a) réaliser une évaluation des passagers avant leur arrivée prévue dans l'État membre ou leur départ prévu de celui-ci, afin d'identifier les personnes pour lesquelles est requis un examen plus approfondi par les autorités compétentes visées à l'article 7 et, le cas échéant, par Europol conformément à l'article 10, compte tenu du fait que ces personnes peuvent être impliquées dans une infraction terroriste ou une forme grave de criminalité;

b) répondre, au cas par cas, aux demandes dûment motivées fondées sur des motifs suffisants des autorités compétentes, visant à ce que des données PNR leur soient communiquées et à ce que celles-ci fassent l'objet d'un traitement dans des cas spécifiques, aux fins de la prévention et de la détection d'infractions terroristes ou de formes graves de criminalité, ainsi qu'aux fins d'enquêtes et de poursuites en la matière, et visant à communiquer aux autorités compétentes ou, le cas échéant,

à Europol le résultat de ce traitement; et

c) analyser les données PNR aux fins de mettre à jour ou de définir de nouveaux critères à utiliser pour les évaluations réalisées au titre du paragraphe 3, point b), en vue d'identifier toute personne pouvant être impliquée dans une infraction terroriste ou une forme grave de criminalité.

3. Lorsqu'elle réalise l'évaluation visée au paragraphe 2, point a), l'UIP peut:

a) confronter les données PNR aux bases de données utiles aux fins de la prévention et de la détection des infractions terroristes et des formes graves de criminalité ainsi que des enquêtes et des poursuites en la matière, y compris les bases de données concernant les personnes ou les objets recherchés ou faisant l'objet d'un signalement, conformément aux règles nationales, internationales et de l'Union applicables à de telles bases de données; ou

b) traiter les données PNR au regard de critères préétablis.

4. L'évaluation des passagers avant leur arrivée prévue dans l'État membre ou leur départ prévu de celui-ci effectuée au titre du paragraphe 3, point b), au regard de critères préétablis est réalisée de façon non discriminatoire. Ces critères préétablis doivent être ciblés, proportionnés et spécifiques. Les États membres veillent à ce que ces critères soient fixés et réexaminés à intervalles réguliers par les UIP en coopération avec les autorités compétentes visées à l'article 7. Lesdits critères ne sont en aucun cas fondés sur l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle.

5. Les États membres s'assurent que toute concordance positive obtenue à la suite du traitement automatisé des données PNR effectué au titre du paragraphe 2, point a), est réexaminée individuellement par des moyens non automatisés, afin de vérifier si l'autorité compétente visée à l'article 7 doit prendre des mesures en vertu du droit national.

6. L'UIP d'un État membre transmet, en vue d'un examen plus approfondi, les données PNR des personnes identifiées conformément au paragraphe 2, point a), ou le résultat du traitement de ces données aux autorités compétentes visées à l'article 7 de ce même État membre. Ces transferts ne sont effectués qu'au cas par cas et, en cas de traitement automatisé des données PNR, après un réexamen individuel par des moyens non automatisés.

7. Les États membres veillent à ce que le délégué à la protection des données ait accès à toutes les données traitées par l'UIP. Si le délégué à la protection des données estime que le traitement de certaines données n'était pas licite, le délégué à la protection des données peut renvoyer l'affaire à l'autorité de contrôle nationale.

8. Le stockage, le traitement et l'analyse des données PNR par les UIP sont effectués exclusivement dans un ou des endroits sécurisés situés sur le territoire des États membres.

9. Les conséquences des évaluations des passagers visées au paragraphe 2, point a), du présent article ne compromettent pas le droit d'entrée des personnes jouissant du droit de l'Union à la libre circulation sur le territoire de l'État membre concerné prévu dans la directive 2004/38/CE du Parlement européen et du Conseil. En outre, lorsque des évaluations sont réalisées pour des vols intra-UE entre des États membres auxquels s'applique le règlement (CE) no 562/2006 du Parlement européen et du Conseil, les conséquences de ces évaluations doivent respecter ledit règlement.

[...]

Article 9
Échange d'informations entre États membres

1. Les États membres veillent à ce que, en ce qui concerne les personnes identifiées par une UIP conformément à l'article 6, paragraphe 2, toutes les données PNR pertinentes et nécessaires ou le résultat du traitement de ces données soient transmis par ladite UIP aux UIP correspondantes des autres États

membres. Les UIP des États membres destinataires transmettent les informations reçues à leurs autorités compétentes, conformément à l'article 6, paragraphe 6.

2. L'UIP d'un État membre a le droit de demander, si nécessaire, à l'UIP de tout autre État membre de lui communiquer des données PNR qui sont conservées dans sa base de données et qui n'ont pas encore été dépersonnalisées par le masquage d'éléments des données au titre de l'article 12, paragraphe 2, ainsi que, si nécessaire, le résultat de tout traitement de ces données, si celui-ci a déjà été réalisé en vertu de l'article 6, paragraphe 2, point a). Cette demande est dûment motivée. Elle peut être fondée sur un quelconque élément de ces données ou sur une combinaison de tels éléments, selon ce que l'UIP requérante estime nécessaire dans un cas spécifique de prévention ou de détection d'infractions terroristes ou de formes graves de criminalité, ou d'enquêtes ou de poursuites en la matière. Les UIP transmettent dès que possible les informations demandées. Si les données demandées ont été dépersonnalisées par le masquage d'éléments des données conformément à l'article 12, paragraphe 2, l'UIP ne transmet l'intégralité des données PNR que lorsqu'il existe des motifs raisonnables de croire que cela est nécessaire aux fins visées à l'article 6, paragraphe 2, point b), et uniquement si elle y est autorisée par une autorité visée à l'article 12, paragraphe 3, point b).

3. Les autorités compétentes d'un État membre ne peuvent demander directement à l'UIP d'un autre État membre de leur communiquer des données PNR qui sont conservées dans sa base de données que lorsque cela est nécessaire dans les cas d'urgence et dans les conditions fixées au paragraphe 2. Les demandes des autorités compétentes sont motivées. Une copie de la demande est toujours envoyée à l'UIP de l'État membre requérant. Dans tous les autres cas, les autorités compétentes canalisent leurs demandes par l'intermédiaire de l'UIP de leur propre État membre.

4. À titre exceptionnel, lorsque l'accès à des données PNR est nécessaire pour répondre à une menace précise et réelle liée à des infractions terroristes ou à des formes graves de criminalité, l'UIP d'un État membre a le droit de demander à ce que l'UIP d'un autre État membre obtienne des données PNR conformément à l'article 8, paragraphe 5, et les communique à l'UIP requérante.

5. L'échange d'informations au titre du présent article peut avoir lieu par l'intermédiaire de n'importe quel canal de coopération existant entre les autorités compétentes des États membres. La langue utilisée pour la demande et l'échange d'informations est celle applicable au canal utilisé. Lorsqu'ils procèdent aux notifications conformément à l'article 4, paragraphe 5, les États membres communiquent également à la Commission les coordonnées des points de contact auxquels les demandes peuvent être adressées en cas d'urgence. La Commission communique lesdites coordonnées aux États membres.

Article 10
Conditions d'accès aux données PNR par Europol

1. Europol est habilité à demander aux UIP des États membres des données PNR ou le résultat du traitement de ces données dans les limites de ses compétences et pour l'accomplissement de ses missions.

