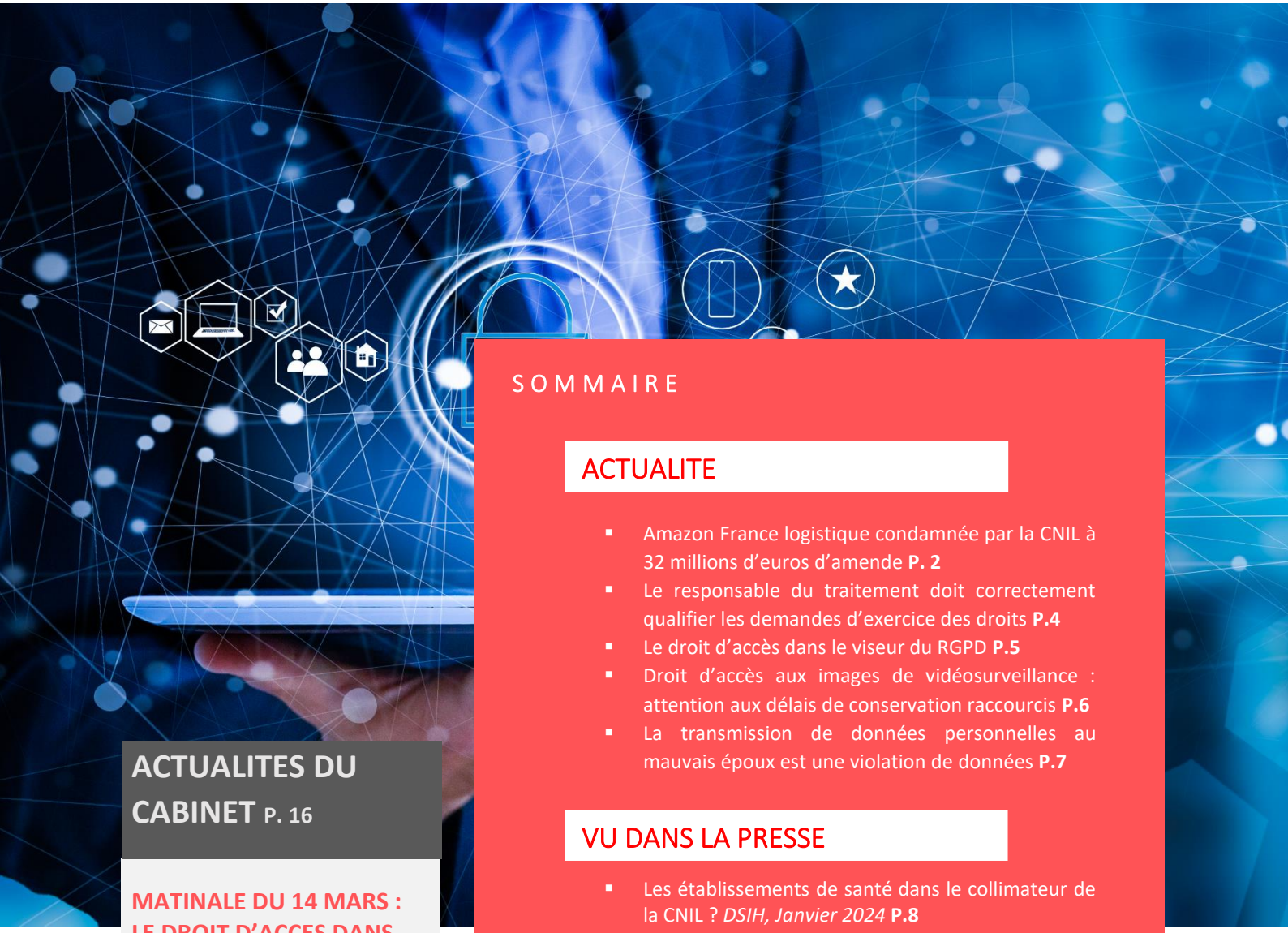
NEWSLETTER RGPD/DATA

NUMÉRO 60 ● 2024



SOMMAIRE

ACTUALITE

VU DANS LA PRESSE

ACTUALITES DU CABINET P. 16

MATINALE DU 14 MARS : LE DROIT D'ACCES DANS L'ŒIL DU CYCLONE

FORMATION A LA PREPARATION A LA CERTIFICATION « DPO ».
DATE SUR DEMANDE

AMAZON FRANCE LOGISTIQUE CONDAMNEE PAR LA CNIL A 32 MILLIONS D'EUROS D'AMENDE

Le 23 janvier 2024, la CNIL a sanctionné la société Amazon France Logistique à une amende administrative de 32 millions d'euros pour avoir mis en place un système de surveillance de l'activité et des performances des salariés « excessivement intrusif » et avoir procédé à des opérations de vidéosurveillance sans information préalable.

À la suite de la publication d'articles de presse visant les pratiques mises en œuvre par Amazon France Logistique, dans le cadre de son activité de gestion des entrepôts du groupe Amazon en France, la CNIL a procédé à des contrôles dans les locaux de cette société.

Le traitement d'un grand volume de données personnelles concernant les salariés

Les contrôles de la CNIL ont mis en lumière l'usage, par Amazon France Logistique, de scanners, confiés à ses salariés, afin de mesurer en temps réel l'exécution de certaines tâches. Les données personnelles issues de ces scanners étaient traitées pour deux ensembles de finalités :

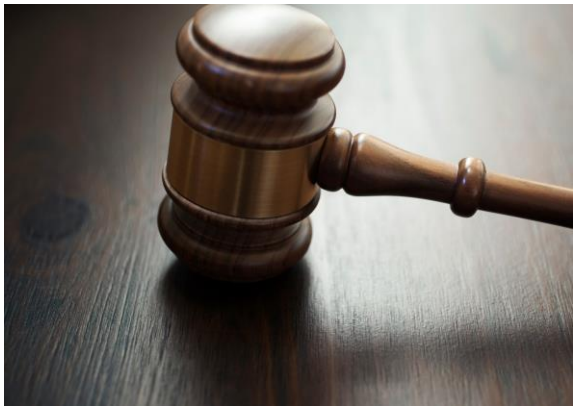
- la gestion des commandes en temps réel, d'une part ; et
- la planification du travail et l'évaluation des performances des salariés, d'autre part.

