NEWSLETTER RGPD/DATA

NUMÉRO 63 ● 2024

SOMMAIRE

ACTUALITE

- Le CEPD défavorable au modèle « consentir ou payer » mis en place par certaines grandes plateformes en ligne. **p. 2**
- Rapport du CEPD sur ChatGPT : Les principes du RGPD malmenés. **p.4**
- Quelles démarches CNIL pour quelle modification du traitement de données de santé ? **p.5**
- Plateforme de prise de rendez-vous médicaux : l'éditeur, sous-traitant, n'a pas à répondre à une demande de droit d'accès. **p.6**
- Profilage et enquêtes privées : Ce que l'employeur n'a pas le droit de faire. **p.7**
- La vidéosurveillance dans les chambres des EHPAD : Est-ce licite ? **P.9**
- La publication d'une vidéo sur les réseaux sociaux est soumise au RGPD **p.10**
- Communication de données de rémunération d'un député européen à des citoyens : La validation du tribunal de l'UE **p. 11**
- Les salariés ne doivent informer leurs congés maladies que les personnes ayant besoin d'en connaître. **p 13**

VU DANS LA PRESSE

- Sécurité : empêcher les accès inappropriés au dossier médical. **p.14**

ACTUALITES DU CABINET P. 15

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

ACTUALITE

LE CEPD DEFAVORABLE AU MODELE « *CONSENTIR OU PAYER* » MIS EN PLACE PAR CERTAINES GRANDES PLATEFORMES EN LIGNE

Face au développement du modèle « Consentir ou Payer » mis en place par de plus en plus de grandes plateformes en ligne, consistant à offrir le choix à l'utilisateur entre, d'une part, utiliser le service proposé par la plateforme gratuitement en contrepartie du consentement au traitement de ses données personnelles à des fins de prospection commerciale ciblée ou, d'autre part, payer pour utiliser le service, le Comité européen de la protection des données (CEPD) s'est penché sur la validité du consentement comme base légale de ce traitement. Plus précisément, le CEPD a considéré, dans un avis du 17 avril dernier, que le consentement donné par les utilisateurs des plateformes dans de telles situations n'était pas « libre » au sens du Règlement Général sur la Protection des Données (RGPD), car ceux-ci ne disposeraient pas d'un réel choix.

Un choix contraint par l'absence d'alternative équivalente

Le CEPD indique que, dans la plupart des cas, les grandes plateformes en ligne ne sauraient se conformer aux exigences du RGPD en matière de consentement valable si elles ne proposent aux utilisateurs qu'un « *choix binaire* » entre le consentement au traitement des données à caractère personnel à des fins de publicité comportementale et le paiement d'une redevance.

L'avis indique clairement que la seule offre d'une alternative payante au service qui inclut le traitement à des fins de publicité comportementale « *ne devrait pas être la solution par défaut pour les responsables du traitement* ».

Par ailleurs, si les plateformes en ligne choisissent de proposer une option payante pour l'utilisation de leurs services, elles devraient envisager de fournir aux utilisateurs une « *alternative équivalente* » n'impliquant ni le paiement d'une redevance, ni le traitement des données personnelles de ces derniers à des fins de ciblage publicitaire. Le Comité indique que « *cette alternative […] peut, par exemple, être une version du service avec une forme différente de publicité impliquant le traitement de moins (ou pas) de données à caractère personnel, par exemple une publicité contextuelle ou générale ou une publicité basée sur des sujets que la personne concernée a sélectionnés à partir d'une liste de sujets d'intérêt*. »

En d'autres termes, pour que le consentement des utilisateurs remplisse le critère de liberté imposé par le RGPD, le Comité indique que les plateformes devraient proposer une alternative équivalente gratuite, sans publicité comportementale, afin de ne pas inciter les personnes concernées à consentir au traitement de leurs données personnelles.

Un choix contraint par le préjudice subi par l'utilisateur en cas de refus

Le CEPD rappelle que le RGPD exige qu'un consentement soit « *librement donné* » pour être considéré comme valide. Ainsi, afin d'éviter tout préjudice qui exclurait le caractère libre du consentement de l'utilisateur, le comité indique que « *les frais imposés ne peuvent être tels qu'ils empêcheraient effectivement les personnes concernées de faire un choix libre* ».