2. Europol peut présenter, au cas par cas, à l'UIP de tout État membre par l'intermédiaire de l'unité nationale Europol, une demande électronique dûment motivée de transmission de données PNR spécifiques ou du résultat du traitement de ces données. Europol peut présenter cette demande lorsque cela est strictement nécessaire au soutien et au renforcement de l'action des États membres en vue de prévenir ou de détecter une infraction terroriste spécifique ou une forme grave de criminalité spécifique, ou de mener des enquêtes en la matière, dans la mesure où ladite infraction ou ladite forme de criminalité relève de la compétence d'Europol en vertu de la décision 2009/371/JAI. Cette demande énonce les motifs raisonnables sur lesquels se fonde Europol pour estimer que la transmission des données PNR ou du résultat du traitement de ces données contribuera de manière substantielle à la prévention ou à la détection de l'infraction concernée, ou à des enquêtes en la matière.

3. Europol informe le délégué à la protection des données nommé conformément à l'article 28 de la décision 2009/371/JAI de chaque échange d'informations au titre du présent article.

4. Les échanges d'information au titre du présent article ont lieu par l'intermédiaire de SIENA et conformément à la décision 2009/371/JAI. La langue utilisée pour la demande et l'échange d'informations est celle applicable à SIENA.

Article 11
Transfert de données vers des pays tiers

1. Un État membre peut transférer à un pays tiers des données PNR et le résultat du traitement de ces données, qui sont conservés par l'UIP conformément à l'article 12, uniquement au cas par cas et si:

a) les conditions prévues à l'article 13 de la décision-cadre 2008/977/JAI sont remplies;

b) le transfert est nécessaire aux fins de la présente directive visées à l'article 1er, paragraphe 2;

c) le pays tiers n'accepte de transférer les données à un autre pays tiers que lorsque cela est strictement nécessaire aux fins de la présente directive visées à l'article 1er, paragraphe 2, et uniquement avec l'accord exprès dudit État membre; et

d) les mêmes conditions que celles prévues à l'article 9, paragraphe 2, sont remplies.

2. Nonobstant l'article 13, paragraphe 2, de la décision-cadre 2008/977/JAI, les transferts de données PNR sans l'accord préalable de l'État membre dont les données ont été obtenues, ne sont autorisés que dans des circonstances exceptionnelles et uniquement si:

a) ces transferts sont essentiels pour répondre à une menace précise et réelle liée à une infraction terroriste ou à une forme grave de criminalité dans un État membre ou un pays tiers; et

b) l'accord préalable ne peut pas être obtenu en temps utile.

L'autorité chargée de donner son accord est informée sans retard et le transfert est dûment enregistré et soumis à une vérification ex post.

3. Les États membres ne transfèrent des données PNR aux autorités compétentes de pays tiers que dans des conditions compatibles avec la présente directive et après avoir obtenu l'assurance que l'utilisation que les destinataires entendent faire de ces données PNR respecte ces conditions et garanties.

4. Chaque fois qu'un État membre transfère des données PNR en vertu du présent article, le délégué à la protection des données de l'UIP de cet État membre en est informé.

Article 12
Période de conservation et dépersonnalisation des données

1. Les États membres veillent à ce que les données PNR fournies par les transporteurs aériens à l'UIP y soient conservées dans une base de données pendant une période de cinq ans suivant leur transfert à l'UIP de l'État membre sur le territoire duquel se situe le point d'arrivée ou de départ du vol.

2. À l'expiration d'une période de six mois suivant le transfert des données PNR visé au paragraphe 1, toutes les données PNR sont dépersonnalisées par le masquage des éléments des données suivants qui pourraient servir à identifier directement le passager auquel se rapportent les données PNR:

a) le(s) nom(s), y compris les noms d'autres passagers mentionnés dans le PNR, ainsi que le nombre de passagers voyageant ensemble figurant dans le PNR;

b) l'adresse et les coordonnées;

c) des informations sur tous les modes de paiement, y compris l'adresse de facturation, dans la mesure où y figurent des informations pouvant servir à identifier directement le passager auquel le PNR se rapporte ou toute autre personne;

d) les informations «grands voyageurs»;

e) les remarques générales, dans la mesure où elles comportent des informations qui pourraient servir à identifier directement le passager auquel le PNR se rapporte; et

f) toute donnée API qui a été recueillie.

3. À l'expiration de la période de six mois visée au paragraphe 2, la communication de l'intégralité des données PNR n'est autorisée que:

a) lorsqu'il existe des motifs raisonnables de croire qu'elle est nécessaire aux fins visées à l'article 6, paragraphe 2, point b); et

b) lorsqu'elle a été approuvée par:

i) une autorité judiciaire; ou

ii) une autre autorité nationale compétente en vertu du droit national pour vérifier si les conditions de communication sont remplies, sous réserve que le délégué à la protection des données de l'UIP en soit informé et procède à un examen ex post.

4. Les États membres veillent à ce que les données PNR soient effacées de manière définitive à l'issue de la période visée au paragraphe 1. Cette obligation s'applique sans préjudice des cas où des données PNR spécifiques ont été transférées à une autorité compétente et sont utilisées dans le cadre de cas spécifiques à des fins de prévention, de détection d'infractions terroristes ou de formes graves de criminalité ou d'enquêtes ou de poursuites en la matière, auquel cas la conservation de ces données par l'autorité compétente est régie par le droit national.

5. Le résultat du traitement visé à l'article 6, paragraphe 2, point a), n'est conservé par l'UIP que le temps nécessaire pour informer les autorités compétentes et, conformément à l'article 9, paragraphe 1, pour informer les UIP des autres États membres de l'existence d'une concordance positive. Lorsque, à la suite du réexamen individuel par des moyens non automatisés visé à l'article 6, paragraphe 5, le résultat du traitement automatisé s'est révélé négatif, il peut néanmoins être archivé tant que les données de base n'ont pas été effacées au titre du paragraphe 4 du présent article, de manière à éviter de futures «fausses» concordances positives.

Article 13
Protection des données à caractère personnel

1. Chaque État membre veille à ce que, pour tout traitement de données à caractère personnel effectué au titre de la présente directive, chaque passager dispose du même droit à la protection de ses données à caractère personnel, des mêmes droits d'accès, de rectification, d'effacement et de limitation, et droits à réparation et à un recours juridictionnel prévus dans le droit de l'Union et le droit national et en application des articles 17, 18, 19 et 20 de la décision-cadre 2008/977/JAI. Lesdits articles sont par conséquent applicables.

2. Chaque État membre veille à ce que les dispositions adoptées en droit national en application des articles 21 et 22 de la décision-cadre 2008/977/JAI concernant la confidentialité du traitement et la sécurité des données s'appliquent également à tous les traitements de données à caractère personnel effectués en vertu de la présente directive.

3. La présente directive est sans préjudice de l'applicabilité de la directive 95/46/CE du Parlement européen et du Conseil au traitement des données à caractère personnel par les transporteurs aériens, en particulier en ce qui concerne leurs obligations de prendre des mesures techniques et organisationnelles appropriées pour protéger la sécurité et la confidentialité des données à caractère personnel.

4. Les États membres interdisent le traitement des données PNR qui révèlent l'origine raciale ou ethnique d'une personne, ses opinions politiques, sa religion ou ses convictions philosophiques, son appartenance à un syndicat, son état de santé, sa vie sexuelle ou son orientation sexuelle. Dans l'hypothèse où l'UIP reçoit des données PNR révélant de telles informations, elle les efface immédiatement.