L'utilisation des scanners, par les salariés d'Amazon France Logistique, donne ainsi lieu à la production de données bruts, issues de 43 « indicateurs ».

Un défaut de base légale

Parmi les 43 « indicateurs » utilisés par Amazon France Logistique, 2 ont particulièrement retenu l'attention de la CNIL :

- L'indicateur « Slow Machine Gun », lié à la vitesse d'exécution d'une tâche, destiné à identifier le nombre de secondes écoulées entre deux tâches. Si cet intervalle est trop court, il déclenche une alerte signalant une potentielle erreur que le salarié pourrait avoir commise dans la précipitation.
- L'indicateur « Idle Times », qui enregistre les périodes d'inactivité du salarié (dues à un problème technique rencontré par le salarié, ou bien à une pause excessivement longue) :
- supérieures à 10 minutes ; et
- inférieures à 10 minutes, lors de certains moments « critiques » de la journée.



Pour la CNIL :

- L'indicateur « Slow Machine Gun » révèle un comportement du salarié dans la façon dont il exécute ses tâches directes et est de nature à exercer sur lui une surveillance continue des délais associés à chacune de ses actions sur des tâches directes, avec une mesure de l'ordre de la seconde. Compte tenu de son caractère particulièrement intrusif, cet indicateur excède ce qui est nécessaire aux fins des intérêts légitimes d'Amazon France Logistique, de sorte que le traitement de cet indicateur ne repose sur aucune base légale.
- L'indicateur « Idle Times » présente, selon la CNIL, un caractère intrusif important puisqu'il contraint le salarié à être en mesure de justifier de tout temps considéré comme non productif, son traitement est donc également dépourvu de base légale.

Une atteinte au principe de minimisation s'agissant de l'ensemble des données

Amazon France Logistique conserve l'ensemble des données brutes issues des indicateurs pendant une durée de 31 jours, afin notamment d'être en mesure de répartir les salariés aux différents postes en fonction de leur niveau de performance sur cette période, et de leur fournir des conseils/supports si les indicateurs sont en baisse.

La CNIL « *ne met pas en cause le besoin opérationnel consistant à pouvoir repérer en temps réel tout besoin de conseil/support ou de réaffectation, puis celui consistant à pouvoir déterminer le meilleur conseil ou support, ou la meilleure réaffectation en disposant de données sur les compétences et performances relatives de ses salariés* ». La poursuite de ces finalités peut, pour la CNIL, en revanche, la CNIL considère que le traitement de l'ensemble de ces données, pendant 31 jours, porte atteinte au principe de minimisation ; des statistiques hebdomadaires, moins fines, par ailleurs réalisées par l'entreprise, auraient permis d'atteindre les finalités du traitement. Elle a également considéré que le traitement de ces 41 indicateurs, aux fins d'évaluation du salarié, en raison de l'atteinte disproportionnée qu'il portait aux droits des salariés, est dépourvu de base légale.

Une amende de 32 millions d'euros

En raison des manquements exposés ci-dessus, ainsi que de manquements aux obligations de sécurité et d'information liées à la mise en œuvre d'un dispositif de vidéosurveillance, la CNIL a prononcé une amende d'un montant de 32 millions d'euros à l'encontre d'Amazon France Logistique, équivalant à 3% de son chiffre d'affaires de 2021.

Source : ici

LE RESPONSABLE DU TRAITEMENT DOIT CORRECTEMENT QUALIFIER LES DEMANDES D'EXERCICE DES DROITS

L'autorité de contrôle autrichienne a sanctionné un responsable du traitement qui a interprété une demande de droit d'accès comme une demande d'effacement.

Une personne concernée a exercé auprès d'une banque son droit d'accès. N'ayant obtenu aucune réponse dans le délai d'un mois, la personne concernée a déposé une plainte.

Invité par l'autorité de contrôle autrichienne à répondre à la demande d'exercice des droits, le responsable du traitement a informé la personne concernée que sa demande de droit d'effacement avait bien été prise en compte et que ses données avaient été effacées.

Après avoir vérifié que la demande portait bien sur le droit d'accès et non le droit à l'effacement, l'autorité de contrôle a considéré que le responsable du traitement avait commis une « *erreur de droit* » en « *partant du principe que la personne concernée souhaitait que ses données soient effacées* ».

La banque justifiait son erreur en indiquant que, comme le client souhaitait mettre fin à la relation contractuelle, elle avait cru, à tort, que sa demande portait sur la suppression de ses données.

Rappelant le droit d'accès est la « clé de voute » permettant à la personne concernée de « vérifier la licéité du traitement et, en outre, de faire valoir ses autres droits », l'autorité de contrôle a considéré que le responsable du traitement avait violé le droit d'accès de la personne concernée :

- en ne traitant pas la demande dans un délai d'un mois ;
- en n'informant pas la personne des mesures prises, et, enfin ;
- en effaçant des données personnelles après avoir reçu une demande d'accès.