En outre, le CEPD indique qu'une personne concernée peut subir un préjudice dans l'hypothèse où, refusant de payer une redevance, elle risquerait d'être « *exclue du service* » proposé par la plateforme. Ce préjudice peut être exacerbé lorsque le service « *joue un rôle important ou est décisif pour la participation à la vie sociale ou l'accès à des réseaux professionnels* », a fortiori en présence d'effets de verrouillage ou de réseau. Les plateformes doivent donc évaluer, au cas par cas, s'il existe un « *déséquilibre des pouvoirs* » entre la personne concernée et le responsable du traitement. Les facteurs à prendre en compte sont notamment « *la position de la grande plateforme en ligne sur le marché* », « *l'existence d'effets de verrouillage ou de réseau* », ou encore « *la mesure dans laquelle la personne concernée dépend du service et le public principal du service* ».

Cet avis s'inscrit dans la même dynamique que les positions de la CJUE – et de la CNIL – relatives à la monétisation des données personnelles : celle-ci est interdite lorsqu'elle a des conséquences préjudiciables sur un individu (par exemple, exclusion d'un service), mais autorisée si elle lui procure un avantage (par exemple, l'octroi d'un code promotionnel à une personne acceptant de s'inscrire à une newsletter).

Source : ici

RAPPORT DU CEPD SUR CHATGPT : LES PRINCIPES DU RGPD MALMENES

Le 23 mai 2024, le CEPD a rendu un rapport au sujet de ChatGPT, l'outil d'intelligence artificielle proposé par la société américaine OpenAI. Ce document met en lumière un certain nombre de sujets relatifs à la conformité au RGPD.

Le CEPD a décidé de mandater une « task force », afin d'échanger avec OpenAI au sujet la conformité au RGPD de son outil ChatGPT. Si cette mission est toujours en cours, le CEPD a d'ores et déjà rendu public un rapport préliminaire faisant état des premiers résultats de ces investigations.

Un principe de licéité imposant une collecte moins large

En premier lieu, le CEPD indique que le principe de licéité, tel que formulé dans le RGPD, pourrait être mis en péril par ChatGPT, dans la mesure où cet outil d'intelligence artificielle procède à du « web scraping » afin de collecter les données utiles à son entrainement, dont certaines sont personnelles, voire sensibles. OpenIA indique se fonder sur la poursuite de son intérêt légitime.

Pour le CEPD, qui paraphrase ici le RGPD, cette base légale nécessite de procéder à une mise en balance des intérêts d'OpenIA et des droits et libertés des personnes concernées. Le CEPD suggère, en l'état actuel des investigations, que des mesures techniques visant à restreindre l'étendue des données personnelles collectées soient implémentées, afin de ménager les droits et libertés des personnes concernées.

Le principe de loyauté : pas de transfert de risque

Selon le CEPD, le principe de loyauté impose au responsable du traitement de ne pas transférer le « *risque juridique* » aux personnes concernées. Cela signifie que les conditions d'utilisation de ChatGPT ne peuvent pas rendre les personnes concernées responsables des informations qu'elles rentrent au moyen du chat.

Au contraire, OpenIA doit partir du principe que les utilisateurs vont rentrer des données à caractère personnel via le chat. Elle reste, à cet égard, responsable de la réutilisation de ces données et s'assurer que celle-ci est conforme au RGPD.

Une exemption s'agissant du principe de transparence

Lorsque ChatGPT procède à des opérations de « web scraping », le CEPD considère, compte tenu du volume de données collectées, qu'il n'est pas possible d'informer les personnes concernées, ce qui pourrait justifier qu'OpenIA soit exemptée de délivrer une telle information.

En revanche, les données personnelles collectées lors des interactions entre ChatGPT et les utilisateurs doivent faire l'objet d'une information dédiée, OpenIA étant ici en relation directe avec l'utilisateur, qui se trouve sur son site internet.

Un principe d'exactitude difficilement conciliable avec des réponses probabilistes

Le principe d'exactitude impose à OpenIA de s'assurer que les données à caractère personnel contenues dans les réponses (ou « outputs ») apportées par ChatGPT soient exactes. Pour rappel, les outputs de ChatGPT sont conçus au moyen d'une approche probabiliste, ce qui signifie qu'une information émanant de ChatGPT peut être biaisée, voire totalement inventée.

