NEWSLETTER RGPD/DATA

NUMÉRO 51 ● 2023

SOMMAIRE

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

REVOCATION DU DPO : CE QUE DIT LA CJUE

Dans deux arrêts du 9 février 2023, la CJUE a répondu à des questions préjudicielles et a donné des indications sur l'interprétation des règles encadrant la révocation du DPO et les conflits d'intérêt.

La CJUE a été saisie de plusieurs questions préjudicielles dans deux affaires allemandes :

- Dans une première affaire, une société a relevé de ses fonctions son DPO salarié au motif qu'il existait un risque de conflit d'intérêts, dans la mesure où le DPO exerçait en même temps les fonctions de président du comité d'entreprise ;
- Dans une seconde affaire, une commune a relevé de ses fonctions son DPO salarié au motif qu'il existait un conflit d'intérêts entre ses activités de DPO et ses autres activités professionnelles.

Les DPO relevés de leurs fonctions ont saisi les juridictions allemandes et se sont appuyés sur une réglementation nationale prévoyant qu'un DPO salarié ne peut être révoqué de ses fonctions que pour un « *motif grave* ».

Saisie d'une première question préjudicielle, la CJUE a dû se demander si l'article 38.3 du RGPD s'oppose à ce qu'une réglementation nationale limite les possibilités de révocation d'un DPO à un « *motif grave* ».

Pour rappel, l'article 38.3 du RGPD précise que : *« le délégué à la protection des données ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions* ».

Dans les deux arrêts, la CJUE a adopté la même solution et a considéré que le RGPD « *ne s'oppose pas à une réglementation nationale prévoyant qu'un responsable du traitement ou un sous-traitant ne peut révoquer un [DPO] qui est membre de son personnel que pour un motif grave, même si la révocation n'est pas liée à l'exercice des missions de ce [DPO]* ».

La CJUE a cependant émis une réserve, en considérant « *qu'une telle réglementation ne [doit pas compromettre] la réalisation des objectifs de ce règlement* ». Tel serait le cas, par exemple, (i) si la réglementation nationale empêchait la révocation d'un DPO qui ne posséderait plus les qualités professionnelles requises pour exercer ses missions (article 37.5 du RGPD), ou empêchait la révocation d'un DPO qui serait dans une situation de conflit d'intérêts (article 37.6 du RGPD).

Saisie d'une seconde question préjudicielle à ce sujet, la CJUE a dû se demander dans quelles conditions un « *conflit d'intérêts* » est susceptible d'être constaté ?

Pour mémoire, l'article 38.9 du RGPD dispose que « *Le délégué à la protection des données peut exécuter d'autres missions et tâches. Le responsable du traitement ou le sous-traitant veillent à ce que ces missions et tâches n'entraînent pas de conflit d'intérêts* ».
Selon la CJUE, un conflit d'intérêts est susceptible d'exister « *lorsqu'un DPO se voit confier d'autres missions ou tâches qui le conduiraient à déterminer les finalités et les moyens du traitement de données à caractère personnel auprès du responsable du traitement ou de son sous-traitant ».*

Cette situation doit cependant être déterminée *« par le juge national », au « cas par cas », « sur la base d'une appréciation de l'ensemble des circonstances pertinentes, notamment de la structure organisationnelle du responsable du traitement ou de son sous-traitant et à la lumière de l'ensemble de la réglementation applicable, y compris des éventuelles règles internes de ces derniers* ».

Source : ici

L'AFFAIRE « LUSHA » : DES LIMITES AU RGPD ?

Par une décision du 20 décembre 2022, la CNIL a considéré que le RGPD ne s'appliquait pas à un traitement de données personnelles de citoyens européens réalisé, sans leur consentement, par une société américaine. Une telle décision, suffisamment rare pour être soulignée, nécessite quelques explications.

L'affaire concerne la filiale américaine de la société israélienne LUSHA, qui commercialise une extension de navigateur internet « Lusha » permettant à un utilisateur navigant sur Linkedin ou Salesforce d'obtenir les coordonnées professionnelles de personnes ayant un profil sur ces plateformes, par l'utilisateur. Ces coordonnées ont été obtenues par la filiale américaine à partir des applications mobiles de gestions de contacts (« Simpler », « Mailbook » et « Cleaner Pro ») disponibles depuis le territoire français et aspirant les carnets d'adresses de ses utilisateurs.