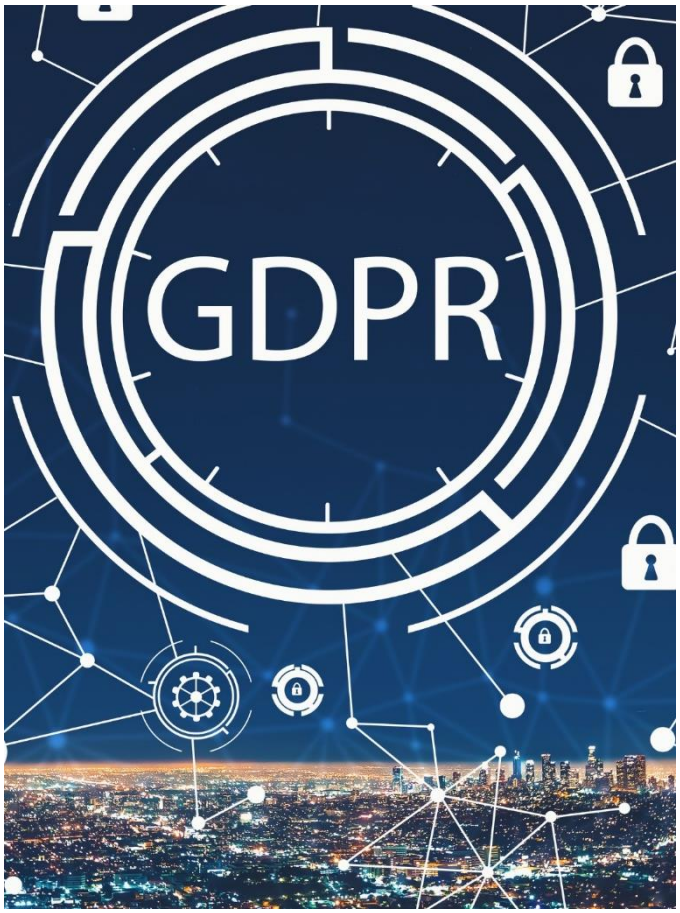
Compte tenu de ce qui précède, l'autorité de contrôle autrichienne a infligé au responsable du traitement une amende de plus de 10 000 € pour avoir violé les articles 12 et 15 du RGPD.

Source : ici

LE DROIT D'ACCES DANS LE VISEUR DU CEPD

Le CEPD a annoncé que le thème de sa troisième action coordonnée 2024 est le droit d'accès.

Créé en 2020, l'action coordonnée vise à « faciliter [entre les autorités de contrôle] des actions conjointes […], allant de la sensibilisation et la collecte d'informations conjointes à des opérations répressives ciblées et coordonnées et des enquêtes conjointes ».



Dans une communication du 17 octobre 2023, confirmée le 17 janvier 2024, le CEPD a annoncé que la prochaine action coordonnée porterait sur « *32* ». Le droit d'accès, consacré à l'article 15 du RGPD, permet notamment à la personne concernée d'obtenir du responsable du traitement la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès auxdites données à caractère personnel ainsi qu'à un certain nombre d'informations en lien avec leur traitement.

Dans son article annonçant les thématiques prioritaires de contrôle 2024, la CNIL a d'ailleurs confirmé qu'en vertu de cette action coordonnée, elle allait, tout comme ses homologues, procéder à des « *vérifications sur les conditions de mise en œuvre du droit d'accès* ».

Dans l'attente de la communication de détails sur cette action coordonnée, il convient, dès à présent, de s'interroger sur la conformité de votre procédure de gestion des demandes de droit d'accès.

Source : ici

DROIT D'ACCES AUX IMAGES DE VIDEOSURVEILLANCE : ATTENTION AUX DELAIS DE CONSERVATION RACCOURCIS

L'autorité de contrôle grecque a sanctionné une banque pour n'avoir pas correctement répondu à une demande d'exercice des droits, aboutissant à une suppression des données.

Le client d'une banque, victime d'une usurpation d'identité, a exercé son droit d'accès auprès de celle-ci afin d'obtenir les « fichiers journaux » de ses connexions sur son application bancaire, mais également une copie des images prises par les caméras de vidéosurveillance lors de sa visite dans son agence bancaire.

La banque, confrontée à un retard de traitement de la demande de droit d'accès « *en raison de sa charge de travail* », a décidé de prolonger le délai de traitement de la demande d'un mois (sans prévenir le client).

Or, conformément à la politique de durée de conservation de la banque, les images des caméras de vidéosurveillance sont conservées pendant une durée de 45 jours, puis automatiquement supprimées.

Ainsi, au moment où la banque a souhaité répondre à la personne concernée, elle n'était plus en mesure de fournir les images des caméras de vidéosurveillance, qui avaient été supprimées conformément à la politique de durée de conservation.

Le client a donc déposé une plainte auprès de l'autorité de contrôle grecque, qui a considéré que la banque « *n'avait pas agi en temps utile* ».

Constatant que la demande de droit d'accès avait été exercée avant la suppression des images des caméras de vidéosurveillance, l'autorité de contrôle a considéré que la banque avait enfreint :

- L'article 5§1a du RGPD (relatif au principe de licéité du traitement), en détruisant les images des caméras de vidéosurveillance après l'exercice du droit d'accès par la personne ;
- L'article 15 du RGPD (relatif au droit d'accès), en ne fournissant pas la copie de l'enregistrement vidéo sollicitée et en n'informant pas la personne concernée de la prolongation du délai de réponse.

Compte tenu de ce qui précède, l'autorité de contrôle grecque a infligé à la banque une amende de 10 000 €.

Source : ici

LA TRANSMISSION DE DONNEES PERSONNELLES AU MAUVAIS EPOUX EST UNE VIOLATION DE DONNEES

L'autorité de contrôle grecque a sanctionné une banque pour avoir transmis des données personnelles à l'épouse de son client.

Le client d'une banque a déposé une plainte auprès de l'autorité de contrôle grecque après avoir découvert que la banque avait communiqué à son épouse des données le concernant, et plus précisément des informations relatives aux transactions bancaires réalisées sur son compte bancaire personnel. Cette transmission a, selon le mari, « *sérieusement perturbée la paix familiale et sa relation avec son épouse* ».