Sur ce point, le CEPD suggère qu'une information claire soit délivrée aux utilisateurs quant à l'approche probabiliste de la création d'outputs. Le CEPD tempère néanmoins sa proposition, en indiquant que cette mesure relèverait plutôt du principe de transparence et serait, à elle seule, insuffisante pour se conformer au principe d'exactitude

Source : ici

QUELLES DEMARCHES CNIL POUR QUELLE MODIFICATION DU TRAITEMENT DE DONNEES DE SANTE ?

Nul n'ignore que certains traitements de données de santé doivent faire l'objet, avant leur mise en œuvre, d'une formalité CNIL. Mais saviez-vous qu'une modification d'un traitement, ayant fait l'objet d'une telle formalité, peut justifier une nouvelle formalité ? C'est ce que vient de nous préciser la CNIL dans un communiqué publié le 13 juin dernier.

Quelles formalités initiales ?

Pour connaître la formalité auquel un traitement de données santé est soumis, il convient de se reporter à la loi Informatique et Libertés.

Les formalités sont de deux ordres : soit le traitement répond aux exigences d'un référentiel établi par la CNIL, et, dans ce cas, un engagement de conformité suffit ; soit le traitement n'y répond pas ou ne peut être rattaché à aucun référentiel, et, dans ce cas, une demande d'autorisation s'impose.

Quelles modifications peuvent justifier une nouvelle formalité ?

Selon la CNIL, seule une modification « *substantielle* » – par opposition à la modification « *non-substantielle* » – du traitement doit faire l'objet d'une nouvelle démarche.

Afin de guider les responsables du traitement dans leurs démarches, la CNIL a proposé un tableau recensant les modifications les plus fréquentes (Extrait : ici)

Quelle nouvelle formalité en cas de modification substantielle ?

Si la traitement avait été mis en œuvre dans le cadre d'engagement de conformité à un référentiel et que la modification « *substantielle* » n'affecte pas la conformité du traitement à ce référentiel, aucune démarche CNIL n'est nécessaire.

En revanche, la modification « *substantielle* » affecte la conformité du traitement à ce référentiel, une demande d'autorisation auprès de la CNIL s'impose.

Si le traitement avait été mis en œuvre après une autorisation de la CNIL et que la modification « *substantielle* » rend le traitement conforme au référentiel dédié à ce type de traitement, un engagement de conformité suffit. En revanche, la modification « *substantielle* » ne rend pas le traitement conforme à ce référentiel, une demande de modification de l'autorisation auprès de la CNIL s'impose.

A vous de jouer !

Source : ici

PLATEFORME DE PRISE DE RENDEZ-VOUS MEDICAUX : L'EDITEUR, SOUS-TRAITANT, N'A PAS A REPONDRE A UNE DEMANDE DE DROIT D'ACCES

APD (Belgique), 25 avril 2024

L'autorité de contrôle belge a considéré que l'éditeur d'une plateforme permettant de prendre des rendez-vous médicaux est un sous-traitant et donc qu'il n'a pas à répondre à une demande de droit d'accès.

Un patient a exercé son droit d'accès auprès de l'éditeur d'une solution logicielle permettant de prendre des rendez-vous, en ligne, auprès de professionnels de santé.

L'éditeur de la solution, indiquant être un sous-traitant, a refusé de faire droit à la demande mais a fourni, après une recherche dans sa base de données, la liste des responsables du traitement, professionnels de santé, à contacter.

Le patient, considérant ce refus comme contraire au RGPD, a déposé une plainte.

L'autorité de contrôle, rappelant que le droit d'accès s'exerce auprès du responsable du traitement, a considéré que l'éditeur de la solution était un sous-traitant :

- D'une part, car la finalité de l'application, à savoir « *permettre la prise de rendez-vous automatisée* », est déterminée par le professionnel de santé, la solution logicielle n'étant qu'« *un moyen d'atteindre cette finalité* » ;
- D'autre part, car le professionnel de santé décide seul du moyen qui est le plus approprié pour atteinte la finalité recherchée, et donc que l'éditeur de la solution n'a qu'un rôle d'intermédiaire, en ce sens qu'il ne fait qu'offrir une application proposant une fonctionnalité de prise de rendez-vous ;
- Enfin, car l'éditeur du logiciel traite les données pour le compte du prestataire de santé, l'éditeur ne disposant en l'espèce d'aucune marge de manœuvre pour traiter les données à caractère personnelles à d'autres fins que celles définies par le professionnel de santé.