5. Les États membres veillent à ce que l'UIP conserve une trace documentaire relative à tous les systèmes et procédures de traitement sous leur responsabilité. Cette documentation comprend au minimum:

a) le nom et les coordonnées de l'organisation et du personnel chargés du traitement des données PNR au sein de l'UIP et les différents niveaux d'autorisation d'accès;

b) les demandes formulées par les autorités compétentes et les UIP d'autres États membres;

c) toutes les demandes et tous les transferts de données PNR vers un pays tiers.

L'UIP met toute la documentation à la disposition de l'autorité de contrôle nationale, à la demande de celle-ci.

6. Les États membres veillent à ce que l'UIP tienne des registres au moins pour les opérations de traitement suivantes: la collecte, la consultation, la communication et l'effacement. Les registres des opérations de consultation et de communication indiquent, en particulier, la finalité, la date et l'heure de ces opérations et, dans la mesure du possible, l'identité de la personne qui a consulté ou communiqué les données PNR, ainsi que l'identité des destinataires de ces données. Les registres sont utilisés uniquement à des fins de vérification et d'autocontrôle, de garantie de l'intégrité et de la sécurité des données ou d'audit. L'UIP met les registres à la disposition de l'autorité de contrôle nationale, à la demande de celle-ci.

Ces registres sont conservés pendant cinq ans.

7. Les États membres veillent à ce que leur UIP mette en œuvre des mesures et des procédures techniques et organisationnelles appropriées afin de garantir un niveau élevé de sécurité adapté aux risques présentés par le traitement et à la nature des données PNR.

8. Lorsqu'une atteinte aux données à caractère personnel est susceptible d'entraîner un risque élevé pour la protection des données à caractère personnel ou d'affecter négativement la vie privée de la personne concernée, les États membres veillent à ce que l'UIP fasse part de cette atteinte à la personne concernée et à l'autorité de contrôle nationale sans retard injustifié.

[...]

Article 15
Autorité de contrôle nationale

1. Chaque État membre prévoit que l'autorité de contrôle nationale visée à l'article 25 de la décision-cadre 2008/977/JAI est chargée de fournir des conseils sur l'application, sur son territoire, des dispositions adoptées par les États membres en vertu de la présente directive et de surveiller l'application de celles-ci. L'article 25 de ladite décision-cadre s'applique.

2. Ces autorités de contrôle nationales exercent les activités au titre du paragraphe 1 en ayant en vue la protection des droits fondamentaux en matière de traitement des données à caractère personnel.

3. Chaque autorité de contrôle nationale:

a) traite les réclamations introduites par toute personne concernée, enquête sur l'affaire et informe la personne concernée de l'état d'avancement du dossier et de l'issue de la réclamation dans un délai raisonnable;

b) vérifie la licéité du traitement des données, effectue des enquêtes, des inspections et des audits conformément au droit national, de sa propre initiative ou en se fondant sur une réclamation visée au point a).

4. Chaque autorité de contrôle nationale conseille, sur demande, toute personne concernée quant à l'exercice des droits que lui confèrent les dispositions adoptées en vertu de la présente directive.

[...]

Texte 3

Mémento à l'usage du directeur d'établissement de santé
Connaître vos risques pour mieux y faire face - Cybersécurité édition 2017

En Bref

Les systèmes d'information sont des outils de partage et d'échange incontournables, au bénéfice des patients, des professionnels et du système de santé. Il est donc crucial de garantir leur sécurité pour maintenir la confiance des patients dans le système de santé et celle des professionnels dans les outils qu'ils utilisent chaque jour. Il convient pour cela d'installer une véritable démarche de gestion du risque numérique. Celle-ci vise à traiter ces risques, c'est-à-dire les réduire, les éviter, les partager ou les accepter, en étant pleinement conscient de ses vulnérabilités et ayant apprécié tout l'impact d'un potentiel accident de sécurité.
Il s'agit également de prendre toute la mesure du véritable patrimoine d'informations que représentent les données du système d'information parmi lesquelles les données de santé sont les plus sensibles. Le nouveau règlement européen pour la protection des données définit ce que sont ces « données à caractère personnel concernant la santé » et il établit tout un cadre de protection qu'il convient d'appliquer à partir du 25 mai 2018, en particulier en désignant un délégué à la protection des données personnelles.
La protection du système d'information et de ses données est un travail de tous les jours et qui concerne tout le monde, un travail par lequel on doit pouvoir garantir la disponibilité des données, leur intégrité, leur confidentialité, et apporter la preuve des seuls usages autorisés. À ce titre, la notion d'hébergement des données de santé requiert le respect d'une réglementation stricte et précise.
Si le premier pas vers la réduction des risques est une prise de conscience collective, le soutien de la Direction est le principal facteur clé de succès et de constance dans l'action. Celle-ci doit, d'ailleurs, rester réaliste pour ne pas décourager les différentes parties prenantes. Elle doit s'exprimer dans le cadre d'une véritable politique de sécurité de l'établissement, élaborée par un responsable sécurité du système d'information, dûment mandaté.
Dans ce travail, l'établissement de santé trouve ses grandes orientations au sein même des référentiels nationaux produits dans le cadre de la politique générale de sécurité des systèmes d'information de santé (PGSSI-S) élaborée par l'ASIP Santé, dans l'atteinte des prérequis du programme Hôpital Numérique, et dans le plan d'action sur la sécurité des systèmes d'information.
Enfin, grâce au tout nouveau dispositif de signalement des incidents de sécurité des systèmes d'information de santé, mis en place depuis le 1er octobre 2017, il dispose désormais d'un accompagnement opérationnel face à un incident grave de sécurité de son système d'information.

1 - L'univers numérique qui entoure le patient s'accroît sans cesse

Dans la perspective de la mise en oeuvre de la stratégie nationale de santé, les technologies numériques constituent un levier majeur pour la modernisation de notre système de santé.
Les programmes nationaux aussi bien que les initiatives locales conduisent à une transition numérique qu'il convient d'accompagner le mieux possible pour en tirer tous les bénéfices sans s'exposer à de nouveaux risques.
La transition numérique touche tous les secteurs d'activité, aussi bien ceux en lien direct avec la production des soins, que ceux liés aux fonctions support nécessaires au bon fonctionnement de l'hôpital

■ Le monde numérique envahit notre quotidien

Les risques les plus élevés concernent aujourd'hui les données. Elles représentent un véritable patrimoine, de plus en plus convoité. Il devient donc essentiel d'identifier les vulnérabilités qui concernent votre établissement afin de réduire les risques numériques auxquels ces données peuvent être exposées.

■ Face à un risque évoluant sans cesse, la prise de conscience est essentielle

Il est important de gérer le risque comme un élément vivant et évoluant sans cesse. Le but de ce guide est de vous aider à en percevoir tous les enjeux et à vous orienter dans la mise en place des outils de pilotage, les actions d'audit et de suivi. Le but de la
gestion des risques doit rester la protection du patient, de vos équipes, et de vous-même.

Les programmes nationaux et les orientations de politique publique soutiennent la transition numérique dans le secteur de la santé, citons à titre d'exemple :
– Le programme Hôpital Numérique
– Les projets Territoire de soins numériques
– La mise en place des Groupements Hospitaliers de Territoire dans le cadre de la loi de modernisation de notre système de santé

2 - Les systèmes d'information vous font-ils prendre des risques inconsidérés ?