Un traitement illicite

L'autorité de contrôle grecque a estimé que la banque avait traité de manière illicite les données personnelles du mari en transmettant des données relatives à ses transactions bancaires à un tiers, en violation du principe de licéité et de confidentialité des données (article 5§1, points a) et f) du RGPD) ;

Une absence de notification contestable

L'autorité de contrôle a ensuite estimé que la banque avait manqué à son obligation de notification de l'incident à l'autorité de contrôle (article 33 du RGPD).

Si la banque a « *pris des mesures organisationnelles appropriées* » et « *établi des politiques pertinentes pour gérer les violations de données* », l'autorité de contrôle a considéré que la banque n'avait pas appliqué ces mesures, au cas d'espèce.

En effet, si la banque avait bien enregistré l'incident dans le registre violations de données, elle a considéré que les risques pour les droits et libertés du client sont « négligeables » car, selon elle, (1) la violation ne concernait qu'une seule personne, (2) les données avaient été transférées à une seule personne, (3) le destinataire était marié avec la personne concernée et (4) l'impact pour la personne concernée se limitait à une perte de confiance dans le couple et de l'anxiété.

L'autorité de contrôle a reproché à la banque (1) d'avoir tardé à enquêter sur la violation dans un premier temps, (2) d'avoir considérablement tardé à qualifier l'incident comme une violation de données et (3) d'avoir sous-estimé les conséquences de la violation pour la personne concernée.

Compte tenu des manquements constatés, l'autorité de contrôle a infligé à la banque une amende de 10 000 €.

Source : ici

LES ETABLISSEMENTS DE SANTE DANS LE COLLIMATEUR DE LA CNIL

La CNIL a diligenté treize contrôles entre 2020 et 2024 auprès d'établissements de santé [1]. Résultat : les mesures mises en œuvre par ces derniers pour garantir la sécurité du dossier patient informatisé (DPI) sont insuffisantes. Plusieurs d'entre eux ont fait l'objet de mise en demeure de prendre des mesures adaptées. La CNIL prévoit des mesures correctrices contre d'autres établissements en 2024.

La sensibilité du dossier patient informatisé (DPI)

Le dossier patient informatisé (DPI) est le fichier dans lequel est centralisé l'ensemble des données de santé des patients pris en charge au sein d'un établissement de santé. Il permet aux professionnels de santé de cet établissement d'accéder facilement à leurs informations médicales.

Compte tenu du volume et de la sensibilité des données qu'il contient, le DPI doit, selon la CNIL, faire l'objet de « *mesures de sécurité renforcées* ».

Des mesures de sécurité souvent inadaptées

Les mesures prises par les établissements de santé concernés ne sont pas satisfaisantes car la politique de gestion des habilitations est trop souvent inadaptée, en ce qu'elle permet notamment à des catégories de personnel desdits établissements de santé d'accéder à des données dont elles n'ont pas besoin de connaître.

Les mesures de sécurité préconisées par la CNIL

Les établissements de santé devraient, selon la CNIL, mettre en place les trois mesures suivantes :

- Sécuriser les accès au DPI grâce à une politique d'authentification robuste, qui devrait prévoir a minima (i) un identifiant unique par utilisateur et interdire les comptes partagés entre plusieurs utilisateurs et (ii) le recours à des mots de passe suffisamment complexes.
- Implémenter des règles d'habilitation répondant à l'exigence selon laquelle un professionnel de santé ou un agent ne peut accéder qu'aux données dont il a besoin de connaître.
  Selon la CNIL, cette deuxième mesure passe par le respect des deux critères suivants :
  - Le critère du « métier exercé » : un agent responsable de l'accueil des patients dans la structure de soins ne doit accéder « qu'au dossier administratif du patient et non aux données médicales », alors qu'un médecin accèdera « également aux données médicales » ;

- Le critère de l'« *équipe de soins* » (telle que définie par la loi (art. L.1110-12 du Code de la santé publique)) : seuls les professionnels effectivement impliqués dans la prise en charge d'un patient ou dans les soins qui lui sont prodigués doivent pouvoir avoir accès aux données couvertes par le secret médical.
  La CNIL précise, toutefois, consciente des enjeux et des nécessités du métier, que « les habilitations accordées peuvent être complétées d'un mode « bris de glace « *qui permet aux agents administratifs et professionnels de santé, en cas d'urgence, d'avoir accès à d'autres données pour tout patient* ».

- Implémenter un dispositif de journalisation permettant de tracer les accès au DPI : « *cette traçabilité doit non seulement permettre d'indiquer qui s'est connecté à la base de données à quel moment, mais, plus précisément, qui a accédé à quoi. Des contrôles réguliers de ces accès doivent être opérés, afin d'identifier ceux susceptibles d'être frauduleux ou illégitimes. Il est vivement recommandé de disposer d'un système d'analyse automatique des journaux de connexion afin de repérer les accès qui semblent anormaux.* »

La CNIL prévoit de poursuivre ses contrôles en 2024.

Source : ici

VU DANS LA PRESSE

« DSIH », JANVIER 2024

UN ORGANISME DE CONTROLE MEDICAL PEUT-IL TRAITER LES DONNEES DE SANTE DE SES PROPRES SALARIES ?

Lorsqu'un organisme de contrôle médical traite des données de santé d'un de ses salariés afin d'évaluer les capacités de travail dudit salarié, la licéité d'un tel traitement au regard du RGPD interroge. Comment effectivement gérer cette double « casquette » de l'organisme, à la fois responsable de traitement agissant dans le cadre de sa mission de contrôle médical, et également employeur de la personne concernée par le traitement ? Un tel traitement peut-il être autorisé ? N'y-a-t-il pas conflit d'intérêts ? Le consentement du salarié concerné pour procéder à un tel traitement est-il requis ? Comment assurer le respect du secret médical au sein de l'organisme, en particulier vis-à-vis de l'équipe travaillant avec le salarié concerné ?