En conséquence, l'autorité de contrôle a considéré que l'éditeur de logiciel n'avait effectivement pas à répondre à la demande de droit d'accès de la personne concernée.

Rappelant, enfin, que le sous-traitant est tenu de traiter les données conformément aux instructions du responsable du traitement, l'autorité de contrôle n'a pas reproché à l'éditeur du logiciel d'avoir recherché la présence de la personne concernée dans les bases de données de ses clients, responsables du traitement, mais a, au contraire, considéré qu'« *il s'agit là d'une bonne pratique qui facilite l'exercice des droits de la personne concernée* ».

Compte tenu de tout ce qui précède, l'autorité de contrôle a rejeté la plainte de la personne concernée.

Source : ici

APD
Autorité de protection des données

PROFILAGE ET ENQUETES PRIVEES : CE QUE L'EMPLOYEUR N'A PAS LE DROIT DE FAIRE

L'employeur peut-il diligenter des enquêtes privées à l'insu de ses salariés ? C'est à cette question que la Chambre criminelle de la Cour de cassation a récemment répondue, dans une affaire dans laquelle avait été découvert un veste système d'espionnage organisé (profilage et enquêtes privées) au sein de la société IKEA France. Retour dans les années 2010…

L'affaire IKEA

A la suite de la plainte d'un syndicat qui faisait état d'un système d'espionnage organisé au sein de la société IKEA France, plusieurs perquisitions ont été réalisées. Des contrôles ont été, par ailleurs, diligentés par la CNIL. A la suite de ces premières opérations, une information judiciaire a été ouverte des chefs notamment de collectes de données personnelles contenues dans un fichier par un moyen frauduleux, déloyal ou illicite, faits réprimés à l'article 226-18 du Code pénal.

Les investigations ont très vite mis en lumière le rôle joué par le directeur du Département Gestion des Risques de la société IKEA France, qui missionnait régulièrement des sociétés – dont la société E – pour effectuer des recherches sur des personnes. C'est ainsi que Monsieur JPF a réalisé, en qualité de dirigeant de la société E, de nombreuses investigations privées sur des candidats (notamment concernant la véracité des informations figurant dans les CV), mais aussi sur du personnel (soupçonné de vol ou encore ayant dénoncé des faits dans l'entreprise, tels que les conditions d'hygiène alimentaire d'un restaurant d'un magasin). Les clients en litige avec la société (dont des clients défaillants) pouvaient également faire l'objet de recherches. Des enquêtes étaient alors réalisées sur leur patrimoine et leur solvabilité.

Pour l'exercice de ces missions, Monsieur JPF utilisait un logiciel qui balayait de manière systématique les diverses bases de données accessibles en ligne (Facebook, Twitter, etc.), dans lesquelles il pouvait collecter de nombreux renseignements sur les personnes ciblées (activités professionnelles ou privées, activités familiales, état d'âme, difficultés conjugales et professionnelles, démêlés judiciaires). Il épluchait également la presse locale, riche en faits divers, et pouvait aussi procéder, au besoin, à des enquêtes de voisinage.

Par un jugement en date du 15 juin 2021, le tribunal correctionnel de Versailles a déclaré le directeur du Département Gestion des Risques de la société IKEA France coupable des faits de collecte de données personnelles par un moyen frauduleux, déloyal ou illicite et l'a condamné à une peine de dix-huit mois d'emprisonnement avec sursis et au paiement d'une amende de dix mille euros. JPF a, quant à lui, été condamné, pour les mêmes faits en tant que complice, à une peine de deux ans d'emprisonnement avec sursis et au paiement d'une amende de vingt mille euros.

Ce dernier a – contrairement au directeur du Département Gestion des Risques de la société IKEA France – interjeté appel de la décision.