Les systèmes d'information sont des outils de partage et d'échanges incontournables, au bénéfice des patients, des professionnels et du système de santé. Il est donc crucial de garantir leur sécurité pour maintenir la confiance des patients dans le système de santé et celle des professionnels dans les outils qu'ils utilisent chaque jour.
La progression réelle du Dossier Patient Informatisé (DPI) dans les établissements de santé montre que les soins s'appuient de plus en plus sur le système d'information (SI).
La standardisation des technologies fait que la barrière séparant les équipements biomédicaux du reste du réseau informatique tend à disparaître. Le pilotage de ces équipements et les données traitées se trouvent donc dépendants de la sécurité globale du Système d'Information (SI).
L'utilisation des technologies de l'information améliore la qualité des soins, les conditions de travail… mais elle est aussi porteuse de nouveaux risques et de nouvelles contraintes.
Ainsi, la mise en place du DPI doit être accompagnée d'une garantie de disponibilité adaptée aux exigences fixées par l'établissement lui-même et la réglementation.
Un dysfonctionnement du SI entraînant un mélange de résultats de biologie peut avoir un impact fort sur une prise en charge d'un patient.

3 – L'engagement dans une démarche de gestion des risques numériques est une réelle opportunité de mieux accompagner l'évolution de son établissement

■ Soutenir la politique de sécurité du système d'information devient aussi une exigence
La politique de sécurité ne se limite pas à la protection contre la perte, l'indisponibilité ou la divulgation de données personnelles médicales ou administratives, elle permet de créer un espace de confiance entre les professionnels et les patients et elle est un levier essentiel de l'amélioration de la qualité des soins. Il est donc de la responsabilité du management des établissements de santé (directeur, directeur des soins, directeur des ressources humaines, présidents des commissions médicales d'établissements) de la promouvoir

4 – L'incident de sécurité : l'éviter, c'est avant tout connaître et réduire ses vulnérabilités, identifier les situations dangereuses et apprendre à réagir face à elles

Tout l'enjeu d'une démarche de gestion des risques est de les traiter, c'est-à-dire, de les réduire, les éviter, les partager ou les accepter. Pour cela il convient d'agir simultanément sur 4 niveaux :
1. Connaître les dangers auxquels on est exposé
2. Comprendre ses principales vulnérabilités et chercher à les réduire
3. Essayer de détecter au plus tôt toute situation dangereuse
4. S'organiser pour gérer l'incident de sécurité

La cartographie des risques est la pierre angulaire de tout plan d'action sécurité du système d'information. Elle vise à définir toutes les actions nécessaires pour parvenir à un niveau de risque résiduel qui puisse être accepté en toute connaissance de cause, au bon niveau de décision. Elle s'applique toujours sur un périmètre d'activité parfaitement défini. Tout établissement de santé doit disposer d'une cartographie des risques liés à son système d'information (cf. les prérequis du programme Hôpital Numérique).

5 – Le nouveau règlement européen donne une définition des données de santé et fixe le cadre de leur protection

Le nouveau règlement européen définit, dans son article 4, ce que sont les « données à caractère personnel concernant la santé » : il s'agit de "données à caractère personnel relatives à la santé physique ou mentale

d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne".
Il précise qu'elles devraient comprendre "toute information concernant, par exemple, une maladie, un handicap, un risque de maladie, un dossier médical, un traitement clinique ou l'état physiologique ou biomédical de la personne concernée, indépendamment de sa source, qu'elle provienne par exemple d'un médecin ou d'un autre professionnel de la santé, d'un hôpital, d'un dispositif médical ou d'un test de diagnostic in vitro".
Il définit aussi les "données génétiques", "relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé", et les données biométriques, "résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique".
■ Les données de santé sont, par essence, des données dites « sensibles »
Et pour les protéger la réforme de la protection des données poursuit 3 objectifs :
- Renforcer les droits des personnes, notamment par la création d'un droit à la portabilité des données personnelles et de dispositions propres aux personnes mineures ;
- Responsabiliser les acteurs traitant des données (responsables de traitement et sous-traitants) ;
- Crédibiliser la régulation grâce à une coopération renforcée entre les autorités de protection des données.

6 – La protection des données est fondée sur la responsabilisation des acteurs et le rôle donné au consentement des personnes.

Qu'il s'agisse de ses personnels, de ses patients ou de ses partenaires, les données personnelles en possession de l'établissement sont protégées par le droit français et européen qui garantit la protection de la vie privée.
■ Le règlement impose la mise à disposition d'une information claire, intelligible et aisément accessible aux personnes concernées par les traitements de données.
Alors que la réglementation nationale reposait jusqu'alors, en grande partie, sur la notion de « formalités préalables » (déclaration, autorisations), le règlement européen repose lui sur une logique de conformité, dont les acteurs sont responsables, sous le contrôle et avec l'accompagnement du régulateur.
Les utilisateurs doivent être informés de l'usage de leurs données et doivent en principe donner leur accord pour le traitement de leurs données, ou doivent pouvoir s'y opposer. La charge de la preuve du consentement incombe au responsable de traitement. Il est primordial pour les établissements de garantir leur confidentialité, une perte de donnée pouvant représenter des risques majeurs tant au niveau de l'image de l'établissement qu'au niveau du préjudice pour la victime du vol de donnée.
La conséquence de la responsabilisation accrue des acteurs est la suppression des obligations déclaratives dès lors que les traitements ne constituent pas un risque pour la vie privée des personnes. Quant aux traitements soumis actuellement à autorisation, le régime d'autorisation pourra être maintenu par le droit national (par exemple en matière de santé) ou sera remplacé par une nouvelle procédure centrée sur l'étude d'impact sur la vie privée.

7 – L'hébergement de données de santé s'inscrit dans un cadre réglementaire spécifique

Les modalités d'hébergement de données de santé à caractère personnel sont encadrées par l'article L.1111-8 du code de la santé publique :
■ Toute personne physique ou morale qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social ou médico-social pour le compte d'un tiers, doit être agréée à cet effet.
■ L'hébergement exige une information claire et préalable de la personne concernée par les données de santé hébergées et une possibilité pour celle-ci de s'y opposer pour motif légitime.
L'ordonnance n° 2017-27 du 12 janvier 2017 relative à l'hébergement de données de santé à caractère personnel a modifié l'article L.1111-8 du code de la santé publique en distinguant explicitement trois grandes catégories de services d'hébergement de données de santé :
■ l'hébergement de données de santé sur support papier, qui doit être réalisé par un hébergeur agréé par le Ministre de la Culture (procédure déjà existante – cf. décret 2011-246) ;
■ l'hébergement de données de santé sur support numérique dans le cadre d'un service d'archivage électronique, qui doit être réalisé par un hébergeur agréé par le Ministre de la Culture dans des conditions

définies par décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés (CNIL) et des conseils des ordres des professions de santé ;
■ l'hébergement de données de santé sur support numérique (hors cas d'un service d'archivage électronique) qui doit être réalisé par un hébergeur certifié dans des conditions définies par décret en Conseil d'État pris après avis de la Commission nationale de l'informatique et des libertés (CNIL) et des conseils des ordres des professions de santé.