La Cour de Justice de l'Union européenne a récemment jugé (lien vers la décision) que ce type de traitement est parfaitement licite au regard du RGPD, sous réserve de respecter, effectivement, les conditions et garanties prévues par ce texte.

En l'occurrence, l'affaire concernait un service médical ayant notamment pour mission légale d'évaluer l'incapacité de personnes assurées auprès de certaines caisses d'assurance maladie. Cette mission, réalisée sous forme d'expertise médicale, permet aux caisses d'assurance maladie d'apprécier leur obligation ou non de verser des indemnités d'incapacité de travail.

A la demande d'une des caisses concernées, le service médical a réalisé une expertise relative à l'incapacité de travail d'un assuré de ladite caisse. La particularité de la situation résidait dans le fait que cet assuré était, par ailleurs, un employé du service médical.

Après avoir découvert que son employeur a réalisé une expertise médicale sur son incapacité de travail, la personne concernée a réussi à obtenir le rapport d'expertise associé par le biais d'un ses collègues.

Considérant qu'un tel traitement de ses données de santé à caractère personnel a été réalisé illicitement, notamment sans son consentement, la personne concernée a alors attrait en justice, son employeur, le service médical.

Pour mémoire, le RGPD prévoit des exceptions à l'interdiction de principe du traitement de données de santé (article 9§1 du RGPD), parmi lesquelles figure le « traitement nécessaire notamment à l'appréciation de la capacité de travail du travailleur » (article 9§2 h)).

Si un tel traitement est possible, il doit, néanmoins, être exercé sous certaines réserves (même article), en particulier le respect d'un devoir de confidentialité dans les conditions indiquées à l'article 9§3 du RGPD (« les données sont traitées par un professionnel de la santé soumis à une obligation de secret professionnel conformément au droit de l'Union, au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents, ou sous sa responsabilité, ou par une autre personne également soumise à une obligation de secret conformément au droit de l'Union ou au droit d'un État membre ou aux règles arrêtées par les organismes nationaux compétents. »).

Les juges européens ont considéré que cette exception (le traitement de données de santé nécessaire à l'évaluation de capacité d'un travailleur) n'a pas à être limitée « aux hypothèses où un « tiers neutre » traite des données concernant la santé aux fins de l'appréciation de la capacité de travail d'un travailleur ». La « casquette » d'employeur du responsable de traitement concerné est donc sans incidence sur la possibilité pour celui-ci, en tant qu'organisme de contrôle médical, de réaliser un tel traitement.

La CJUE a également précisé qu'il n'est pas nécessaire, par principe, que le responsable du traitement garantisse qu'aucun collègue de la personne concernée ne puisse accéder aux données se rapportant à l'état de santé de celle-ci. Pour la Cour, il suffit que les traitements soient réservés à des personnes soumises à une obligation de secret, conformément aux conditions prévues par le RGPD (article 9§3 du RGPD).

Par ailleurs, les juges européens ont précisé qu'un traitement autorisé, par exception en vertu du RGPD, n'est pas pour autant dispensé de base légale et ce, comme tout traitement de données à caractère personnel. Un tel traitement doit donc également respecter l'une des conditions de licéité prévues à l'article 6§1 du RGPD (consentement, exécution d'un contrat, obligation légale, sauvegarde des intérêts vitaux, mission d'intérêt public, intérêt légitime).

Cette solution nous donne ainsi des éclairages pour apprécier la licéité de certains traitements de données de santé réalisés pour les besoins d'une mission légale/de service public, d'une part, et l'organisation de la protection du secret médical dans un tel cadre, d'autre part.

Source : ici

UN ENTREPOT DE DONNEES DE SANTE PEUT-IL ETRE HEBERGE PAR MICROSOFT ?

Rappel du cadre légal des entrepôts de données de santé

Pour mémoire, la CNIL a publié un référentiel relatif « aux traitements de données à caractère personnel mis en œuvre à des fins de création d'entrepôts de données de santé dans le domaine de la santé » (le « Référentiel »). Ce Référentiel concerne uniquement les entrepôts de données de santé « *nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable de traitement* ».

Ainsi, un organisme, responsable de traitement, souhaitant mettre en œuvre un entrepôt de données de santé ayant une telle finalité d'intérêt public doit, par principe, s'assurer de la conformité de son projet au Référentiel.

Dans le cas où l'organisme considère que son projet est en stricte conformité avec le Référentiel, il peut alors se contenter d'une déclaration de conformité auprès de la CNIL (Cas n°1). Dans l'hypothèse où il y aurait des écarts avec les exigences prévues au Référentiel, l'organisme doit saisir la CNIL d'une demande d'autorisation spécifique préalable (Cas n°2).

La demande d'autorisation du Health Data Hub pour « EMC2 »

Le Health Data Hub s'est trouvé dans le Cas n°2 concernant son projet d'entrepôt de données de santé « EMC2 ». Il a donc saisi la CNIL d'une demande d'autorisation.

Pour information, le projet « EMC2 », qui s'inscrit dans le cadre d'une convention de services liant le Health Data Hub à l'Agence européenne des médicaments (EMA), a pour objet la création d'une base de données afin de réaliser des études en pharmaco-épidémiologie.

Le projet « EMC2 » a, plus précisément, notamment pour objectif d'« *observer et évaluer la prise en charge des patients (…)* », d'« *évaluer l'utilisation et/ou les pratiques, l'efficacité et la sécurité en vie réelle des produits de santé, en particulier les médicaments et les dispositifs médicaux inscrits au remboursement ou en accès précoce (…)* ». A noter que « la constitution de l'entrepôt nécessite un appariement entre les données de la base principale du système national des données de santé (SNDS) et les dossiers médicaux fournis par les établissements de santé partenaires ».