Mais la juridiction du second degré n'est pas allée dans son sens et l'a reconnu coupable – en tant qu'auteur et non plus en tant que complice – du délit visé à l'article 226-18 du Code pénal, car selon la Cour d'appel de Versailles : « *Il est considéré comme déloyal, notamment dans les relations employeur/employé lorsque la collecte a été assurée par la capture d'informations diffusées sur des sites publics – sites Web, annuaires, forums de discussion, réseaux sociaux… – dès lors que les informations collectées ont donné lieu à une utilisation sans rapport avec l'objet de leur mise en ligne, et ont été recueillies à l'insu des personnes concernées les privant ainsi de leur droit d'opposition institué par la Loi informatique et libertés.* » JPF a, sans plus de succès, formé un pourvoi en cassation.

Ce que dit la Cour de cassation

La Chambre criminelle a estimé que la cour d'appel, en se déterminant comme elle l'a fait, n'avait pas méconnu les termes de l'article 226-18 du Code pénal. En effet, « *le fait que les données à caractère personnel collectées par le prévenu aient été pour partie en accès libre sur internet ne retire rien au caractère déloyal de cette collecte, dès lors qu'une telle collecte, de surcroît réalisée à des fins dévoyées de profilage des personnes concernées et d'investigation dans leur vie privée, à l'insu de celles-ci, ne pouvait s'effectuer sans qu'elles en soient informées*. »

En d'autres termes, l'employeur, qui collecte des données personnelles concernant ses salariés sans les en informer préalablement, s'expose à un risque pénal, quand bien même les données collectées étaient accessibles à tous parce qu'en libre accès sur internet.

L'ironie de l'histoire c'est que cela ne signifie pas pour autant, au regard des derniers arrêts de la chambre sociale et de l'assemblée plénière de la Cour de cassation, que l'employeur ne pourra pas se prévaloir, dans le cadre d'un procès civil, des moyens de preuve obtenus dans le cadre de cette collecte illicite, puisque, dans une telle situation, le juge ne peut écarter des débats les preuves ainsi obtenues sans avoir mis en balance, d'une part, le droit au respect de la vie personnelle du salarié et, d'autre part, le droit à la preuve. Il reste alors à l'employeur de mettre en balance, d'un côté, son intérêt à produire en justice le moyen de preuve illicite et, de l'autre côté, son risque pénal.

Source : ici

LA VIDEOSURVEILLANCE DANS LES CHAMBRES DES EHPAD : EST-CE LICITE ?

Par une délibération du 29 février 2024, la CNIL a adopté ses recommandations relatives à la mise en place de dispositifs de vidéosurveillance au sein des chambres des établissements accueillant des personnes âgées.

En février 2023, la CNIL annonçait lancer une consultation publique relative à la vidéosurveillance dans les chambres d'EHPAD. Un an plus tard, la CNIL a publié ses recommandations et encadré l'utilisation de cet outil.

Le principe : l'interdiction

La CNIL considère que, par principe, l'installation d'un dispositif de vidéosurveillance dans la chambre d'un résident est disproportionnée.

Plus précisément, et même si la personne concernée y consent, l'installation des caméras est interdite, y compris pour les finalités suivantes :

- Améliorer le service offert ;
- Assurer la sécurité des personnes concernées en cas de chute ou d'accident.

La CNIL justifie ces interdictions par le fait que d'autres dispositifs moins attentatoires à la vie privée existent et devraient être privilégiés.

L'exception : les suspicions fortes de maltraitance

Par exception, la CNIL considère que l'installation d'un tel dispositif est possible à deux conditions :

- Premièrement, il doit y avoir une « *suspicion de maltraitance basée sur un faisceau d'indices concordants (hématomes, changements comportementaux…) malgré l'existence de dispositifs alternatifs déjà mis en place* » ;

- Deuxièmement, une enquête interne doit, préalablement, avoir été initiée et ne doit pas avoir permis de détecter des actes de maltraitance avec certitude, mais doit établir que de fortes suspicions subsistent quant à l'existence de tels actes.

C'est seulement à ces conditions qu'un dispositif de vidéosurveillance pourra être installé dans la chambre et, s'il existe toujours des doutes par la suite, dans les lieux d'intimité (douche, toilettes…).