Dès 2018 : La certification « Hébergeur de données de santé »
■ Le nouveau dispositif pour l'hébergement de données de santé sur support numérique est défini par la DSSIS et l'ASIP Santé. Il est validé par un comité de pilotage qui réunit des représentants institutionnels (Ministère de la Santé, ANSSI, CNIL, Fédérations hospitalières, Ordres, etc.) et des représentants d'industriels.
A partir de 2018, pour toute nouvelle demande, la qualité d'hébergeur de données de santé reposera sur une évaluation de conformité à un référentiel de certification, délivrée par un organisme certificateur accrédité par le COFRAC et choisi par l'hébergeur. Deux types de certificats seront délivrés aux hébergeurs :
■ Un certificat « hébergeur d'infrastructure physique » pour les activités de mise à disposition de locaux d'hébergement physique et d'infrastructure matérielle ;
■ Un certificat « hébergeur infogéreur » pour les activités de mise à disposition d'infrastructure virtuelle, de mise à disposition de plateforme logicielle, d'infogérance et de sauvegarde externalisée.

8 – Disponibilité, intégrité, confidentialité et preuve

Une donnée ne devient une véritable information que si l'on y accède facilement, en permanence, de façon maîtrisée, si on la comprend et si on est en mesure de lui faire confiance. Quatre caractéristiques sont indispensables pour cela :
■ Disponibilité : un niveau contextualisé selon les finalités d'usage des données
La disponibilité des systèmes numériques permet à l'information d'être accessible et utilisable par la personne autorisée à l'endroit et à l'instant où elle en a besoin.
■ Intégrité : une fiabilité maximale des données de santé
Les données ne doivent pouvoir être modifiées que suivant des processus clairement définis et par des personnes clairement identifiées. Plus la fiabilité de l'information est critique, plus ces critères sont à prendre en compte.
■ Confidentialité : un accès modulable aux données de santé
L'information ne doit être accessible qu'aux personnes autorisées. En amont, la réflexion sur la gestion des droits et des accès est essentielle. Seules les personnes ayant besoin de l'information doivent pouvoir y accéder. Plus cette information est « sensible » plus le nombre de personnes doit être réduit.
■ Preuve : une conservation de traces à valeur de preuve
La preuve permet l'investigation en cas de dysfonctionnement et d'incidents. Il s'agit clairement de conserver les traces de l'état et des mouvements de l'information.
La réforme de la protection des données rend cette preuve particulièrement importante car elle peut permettre de prouver qu'un contrôle sur l'utilisation des données est en place.

9 – Hôpital Numérique : poser un socle de sécurité incontournable

Le programme Hôpital numérique, lancé en 2011 et piloté par la Direction générale de l'offre de soins (DGOS), a pour ambition d'amener l'ensemble des établissements de santé à un palier de maturité de leur système d'information permettant :
■ le partage et l'échange d'informations au sein des établissements
■ l'amélioration significative de la qualité, de la sécurité des soins, et la performance dans des domaines fonctionnels prioritaires autour de la production de soins.
Trois grands objectifs sont poursuivis, en matière de sécurité, par le programme Hôpital Numérique, chacun correspond à un domaine de prérequis, chaque domaine possédant des indicateurs cibles à atteindre.
1. Pouvoir rattacher la bonne information, au bon patient, au bon endroit (prérequis P1 – Identité / mouvement)
- Utiliser des référentiels uniques d'identité patient, de séjours et de mouvements pour la majorité des applications
- Mettre en oeuvre une identitovigilance opérationnelle pour assurer la sécurité du patient liée aux soins

- Décrire la structure d'organisation de l'établissement et l'actualiser
2. En toutes circonstances (prérequis P2 – Fiabilité, disponibilité)
- Disposer d'un plan de reprise d'activité formalisé pour assurer la continuité de service
- S'engager sur la disponibilité des applications
- Savoir gérer les situations de pannes au moyen de procédures dégradées
3. Et en toute confiance (prérequis P3 – Confidentialité, preuve)
- Évaluer les situations à risques et définir une politique de sécurité pour les prévenir et les maîtriser
- Définir les bonnes pratiques dans l'utilisation du SI afin de garantir la confidentialité auprès du patient et demander un engagement à les respecter
- Définir qui accède à quoi et être en mesure de le vérifier

10 – L'organisation collective : premier pas vers la réduction des risques

Le soutien de la Direction est le principal facteur clé de succès.
La Direction doit promouvoir, soutenir la démarche et en rappeler, si nécessaire, les enjeux. Il faut transformer l'image de la sécurité vue comme une contrainte sans apport sur la qualité et la sécurité des soins. Seule la Direction peut soutenir ce message de la sécurité créatrice de confiance sur le système d'information.
■ La gestion des risques liés au numérique ne passe pas uniquement par la mise en place de solutions techniques. C'est surtout une organisation prenant en compte les éléments de risque qui est la clef d'un pilotage réussi.
Cela est renforcé par la normalisation des obligations réglementaires poussant les directions à mettre en place une gouvernance clairement définie et des objectifs stratégiques et opérationnels associés.
La sécurité est l'affaire de tous les utilisateurs.
Ceux-ci doivent respecter les règles d'usage du Système d'Information, même si bien souvent ces règles sont vues comme une contrainte sans intérêt opérationnel.
Pour accepter cette contrainte, il faut communiquer vers les utilisateurs et les convaincre des enjeux sous-jacents.
Le soutien de la Direction est alors d'autant plus important et précieux que les chantiers les plus complexes ont un impact sur l'organisation de l'établissement et les aspects opérationnels des services.
C'est le cas, par exemple, de la gestion des identités et des accès des utilisateurs au système d'information ou de la mise en place d'un plan de continuité d'activité (en cas de panne grave du système d'information).

Texte 4

Ce qu'il faut savoir sur l'analyse d'impact relative à la protection des données (AIPD)

19 février 2018

L'article 35 du RGPD prévoit la conduite d'une analyse d'impact relative à la protection des données (AIPD - Data Protection Impact Assessment), lorsqu'un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

✔ Qu'est-ce qu'une analyse d'impact relative à la protection des données (AIPD) ?

L'analyse d'impact (AIPD) est un outil important pour la responsabilisation des organismes : elle les aide non seulement à construire des traitements de données respectueux de la vie privée, mais aussi à démontrer leur conformité au Règlement général sur la protection des données (RGPD). Elle est obligatoire pour les traitements susceptibles d'engendrer des risques élevés.

Une fois la description du traitement réalisée, l'AIPD repose sur deux piliers :

- l'évaluation, de nature plus juridique, de la nécessité et de la proportionnalité concernant les principes et droits fondamentaux (finalité, données et durées de conservation, information et droits des personnes, etc.) non négociables, qui sont fixés par la loi et doivent être respectés, quelle que soit la nature, gravité et vraisemblance des risques ;
- l'étude, de nature plus technique, des risques sur la sécurité des données (accès non autorisé, modification et disparition de données, et leurs impacts potentiels sur la vie privée), qui permet de déterminer les mesures techniques et d'organisation pour protéger les données.

On note qu'analyse d'impact relative à la protection des données, AIPD (Data Protection Impact Assessment, terme retenu dans le RGPD) et PIA (Privacy Impact Assessment, terme plus commun utilisé dans d'autres régions du monde) sont synonymes.

✔ Qu'est-ce qu'un risque sur la vie privée ?