La position de la CNIL

Dans le cadre de l'analyse du projet « EMC2 », la CNIL s'est notamment penchée sur la question du recours à la société Microsoft Ireland Operations Ltd en tant qu'hébergeur des données.

En premier lieu, la CNIL a relevé que :

- les données seront conservées dans des centres de données localisés en France ;
- seules les « *données techniques d'usage de la plateforme (qui ne révèlent aucune information de santé)* », feront, pour des raisons d'administration de ladite plateforme, l'objet de transferts aux Etats-Unis (transferts encadrés par les Clauses Contractuelles Types de la Commission européenne et nécessitant une information spécifique des personnes concernées).

Ensuite, la CNIL a estimé qu'il existe tout de même un risque d'accès aux données par les autorités américaines puisque la maison mère de la société Microsoft Ireland Ltd est située aux Etats-Unis (et donc soumise au droit de cet Etat). Un tel risque demeure, pour la CNIL, en dépit de la décision d'adéquation du 10 juillet 2023 (le « Data Privacy Framework ») reconnaissant que le cadre de transferts des données « Etats-Unis/UE » assure un niveau de protection adéquat.

« Si ce risque est le plus souvent acceptable, notamment s'agissant des pays adéquats », la CNIL recommande « *pour les bases de données les plus sensibles* » de faire appel à un hébergeur exclusivement soumis droit européen et certifié « SecNumCloud ». *« En particulier, pour les entrepôts de données de santé appariées avec le SNDS, et malgré le fait que ces données soient pseudonymisées, la CNIL a toujours demandé aux porteurs de projet, publics et privés, de s'assurer que l'hébergeur des données n'est pas soumis à une législation extra-européenne* ». Pour la CNIL, « *cette politique apparaît en cohérence avec (…) la circulaire de la Première ministre du 31 mai 2023 (…) qui demande, sans sa règle n°9, aux autorités publiques de s'assurer que les données « d'une sensibilité particulière » hébergées dans le cloud ne soient pas soumises à des lois extra-européennes* ». Ainsi, le choix du Health Data Hub, « *chargé par la loi de recueillir les bases de données de santé les plus importants du pays », « apparaît en très nette contradiction avec [ces] éléments* ».

Pour répondre aux interrogations de la CNIL, les pouvoirs publics ont fait réaliser une expertise, pilotée par la délégation numérique en santé (DNS), la direction interministérielle du numérique (DINUM) et l'Agence Numérique en santé, « *aux fins de déterminer si le projet EMC2 pouvait, sans compromettre le projet vis-à-vis des conditions fixées par [l'Agence européenne du médicament], être mis en œuvre via un prestataire soumis uniquement aux lois de l'Union européenne* ». Le rapport d'expertise a conclu à l'absence d'offres d'hébergement répondant à de telles conditions dans les délais requis.

Après avoir (i) « *déplor[é] qu'aucun prestataire susceptible de répondre actuellement aux besoins exprimés par le [Health Data Hub] ne protège les données contre l'application de lois extraterritoriales de pays tiers* » et (ii) considéré que « le projet EMC2 aurait pu être retenu par le [Health Data Hub] pour préfigurer la solution souveraine vers laquelle il doit migrer », la CNIL a tout de même autorisé l'entrepôt de données de santé « EMC2 » pour une durée de 3 ans (durée de la

A cet égard, la CNIL a souligné « *qu'il est nécessaire que les engagements pris vis-à-vis de [l'Agence européenne du médicament] puissent être honorés* ».

En conséquence, la CNIL a validé l'hébergement de l'entrepôt de données de santé « EMC2 » par Microsoft.

Cette décision ouvre-t-elle alors la possibilité à certains entrepôts de données de santé d'être hébergés par Microsoft ou d'autres hébergeurs américains ?

Les débats associés à la décision de la CNIL

Cette décision de la CNIL a suscité et suscite encore de vifs débats. Il en ressort notamment la difficulté de concilier, d'une part, la récente décision d'adéquation de la Commission européenne qui constate que les Etats-Unis ont un niveau de protection de données personnelles équivalent à celui de l'Union européenne et, d'autre part, les exigences nationales en matière de souveraineté. Aussi, la position de la CNIL est critiquée (i) en ce qu'elle révèle une « contradiction » du projet « EMC2 » à ces exigences de souveraineté, sans pour autant conclure à une « invalidité » de ce projet, (ii) et ce, alors que d'autres projets d'entrepôts de données de santé similaires au projet « EMC2 » hébergés sur Microsoft Azure ont été refusés par la CNIL.

Il appartient désormais au Conseil d'Etat de trancher cette épineuse question. L'Internet Society France a effectivement annoncé avoir déposé un recours en annulation de la délibération de la CNIL.

Source : ici

DOCTRINE

RGPD

Quelques déclinaisons du droit à l'oubli

Comme chaque mois, Alexandre Fievée tente d'apporter des réponses aux questions que tout le monde se pose en matière de protection des données personnelles, en s'appuyant sur les décisions rendues par les autorités nationales de contrôle au niveau européen et les juridictions européennes. Ce mois-ci, il se penche sur la question du droit à l'oubli appliqué, non pas à un moteur de recherche, mais à un média, éditeur de site web.

Il ressort des termes de l'article 17, paragraphe 1, du RGPD que la personne concernée a « *le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données à caractère personnel la concernant* », sous réserve toutefois qu'elle puisse se prévaloir de l'un des motifs listés au paragraphe 2 du même article. En tout état de cause, le droit à l'effacement (également appelé « *droit à l'oubli* ») ne s'applique pas, en application du paragraphe 3 de cet article, « *dans la mesure où ce traitement est nécessaire (...) à l'exercice du droit à la liberté d'expression et d'information* ».