Les garanties appropriées

Bien qu'exceptionnellement autorisé, l'installation d'un tel dispositif suppose la mise en œuvre des garanties appropriées suivantes : (i) limiter l'activation dans le temps, (ii) désactiver le dispositif lors des visites de proches, (iii) déterminer les conditions justifiant l'installation d'un tel dispositif, (iv) informer les personnes concernées, (v) flouter les parties intimes, (vi) indiquer dans le règlement intérieur qu'un tel dispositif peut être mis en place, (vii) installer le dispositif de manière concertée et, enfin, (viii) sensibiliser et former le personnel.

L'obligation d'effectuer une analyse d'impact

Pour finir, au regard des risques élevés qu'est susceptible d'engendrer ce traitement pour les droits et libertés des personnes concernées, la CNIL a indiqué qu'une analyse d'impact (AIPD) est obligatoire.

Source : ici

LA PUBLICATION D'UNE VIDEO SUR LES RESEAUX SOCIAUX EST SOUMISE AU RGPD

AEPD (Espagne), 10 mai 2024

L'autorité de contrôle espagnole a rappelé que le fait de publier, sur les réseaux sociaux, une vidéo d'une personne sans son consentement, est contraire au RGPD.

La vidéo d'une femme a été publiée sur des réseaux sociaux par une personne inconnue.

Cette vidéo, devenue virale, a été visionnée plusieurs millions de fois. La femme, n'ayant pas consenti à une telle publication, a déposé une plainte contre « X » et contre chaque personne ayant partagé et / ou relayé ladite vidéo.

L'autorité de contrôle espagnole a rappelé que la publication d'une vidéo d'une personne sur les réseaux sociaux sans son consentement est un traitement de données à caractère personnel potentiellement illicite, car ne reposant sur aucune base légale. L'autorité de contrôle espagnole a d'abord infligé une amende de 2000 € à l'encontre de chaque personne ayant partagé et / ou relayé la vidéo, puis est revenue sur sa décision faute de preuves suffisantes permettant d'identifier avec certitude les auteurs desdits partages.

Source : ici

COMMUNICATION DE DONNEES DE REMUNERATION D'UN DEPUTE EUROPEEN A DES CITOYENS : LA VALIDATION DU TRIBUNAL DE L'UE

Le Tribunal de l'Union européenne a eu à se prononcer sur la légalité d'une communication à des citoyens de l'UE, par le Parlement européen, de données relatives aux indemnités perçues par un député européen, condamné à une peine d'emprisonnement.

Dans une décision du 8 mai 2024, le Tribunal de l'Union européenne (TUE) a été saisi par des citoyens faisant valoir leurs droits à se voir communiqué les données personnelles d'un député européen, par le Parlement européen.

Une demande de communication de données personnelles d'un député européen

Suite à la condamnation d'un député européen à une lourde peine d'emprisonnement pour participation à une organisation criminelle, des citoyens de l'UE ont sollicité du Parlement européen qu'il leur communique les montants concrets des sommes allouées, par le Parlement, au député, ainsi que la façon dont ces sommes ont été dépensées.

Les citoyens, dont la demande se fondait sur le Règlement 1049/2001 sur l'accès au public aux documents du Parlement européen, faisaient valoir que ces sommes avaient contribué, directement ou indirectement, au financement ou à la perpétuation d'activités criminelles ou illégales.

Le Parlement n'a pas donné de suite favorable à cette requête, estimant notamment qu'une telle communication violerait l'article 9 du Règlement 2018/1725, qui lui interdit de communiquer des données personnelles, sauf :

- si le destinataire établit que les données sont nécessaires à l'exécution d'une mission d'intérêt public ; ou

- si les données sont communiquées dans un but spécifique d'intérêt public et si, après mise en balance des intérêts du destinataire et de ceux de la personne concernée, il s'avère que la communication de données est « *proportionné* » (dans l'hypothèse où la communication de données personnelles porterait atteinte aux intérêts légitimes de la personne concernée).

La divulgation des lieux de déplacement récurrents du député, via ses notes de frais, était susceptible, aux yeux du Parlement européen, de faire courir un risque quant à sa sécurité, ce qui justifiait une rétention des données personnelles.

Les requérants ont formé un recours contre la décision du Parlement européen, devant le TUE.