Un « risque sur la vie privée » est un scénario décrivant :

- un événement redouté (accès non autorisé, modification non désirée ou disparition de données, et ses impacts potentiels sur les droits et libertés des personnes) ;
- toutes les menaces qui permettraient qu'il survienne.

Il est estimé en termes de gravité et de vraisemblance. La gravité doit être évaluée pour les personnes concernées, et non pour l'organisme.

Par exemple, un salarié soudoyé par un concurrent pourrait lui envoyer le fichier des adresses email des clients par courrier électronique. Si cela se produisait, les clients pourraient ensuite être sollicités et avoir un sentiment d'atteinte à la vie privée, des ennuis personnels ou professionnels, etc. Du point de vue « informatique et libertés », ce risque pourrait être estimé comme peu grave (conséquences peu importantes) et très vraisemblable (dans la mesure où ce scénario s'est déjà produit) par l'entreprise.

✔ Une analyse d'impact peut-elle porter sur un ou plusieurs traitements ?

Oui : Une AIPD peut concerner un seul traitement ou un ensemble de traitements similaires.

Par exemple :

- des collectivités qui mettent chacune en place un système de vidéosurveillance similaire pourraient effectuer une seule analyse qui porterait sur ce système bien que celui-ci soit ultérieurement mis en œuvre par des responsables de traitements distincts ;
- un opérateur ferroviaire (responsable de traitement unique) pourrait effectuer une seule analyse d'impact sur le dispositif de la surveillance vidéo déployé dans plusieurs gares.

En tant que bonne pratique, une AIPD peut également être menée par le fournisseur d'un produit matériel ou logiciel, pour évaluer l'impact sur la protection des données de son produit. Les différents responsables de traitement qui utilisent ensuite ce produit doivent mener leurs propres AIPD mais, le cas échéant, ceux-ci peuvent être alimentés par l'AIPD du fournisseur du produit.

✔ Quand est-ce qu'une analyse d'impact n'est pas obligatoire ?

Une AIPD n'est pas nécessaire dans les cas suivants :

- quand le traitement ne présente pas de risque élevé pour les droits et libertés des personnes concernées ;
- lorsque la nature, la portée, le contexte et les finalités du traitement envisagé sont très similaires à un traitement pour lequel une AIPD a déjà été menée ;
- quand le traitement répond à une obligation légale ou est nécessaire à l'exercice d'une mission de service public (art 6.1.c 6.1.e), sous réserve que les conditions suivantes soient remplies :

a) qu'il ait une base juridique dans le droit de l'UE ou le droit de l'État membre ;

b) que ce droit règlemente cette opération de traitement ;

c) et qu'une AIPD ait déjà été menée lors de l'adoption de cette base juridique ;

- quand le traitement correspond à une exception déterminée par la CNIL conformément à l'article 35(5). La CNIL adoptera courant 2018 la liste de ces exceptions.

✔ Quand est-ce qu'une analyse d'impact est obligatoire ?

Une AIPD doit obligatoirement être mené quand le traitement est « susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées ».

Ainsi, généralement, les traitements qui remplissent au moins deux des critères suivants doivent faire l'objet d'une analyse d'impact :

- évaluation/scoring (y compris le profilage) ;
- décision automatique avec effet légal ou similaire ;
- surveillance systématique ;
- collecte de données sensibles ;
- collecte de données personnelles à large échelle ;
- croisement de données ;
- personnes vulnérables (patients, personnes âgées, enfants, etc.) ;
- usage innovant (utilisation d'une nouvelle technologie) ;
- exclusion du bénéfice d'un droit/contrat.

Exemple : une entreprise met en place un contrôle de l'activité de ses salariés, ce traitement remplit le critère de la surveillance systématique et celui des données concernant des personnes vulnérables donc la réalisation d'une AIPD sera nécessaire.

✔ À quel moment faut-il mener une analyse d'impact ?

L'AIPD doit être menée avant la mise en œuvre du traitement. Il doit être démarré le plus en amont possible et sera mise à jour tout au long du cycle de vie du traitement.

Il est également recommandé de revoir une AIPD de manière régulière pour s'assurer que le niveau de risque reste acceptable.

✔ Faut-il mener une analyse d'impact pour les traitements déjà mis en œuvre au 25 mai 2018 ?

Une étude d'impact ne sera pas exigée pour :

- les traitements qui ont fait l'objet d'une formalité préalable auprès de la CNIL avant le 25 mai 2018
- les traitements qui ont été consignés au registre d'un correspondant « informatique et libertés ».

Cette dispense d'obligation de réaliser une AIPD, pour les traitements en cours régulièrement mis en œuvre, sera limitée à une période de 3 ans : à l'issue de ce délai, les responsables de traitement devront avoir effectué une telle étude si le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes

En revanche, l'étude d'impact devra être réalisée, sans attendre l'issue de ce délai de trois ans, dans tous les autres cas, dès lors que le traitement présente un risque élevé :

- pour tout nouveau traitement mis en œuvre après le 25 mai 2018 ;
- pour les traitements antérieurs n'ayant pas fait l'objet de formalités préalables auprès de la CNIL ;
- pour les traitements, antérieurs au 25 mai et qui ont été dispensés d'étude d'impact en raison de l'accomplissement d'une formalité préalable auprès de la CNIL, mais qui font l'objet d'une modification significative.

La réalisation d'une AIPD constitue, dans tous les cas, une bonne pratique facilitant la démarche de mise en conformité avec les conditions de fond prévues par le RGPD.

✔ Qui intervient dans la réalisation d'une analyse d'impact ?

Le responsable de traitement est tenu par l'obligation de s'assurer de la conformité de son traitement au RGPD.

S'il a désigné un délégué à la protection des données, il lui demande conseil et le charge de vérifier l'exécution de l'AIPD.

Si un sous-traitant intervient dans le traitement, il doit fournir son aide et les informations nécessaires à la réalisation de l'AIPD.

Le responsable de traitement devrait également demander l'avis des personnes concernées (par le biais d'une enquête, d'un sondage, d'une question formelle aux représentants du personnel), ou le justifier sinon.

Idéalement, les métiers (maîtrise d'ouvrage), les équipes chargées de la mise en œuvre (maîtrise d'œuvre), et la personne chargée de la sécurité des systèmes d'information devraient également participer au processus de réalisation de l'AIPD et à sa validation.

✔ Comment fait-on une analyse d'impact, existe-t-il une méthode pour faire une analyse d'impact?

Un AIPD contient à minima :

- une description systématique des opérations de traitement envisagées et les finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement;
- une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités;
- une évaluation des risques sur les droits et libertés des personnes concernées et ;
- les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du règlement.

Pour ce faire, plusieurs méthodes sont utilisables. Le responsable de traitement est libre de choisir sa méthode. Mais quelle que soit la méthode, celle-ci devrait respecter les critères définis dans l'annexe 2 des lignes directrices du G29.

Les guides AIPD de la CNIL (en cours de révision) décrivent la méthode suivante :

1. délimiter et décrire le contexte du (des) traitement(s) considéré(s) ;
2. analyser les mesures garantissant le respect des principes fondamentaux : la proportionnalité et la nécessité du traitement, et la protection des droits des personnes concernées ;
3. apprécier les risques sur la vie privée liés à la sécurité des données et vérifier qu'ils sont convenablement traités ;

4. formaliser la validation du PIA au regard des éléments précédents ou bien décider de réviser les étapes précédentes.