Depuis plusieurs années, à la suite du développement de la technologie et des outils de communication, des personnes ont cherché, en invoquant le droit à l'oubli (soit sur le fondement du droit de la vie privée, soit sur le fondement de la protection des données), à faire effacer, modifier ou limiter l'accès à des informations passées affectant la perception actuelle de ces personnes dans l'opinion publique, et ce afin d'éviter de se faire reprocher indéfiniment des actes dans des contextes variables, tels que l'embauche ou les relations d'affaires. Pendant longtemps, ces demandes ont été dirigées contre les moteurs de recherche afin qu'ils procèdent au déréférencement des articles relatant les informations litigieuses, de telle manière à ce que ces articles n'apparaissent plus dans les résultats de recherche lorsque la requête porte leurs nom et prénom. Désormais, on constate que les demandes fondées sur le droit à l'oubli sont de plus en plus souvent dirigées contre les éditeurs des sites web, c'est-à-dire ceux qui publient les articles en ligne. De telles demandes – qui consistent en des demandes de désindexation ou d'anonymisation – ne constituent-elles pas une ingérence dans l'exercice par l'éditeur du site du droit à la liberté d'expression et d'information ?

L'affaire

Une personne, visée dans un article comme étant impliquée dans des activités criminelles de type mafieux, avait adressé au média concerné une demande de déréférencement de l'article, au motif que les faits étaient racontés d'une manière complètement déformée et fausse. Le média n'ayant pas donné suite à cette demande, alors même qu'une recherche sur son site internet en utilisant les nom et prénom de la personne renvoyait à cet article, cette dernière a déposé une plainte auprès de l'autorité maltaise de protection des données.

Indiquant que toute personne concernée a le droit, en application de l'article 17, paragraphe 1, du RGPD d'obtenir du responsable du traitement l'effacement de ses données personnelles, l'autorité maltaise a rappelé que ce droit ne s'applique pas, selon les termes du paragraphe 3 du même article, dans la mesure où le traitement est nécessaire à l'exercice du droit à la liberté d'expression et d'information, étant précisé que le RGPD permet aux Etats membres de concilier le droit à la protection des données et la liberté

d'expression et d'information. L'autorité a ajouté, en s'appuyant sur la loi maltaise, que « *le facteur décisif dans la mise en balance [des deux droits] devrait être l'apport des informations publiées dans un débat d'un "intérêt public important"* ». Prenant largement en compte les dernières décisions rendues sur le sujet par la Cour de justice de l'Union européenne (« *CJUE* ») et la Cour européenne des droits de l'homme (« *CEDH* »), et dans une volonté de concilier ces deux droits fondamentaux, l'autorité de protection a fait injonction au responsable du traitement d'introduire une métabalise « *no-index* » dans l'entête du contenu HTLM de la page en ligne litigieuse, et ce « *de manière à empêcher les moteurs de recherche d'indexer cette page et de la faire apparaître dans les résultats de recherche* ».

À noter que, dans une affaire assez similaire, la CEDH a opté, tout récemment, « *au nom du droit à l'oubli* », non pas pour la désindexation de l'article litigieux, mais pour une anonymisation par le média, responsable du traitement, de la version électronique dudit article, considérant qu'une telle solution ne constituait pas, pour le média, une « *charge exorbitante excessive* », tout en représentant, pour le requérant, la mesure la plus efficace pour la protection de sa vie privée. Pour justifier sa décision, la Cour a retenu plusieurs critères : la nature et la gravité des faits de nature judiciaire relatés dans l'article en cause, l'absence d'actualité ou d'intérêt historique ou scientifique de celui-ci, ainsi que l'absence de notoriété du plaignant et l'importance de son préjudice consécutif au maintien en ligne de l'article, lequel est de nature à créer un « *casier judiciaire en ligne* ».

Quelles recommandations ?

Pendant longtemps, le droit à l'oubli s'est analysé comme un droit au déréférencement permettant d'obtenir d'un moteur de recherche la suppression de certains résultats de recherche associés aux nom et prénom d'une personne. Il consistait donc à supprimer l'association d'un résultat de recherche à la requête « *nom prénom* », sans conduire à l'effacement de l'information sur le site internet source. L'idée était de rendre l'article moins visible, du fait qu'il n'était plus référencé. Cela est toujours vrai. Mais désormais, nous savons, à la lecture des dernières décisions, qu'il est également possible, toujours sur le même fondement du droit à l'oubli, d'agir directement contre l'éditeur du site web en cause et d'obtenir une mesure de type désindexation ou anonymisation de l'article litigieux, dès lors qu'une telle mesure permet de concilier le droit à la protection des données et le droit la liberté d'expression et d'information.