Il s'agissait, pour les requérants, de caractériser (i) l'existence d'un but légitime et, (ii) dans l'hypothèse d'une atteinte aux intérêts légitimes du député, de la « *proportionnalité* » de la communication, après mise en balance des intérêts des requérants et du député.

Une demande de communication poursuivant un but spécifique d'intérêt public.

Le TUE a estimé que le but consistant à connaître les montants concrets des sommes allouées par le Parlement au député et la façon dont ces sommes ont été dépensées, contribue « *à la transparence quant à la manière dont l'argent des contribuables est dépensé » et doit donc être considéré comme étant « un but spécifique d'intérêt public* ».

Une communication dépourvue d'atteinte aux intérêts légitimes du député

Le TUE a estimé, au sujet des risques quant à la sécurité du député dont les donnée personnelles étaient sollicitées : « *il suffit de rappeler que M. Lagos étant emprisonné, il ne pouvait pas, à la date d'adoption de la décision attaquée, et ne peut davantage, à celle du prononcé du présent arrêt, se déplacer. Partant, la question de sa sécurité lors de tels déplacements hypothétiques ne se pose pas. Eu égard aux circonstances particulières du cas d'espèce, cet argument, par ailleurs non suffisamment étayé par le Parlement, doit donc également être écarté* ».

Le TUE a décidé qu'en l'absence d'atteinte aux intérêts légitimes du député, la mise en balance des intérêts des requérants et du député n'était pas nécessaire. Le Parlement européen aurait donc bien dû procéder à la communication des données personnelles au regard des exigences l'article 9 du Règlement 2018/1725.

Ainsi, le TUE a annulé la décision du Parlement européen.

Source : ici

LES SALARIES NE DOIVENT INFORMER DE LEURS CONGES MALADIE QUE LES PERSONNES AYANT BESOIN D'EN CONNAITRE

HBfDI (Hambourg, Allemagne), Rapport annuel 2023

L'autorité de contrôle de Hambourg a sanctionné un employeur qui obligeait les salariés à informer le reste du personnel de l'entreprise de leur absence pour congés maladie.

Un employeur obligeait ses salariés en congés maladie à prévenir par courriel tous les autres salariés de l'entreprise de leur absence.

Un salarié a déposé une plainte auprès de l'autorité de contrôle hambourgeoise, qui a considéré que l'employeur :

D'une part, n'avait pas respecté sa propre procédure interne, qui prévoit que les salariés doivent uniquement informer leur supérieur hiérarchique et le département des ressources humaines de leur congé maladie ;

D'autre part, n'avait pas respecté le principe de minimisation, puisque l'information des autres salariés de l'entreprise n'était, en l'espèce, pas nécessaire ;

Enfin, avait traité des données de santé en violation du principe d'interdiction posé à l'article 9 du RGPD.

Compte tenu de ce qui précède, l'autorité de contrôle a rappelé le principe selon lequel « *Les salariés ne doivent pas être obligés de divulguer leurs absences pour cause de maladie à leurs collègues si cela n'est pas nécessaire aux fins de la planification et de la réaffectation des tâches* » et a infligé à l'employeur une amende de 75 000 €.

Source : ici

DOCTRINE

RGPD

Sécurité : empêcher les accès inappropriés au dossier médical

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 différentes autorités nationales de contrôle au niveau européen et les juridictions européennes. Ce mois-ci, il se penche sur la question des règles d'habilitation qui font souvent défaut dans les établissements de santé, et ce en violation du principe de sécurité.

Il ressort des termes de l'article 5.1.f du RGPD que les données doivent être traitées « *de façon à garantir une sécurité appropriée des données à caractère personnel, y compris la protection contre le traitement non autorisé ou illicite et contre la perte, la destruction ou les dégâts d'origine accidentelle, à l'aide de mesures techniques ou organisationnelles appropriées* ». L'article 32 du même texte ajoute que le responsable du traitement est tenu de mettre en œuvre « *les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque* ». En d'autres termes, le responsable du traitement est le garant de la sécurité des données personnelles qu'il traite dans le cadre de l'exercice de son activité. À ce titre, il lui appartient notamment de s'assurer que seules les personnes autorisées ont accès aux données personnelles, à savoir uniquement les personnes ayant besoin d'en connaître dans le cadre de l'exercice de leur fonction au sein de l'organisme.