✔ Faut-il communiquer l'analyse d'impact ?

Il n'y a aucune obligation de publication. Toutefois, l'AIPD peut aboutir à la production d'un rapport ou d'un résumé, pouvant être partagé, publié, communiqué. Cette bonne pratique contribue à améliorer la confiance entre les parties prenantes.

En outre, l'AIPD doit être communiquée à la CNIL, dans son intégralité, en cas de consultation préalable (cf. article 36).

✔ Quand faut-il transmettre son analyse d'impact à la CNIL ?

L'AIPD doit être transmise à la CNIL dans les cas suivants :

- s'il apparait que le niveau de risque résiduel reste élevé (cas où la CNIL doit être consultée) ;
- quand la législation nationale d'un État membre l'exige ;
- en cas de contrôle par la CNIL.

✔ Quel est le montant des sanctions prévues par le règlement en cas de manquements aux dispositions relatives aux analyses d'impact ?

Le montant des amendes peut s'élever jusqu'à 10 000 000 d'euros ou, dans le cas d'une entreprise, jusqu'à 2 % du chiffre d'affaires annuel mondial total de l'exercice précédent, le montant le plus élevé étant retenu (art. 83(4)(a)).

Texte 5

Devenir délégué à la protection des données - 23 mai 2017 – www.cnil.fr.

Le délégué à la protection des données est au cœur du nouveau règlement européen. Les lignes directrices adoptées dans leur version finale le 5 avril 2017 par le G29, groupe des « CNIL » européennes, clarifient et illustrent d'exemples concrets le nouveau cadre juridique applicable en mai 2018 dans toute l'Europe.

La CNIL organise des journées d'information sur le RGPD, à destination des futurs délégués à la protection des données (DPO) ou tout professionnel en charge de la protection des données au sein de son organisme.

Le règlement européen sur la protection des données pose les règles applicables à la désignation, à la fonction et aux missions du délégué, sous peine de sanctions.

Les lignes directrices du G29 ont pour objectif d'accompagner les responsables de traitement et les sous-traitants dans la mise en place de la fonction de délégué ainsi que d'assister ces délégués dans l'exercice de leurs missions. Elles contiennent des recommandations et des bonnes pratiques permettant aux professionnels de se préparer et de mettre en œuvre leurs obligations avec flexibilité et pragmatisme.

À la suite d'un appel à commentaires, les lignes directrices ont été enrichies et adoptées par le G29 dans leur version finale le 5 avril 2017.

À retenir

Le délégué est chargé de mettre en œuvre la conformité au règlement européen sur la protection des données au sein de l'organisme qui l'a désigné s'agissant de l'ensemble des traitements mis en œuvre par cet organisme.

Sa désignation est obligatoire dans certains cas. Un délégué, interne ou externe, peut être désigné pour plusieurs organismes sous conditions.

Pour garantir l'effectivité de ses missions, le délégué :

- doit disposer de qualités professionnelles et de connaissances spécifiques,
- doit bénéficier de moyens matériels et organisationnels, des ressources et du positionnement lui permettant d'exercer ses missions.

✔ Dans quels cas un organisme doit-il obligatoirement désigner un délégué à la protection des données ?

La désignation d'un délégué est obligatoire pour :

1. Les autorités ou les organismes publics,
2. Les organismes dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle,
3. Les organismes dont les activités de base les amènent à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations pénales et infractions.

En dehors des cas de désignation obligatoire, la désignation d'un délégué à la protection des données est encouragée par les membres du G29. Elle permet en effet de confier à un expert l'identification et la coordination des actions à mener en matière de protection des données personnelles.

Les organismes peuvent désigner un délégué interne ou externe à leur structure. Le délégué à la protection des données peut par ailleurs être mutualisé c'est-à-dire désigné pour plusieurs organismes sous certaines conditions. Par exemple, lorsqu'un délégué est désigné pour un groupe d'entreprises, il doit être facilement joignable à partir de chaque lieu d'établissement. Il doit en effet être en mesure de communiquer efficacement avec les personnes concernées et de coopérer avec l'autorité de contrôle.

Les lignes directrices du G29 clarifient les critères posés par le règlement, notamment les notions d'autorité ou d'organisme public, d'activités de base, de grande échelle et de suivi régulier et systématique.

✔ Quelles différences entre le CIL et le délégué ?

Le délégué à la protection des données est le successeur naturel du CIL. Leurs statuts sont similaires.

Toutefois, le règlement précise les exigences portant sur le délégué s'agissant de ses qualifications (qualités professionnelles, connaissances spécialisées du droit et des pratiques en matière de protection de données) et de sa formation continue (entretien de ses connaissances spécialisées).

Ses prérogatives et missions sont renforcées, s'agissant en particulier de son rôle de conseil et de sensibilisation sur les nouvelles obligations du règlement (notamment en matière de conseil et, le cas échéant, de vérification de l'exécution des analyses d'impact).

Par ailleurs, les organismes doivent fournir à leur délégué les ressources nécessaires à ses missions (notamment l'associer d'une manière appropriée et en temps utile à toutes les questions relatives à la protection des données, lui donner accès aux données ou encore lui permettre de se former).

Enfin, contrairement au CIL dont la désignation est facultative, celle du délégué est obligatoire dans certains cas (voir question ci-dessus).

✔ Qui peut être délégué ?

Le délégué doit être désigné « sur la base de ses qualités professionnelles et, en particulier de ses connaissances spécialisées du droit et des pratiques en matière de protection des données, et de sa capacité à accomplir [ses] missions » (article 37.5 du règlement européen).

La personne qui a vocation à devenir délégué à la protection doit pouvoir réunir les qualités et compétences suivantes :

- l'aptitude à communiquer efficacement et à exercer ses fonctions et missions en toute indépendance. Le délégué ne doit pas avoir de conflit d'intérêts avec ses autres missions. Cela signifie qu'il ne peut occuper des fonctions, au sein de l'organisme, qui le conduise à déterminer les finalités et les moyens d'un traitement (éviter d'être « juge et partie ») (voir la question spécifique sur le conflit d'intérêts).
- une expertise en matière de législations et pratiques en matière de protection des données, acquise notamment grâce à une formation continue. Le niveau d'expertise doit être adapté à l'activité de l'organisme et à la sensibilité des traitements mis en œuvre.
- une bonne connaissance du secteur d'activité et de l'organisation de l'organisme et en particulier des opérations de traitement, des systèmes d'information et des besoins de l'organisme en matière de protection et de sécurité des données.
- un positionnement efficace en interne pour être en capacité de faire directement rapport au niveau le plus élevé de l'organisme et également d'animer un réseau de relais au sein des filiales d'un groupe par exemple et/ou une équipe d'experts en interne (expert informatique, juriste, expert en communication, traducteur, etc.).

Il n'existe donc pas de profil type du délégué qui peut être une personne issue du domaine technique, juridique ou autre. Une étude menée pour la CNIL en 2015 a en effet montré que les CIL proviennent de domaines d'expertise très variés (profil technique à 47 %, profil juridique à 19 % et profil administratif à 10 %).

✔ Dans quel cas peut-il exister un conflit d'intérêts ?

La fonction de délégué peut être exercée à temps plein ou à temps partiel. Dans ce dernier cas, le délégué ne peut occuper des fonctions au sein de l'organisme le conduisant à déterminer les finalités et les moyens d'un traitement (éviter d'être « juge et partie »). L'existence d'un conflit d'intérêts est donc appréciée au cas par cas.