Alexandre FIEVEE
Avocat associé
Derriennic Associes

Notes

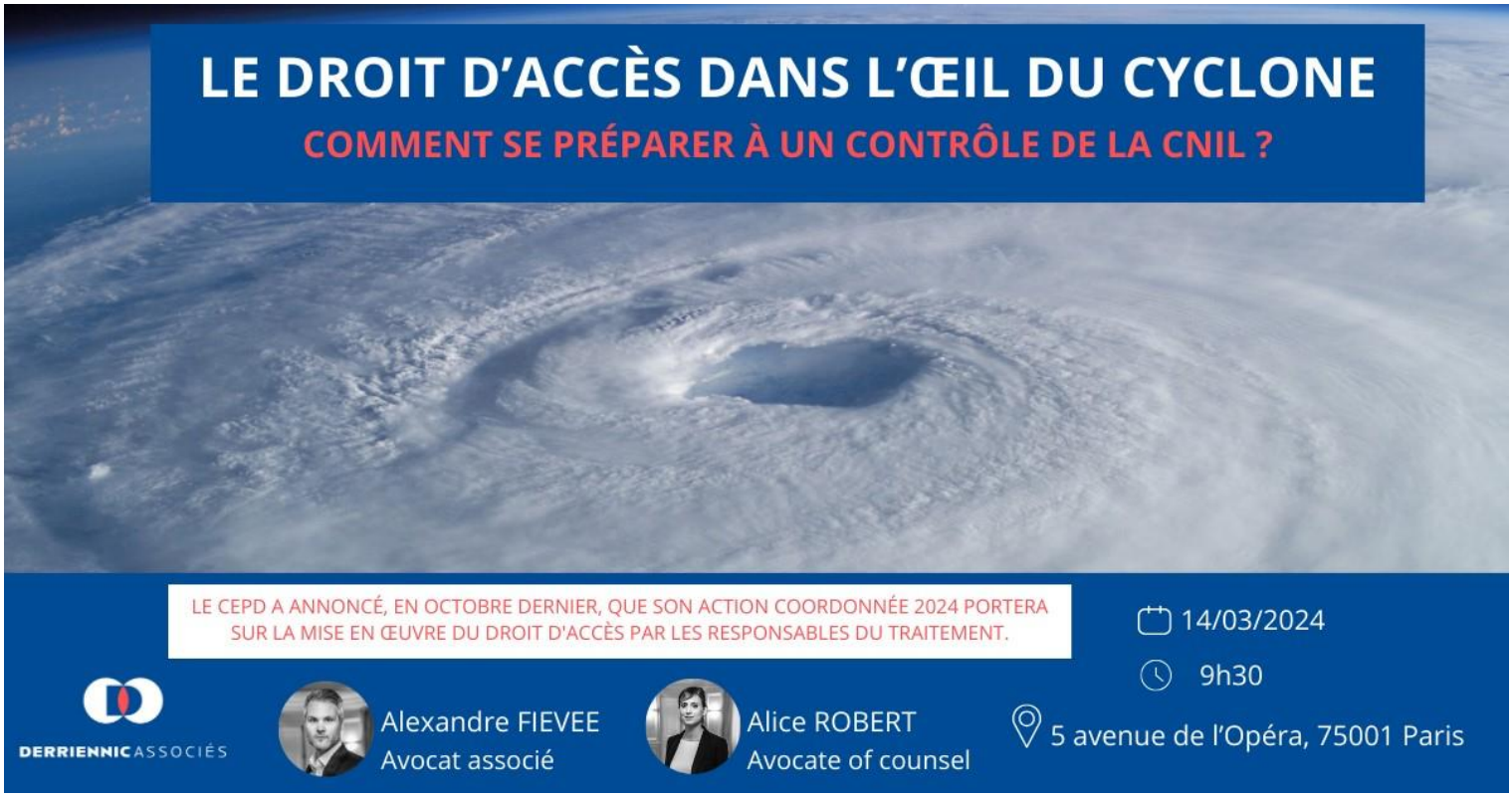
(1) Convention européenne des droits de l'homme, article 8.

(2) RGPD, article 17.

(3) Autorité maltaise de protection des données, CDP/COMP/144/2022, 11 octobre 2023.

(4) CEDH, Affaire Hurbain c. Belgique, 4 juillet 2023.

Matinale du 14 mars 2024 présentée par le pôle RGPD du cabinet Derriennic Associés



Inscriptions : matinales@derriennic.com

ACTUALITÉS DU CABINET

DERRIENNIC ASSOCIÉS PROPOSE UN PROGRAMME DE FORMATION DE 35 HEURES POUR LA PRÉPARATION À LA CERTIFICATION DPO

OBJECTIFS

1/ Acquérir les compétences, les connaissances et le savoir-faire attendus par la CNIL et permettre au collaborateur de se présenter à l'examen de certification en maximisant ses chances de succès.

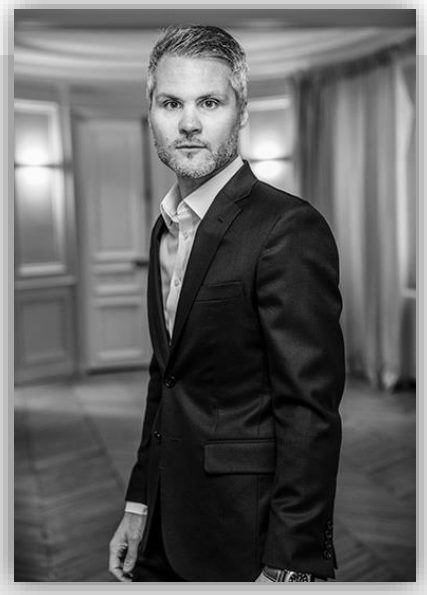
2/ Indépendamment de la certification, la formation permet à l'apprenant de se familiariser avec la matière et d'acquérir les compétences, les connaissances et le savoir-faire pour :

- analyser une situation impliquant un traitement de données personnelles ;
- définir et appréhender les problématiques, les enjeux et les risques qui en découlent ;
- prendre les décisions qui s'imposent en concertation avec l'équipe « DPO ».

CONTENU DE LA FORMATION

Partie 1 - Réglementation générale en matière de protection des données et mesures prises pour la mise en conformité
Partie 2 - Responsabilité (Application du principe d'« Accountability »)
Partie 3 - Mesures techniques et organisationnelles pour la sécurité des données au regard des risques

INTERVENANT



Alexandre FIEVEE
Avocat Associé
01.47.03.14.94
afievee@derriennic.com

CLASSEMENTS
Alexandre Fievee figure dans le classement BestLawyers dans la catégorie « *Information Technology Law* » (2023).
Il a également fait en 2020 son entrée dans le classement Legal 500 dans la catégorie *« Next Generation Partners* ».

RENSEIGNEMENTS PRATIQUES
Prochaine session en 2024 :
Sur demande.
Lieu de la formation :
Au cabinet Derriennic Associés (5 avenue de l'opéra - 75001 Paris) ou en visio-conférence.
Inscription et informations :
afievee@derriennic.com