Entre 2020 et 2024, la Cnil s'est intéressée à la situation des établissements de santé. Au terme de treize contrôles, l'autorité française de protection des données a pu constater que les mesures mises en œuvre par ces établissements concernant la sécurité du dossier patient informatisé (DPI) sont insuffisantes notamment en raison d'une politique de gestion des habilitations trop souvent inadaptée, en ce qu'elle permet à des catégories de personnel d'accéder à des données de santé de patients dont elles n'ont pas la charge. L'affaire commentée illustre l'insuffisance des moyens mis en œuvre par les établissements de santé.

L'affaire[3]

L'autorité italienne de protection des données (ou « *GPDP* ») a reçu plusieurs plaintes concernant des accès suspects, au sein d'un établissement de santé, aux dossiers médicaux de patients. L'enquête a montré que ces accès étaient, en effet, inappropriés dans la mesure où ils ont été effectués par des professionnels de santé qui n'étaient pas en charge des patients concernés par les dossiers médicaux consultés. La GPDP a, après avoir analysé les mesures en place au sein de l'établissement, sanctionné ce dernier pour avoir traité des données à caractère personnel en violation notamment des article 5.1.f et 32 du RGPD, la configuration du système permettant à tout personnel de santé de l'organisme d'accéder, sans restriction, aux dossiers médicaux des patients.

Selon l'autorité, « *les mesures mises en place n'apparaissaient pas pleinement adéquates pour garantir que seul le personnel de santé traitant un patient puisse accéder au dossier de santé de ce dernier* », tout en rappelant que « *le responsable du traitement doit identifier, par rapport aux différentes fonctions auxquelles le personnel est affecté, des profils spécifiques pour l'accès au dossier, y compris en ce qui concerne les organes administratifs de la direction médicale* ». Par ailleurs, la GPDP a relevé que l'établissement n'avait

P14

prévu aucun système de détection des anomalies visant à identifier les comportements anormaux (ou à risque) relatifs aux opérations effectuées par le personnel de l'organisme.

Quelles recommandations ?

Les établissements de santé devraient, selon la Cnil, mettre en place des mesures visant à sécuriser les accès au dossier médical, grâce notamment à une politique d'authentification robuste, qui devrait prévoir a minima (i) un identifiant unique par utilisateur,interdire les comptes partagés entre plusieurs utilisateurs et (ii) imposer le recours à des mots de passe suffisamment complexes.

Par ailleurs, ils devraient implémenter des règles d'habilitation répondant à l'exigence selon laquelle un professionnel de santé ou un agent ne peut accéder qu'aux seules données dont il a besoin de connaître.

Selon la Cnil, cette deuxième mesure passe par le respect des deux critères suivants : (i) 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* » ; (ii) le critère de l'« *équipe de soins* » (tel que défini à l'article 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* ». Enfin, la Cnil recommande l'implémentation d'un dispositif de journalisation permettant de tracer les accès au dossier : « *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.* »

Alexandre FIEVEE
Avocat associé
Derriennic Associes

Notes

(1) https://www.cnil.fr/fr/donnees-de-sante-la-cnil-rappelle-les-mesures-de-securite-et-de-confidentialite-pour-lacces-au#:~:text=La%20CNIL%20a%20mis%20en,du%20besoin%20d'en%20conna%C3%AEtre.

(2) GPDP, 22 février 2024.

(3) https://www.cnil.fr/fr/donnees-de-sante-la-cnil-rappelle-les-mesures-de-securite-et-de-confidentialite-pour-lacces-au#:~:text=La%20CNIL%20a%20mis%20en,du%20besoin%20d'en%20conna%C3%AEtre

Vous avez envie de vous exprimer sur un sujet qui vous tient à cœur, de partager votre analyse avec la communauté des lecteurs d'Expertises, d'exposer un point de vue différent sur un article déjà publié, de lancer un débat sur un thème émergent, ou simplement de commenter l'actualité du droit du numérique ?

Contactez la rédactrice en chef d'Expertises Sylvie Rozenfeld sr@expertises.info

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

COÛT

3000€ HT/personne

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* » (2024).

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