A titre d'exemple, les fonctions suivantes sont susceptibles de donner lieu à un conflit d'intérêts : secrétaire général, directeur général des services, directeur général, directeur opérationnel, directeur financier, médecin-chef, responsable du département marketing, responsable des ressources humaines ou responsable du service informatique, mais également d'autres rôles à un niveau inférieur de la structure organisationnelle si ces fonctions ou rôles supposent la détermination des finalités et des moyens du traitement. Un conflit d'intérêt peut également exister par exemple si un délégué sur la base d'un contrat de service représente l'organisme devant les tribunaux dans des dossiers impliquant des sujets en matière de données à caractère personnel.

- ✔ Quelle est la responsabilité du délégué à la protection des données ?

La responsabilité du délégué est similaire à celle du CIL. Les lignes directrices du G29 précisent que le délégué n'est pas responsable en cas de non-respect du règlement. Ce dernier établit clairement que c'est le responsable du traitement (RT) ou le sous-traitant (ST) qui est tenu de s'assurer et d'être en mesure de démontrer que le traitement est effectué conformément à ses dispositions (article 24.1 du règlement). Le respect de la protection des données relève donc de la responsabilité du RT ou du ST.

Il n'est pas possible de transférer au Délégué, par délégation de pouvoir, la responsabilité incombant au responsable de traitement ou les obligations propres du sous-traitant. En effet, cela reviendrait à conférer au Délégué un pouvoir décisionnel sur la finalité et les moyens du traitement ce qui serait constitutif d'un conflit d'intérêts contraire à l'article 38.6 du règlement européen.

- ✔ Quelle protection pour le délégué à la protection des données ?

Le délégué doit agir d'une manière indépendante et bénéficier d'une protection suffisante dans l'exercice de ses missions. Le règlement prévoit ainsi que le délégué ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions.

Les sanctions ne sont pas possibles si elles sont imposées en raison de l'exercice par le délégué de sa fonction. A titre d'exemple, si un délégué estime qu'un traitement est susceptible d'engendrer un risque élevé et conseille au responsable de traitement de procéder à une analyse d'impact, et si le responsable de traitement n'est pas d'accord avec l'analyse du délégué, ce dernier ne peut être relevé de sa fonction pour avoir formulé ce conseil.

Les sanctions peuvent prendre des formes diverses et peuvent être directes ou indirectes. Il peut s'agir, par exemple, d'absence de promotion ou de retard dans la promotion, de freins à l'avancement de carrière ou du refus de l'octroi d'avantages dont bénéficient d'autres employés. Il n'est pas nécessaire que ces sanctions soient effectivement mises en œuvre, une simple menace suffit pour autant qu'elle soit utilisée pour sanctionner le délégué pour des motifs liés à ses activités en tant que délégué.

A noter toutefois que le délégué n'est pas un salarié protégé au sens du code du travail français. Dès lors, il pourrait être licencié légitimement, comme tout autre employé, pour des motifs autres que l'exercice de ses missions de délégué (par exemple, en cas de vol, de harcèlement physique, moral ou sexuel ou fautes graves similaires).

- ✔ Où le délégué doit-il être localisé ?

Afin de permettre que le délégué soit joignable, il est recommandé qu'il soit localisé dans un Etat membre de l'Union européenne.

Toutefois, dans certaines situations où l'organisme n'a pas d'établissement dans l'Union européenne, un délégué peut être en mesure d'exercer ses missions plus efficacement s'il est localisé en dehors de l'Union européenne.

✔ Quelles sont les missions du délégué à la protection des données ?

« Chef d'orchestre » de la conformité en matière de protection des données au sein de son organisme, le délégué à la protection des données est principalement chargé :

- d'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que leurs employés ;
- de contrôler le respect du règlement et du droit national en matière de protection des données ;
- de conseiller l'organisme sur la réalisation d'une analyse d'impact relative à la protection des données et d'en vérifier l'exécution ;
- de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci (voir question ci-après).

Les missions du délégué couvrent l'ensemble des traitements mis en œuvre par l'organisme qui l'a désigné.

Les lignes directrices détaillent le rôle du délégué en matière de contrôle, d'analyse d'impact et de tenue du registre des activités de traitement.

Elles indiquent que le délégué n'est pas personnellement responsable en cas de non-conformité de son organisme avec le règlement.

✔ Que signifie coopérer avec l'autorité de contrôle et être le point de contact avec celle-ci ?

L'une des missions du délégué est d'être le point de contact pour l'autorité de protection des données et de coopérer avec elle. À ce titre, le délégué doit faciliter l'accès par l'autorité aux documents et informations dans le cadre de l'exercice des missions et des pouvoirs de cette autorité (par exemple lors d'échanges avec l'autorité dans l'instruction d'une plainte, ou en cas besoin de précisions sur un projet en cours ou bien encore, dans le cadre d'un contrôle de l'autorité).

L'obligation de confidentialité ou de secret professionnel du délégué ne doit pas l'empêcher de demander conseil à l'autorité sur tout sujet, si nécessaire.

✔ Quels sont les moyens d'action du délégué à la protection des données ?

Le délégué doit bénéficier du soutien de l'organisme qui le désigne. L'organisme devra en particulier :

- s'assurer de son implication dans toutes les questions relatives à la protection des données (exemple : communication interne et externe sur sa désignation)
- lui fournir les ressources nécessaires à la réalisation de ses tâches (exemples : formation, temps nécessaire, ressources financières, équipe)
- lui permettre d'agir de manière indépendante (exemples : positionnement hiérarchique adéquat, absence de sanction pour l'exercice de ses missions)
- lui faciliter l'accès aux données et aux opérations de traitement (exemple : accès facilité aux autres services de l'organisme)
- veiller à l'absence de conflit d'intérêts.

Les lignes directrices fournissent des exemples concrets et opérationnels des ressources nécessaires à adapter selon la taille, la structure et l'activité de l'organisme. S'agissant du conflit d'intérêts, le délégué ne peut occuper des fonctions, au sein de l'organisme, qui le conduise à déterminer les finalités et les moyens d'un traitement (ne pas être juge et partie). L'existence d'un conflit d'intérêt est appréciée au cas par cas. Les lignes directrices indiquent les fonctions qui, en règle générale, sont susceptibles de conduire à une situation de conflit d'intérêts.

✔ Comment désigner un délégué à la protection des données ?

Vous pouvez dès maintenant désigner un délégué en ligne.

Sa désignation prendra officiellement effet le lendemain de sa désignation en ligne.

✔ Comment organiser la fonction de délégué à la protection des données ?

En vue de la préparation à la fonction de délégué, il est recommandé de :

- s'approprier les nouvelles obligations imposées par le règlement européen, en s'appuyant notamment sur les lignes directrices du G29 (portabilité, autorité chef de file, analyse d'impact).
- confier au futur délégué les missions suivantes :
  - réaliser l'inventaire des traitements de données personnelles mis en œuvre ;
  - évaluer ses pratiques et mettre en place des procédures (audits, privacy by design, notification des violations de données, gestion des réclamations et des plaintes, etc.) ;
  - identifier les risques associés aux opérations de traitement ;
  - établir une politique de protection des données personnelles ;
  - sensibiliser les opérationnels et la direction sur les nouvelles obligations.