La particularité de cette situation réside dans le fait que les personnes concernées (c'est-à-dire les personnes ayant un profil Linkedin ou Salesforce et dont des données ont été aspirées dans le/les carnet(s) d'adresses de tiers les comportant) ne sont pas des utilisateurs (i) de l'extension « Lusha », (ii) ni des applications mobiles de LUSHA. Leurs données de contact ont été collectées parce qu'elles se trouvaient dans le carnet d'adresses d'un ou de plusieurs de leurs contacts, ces derniers étant utilisateurs des applications mobiles LUSHA. Les personnes concernées n'avaient ainsi reçu aucune information sur de tels traitements ni donné leur consentement.

A la suite de signalements et plaintes, dont les premières dataient de 2018, la CNIL a opéré plusieurs contrôles en ligne pour vérifier la conformité de tels traitements au RGPD et à la loi « Informatique et Libertés ». Le rapporteur, désigné aux fins d'instructions de ces éléments, a rendu un rapport précisant les manquements au RGPD considérés comme constitués.

La formation restreinte de CNIL ne l'a pourtant pas suivi, considérant que le RGPD n'était pas territorialement applicable.

Pour mémoire, conformément à l'article 3 du RGPD, celui-ci est applicable :

- *« au traitement des données à caractère personnel effectué dans le cadre des activités d'un établissement d'un responsable du traitement ou d'un sous-traitant sur le territoire de l'Union, que le traitement ait lieu ou non dans l'Union »* (critère de l'établissement) ;
- *« au traitement des données à caractère personnel relatives à des personnes concernées qui se trouvent sur le territoire de l'Union par un responsable du traitement ou un sous-traitant qui n'est pas établi dans l'Union, lorsque les activités de traitement sont liées : a) à l'offre de biens ou de services à ces personnes concernées dans l'Union, qu'un paiement soit exigé ou non desdites personnes* [critère de l'offre de biens ou services] *; ou b) au suivi du comportement de ces personnes, dans la mesure où il s'agit d'un comportement qui a lieu au sein de l'Union* [critère du suivi du comportement] *».*

La formation restreinte de la CNIL a considéré, sans surprise, que le critère de l'établissement ne pouvait être applicable dans la mesure où la filiale américaine ne dispose d'aucun établissement dans l'UE. Elle a également estimé que, dans la mesure où l'extension « Lusha » n'est pas liée à une offre de biens ou services aux personnes concernées (objet des données de contact), le critère de l'offre de biens ou services n'est pas non plus rempli.

Il restait alors le critère du suivi du comportement. A cet égard, la formation restreinte de la CNIL a jugé qu'il n'est pas établi que les personnes concernées font bien l'objet d'un suivi de comportement.

Selon l'autorité : « la constitution de la base de données par la société repose uniquement sur le rapprochement entre des données de contacts professionnels (…) avec l'identité des personnes dont le profil est visité sur LinkedIn afin d'en vérifier la véracité. Il ne s'agit donc pas, en l'espèce, d'un traitement qui consiste à analyser ou prédire un comportement, les préférences personnelles ou les déplacements d'une personne, ses intérêts, sa situation économique ou son état de santé. La formation restreinte considère que la société n'utilise pas de techniques de traitement de données à caractère personnel qui consistent en un profilage d'une personne physique. ».

Le RGPD n'étant pas applicable, la formation restreinte n'a donc pas le pouvoir de prononcer une sanction. La décision a toutefois été publiée afin d'informer « *l'ensemble des utilisateurs des applications en cause soient informés que les traitements mis en œuvre par la société Lusha ne sont pas soumis au RGPD* ».

Cette décision met en lumière le fait que certains traitements de données personnelles de citoyens européens réalisés, à leur insu, sans leur consentement, par des acteurs privés à des fins commerciales, peuvent échapper au RGPD.

Le RGPD est-il à revoir dans son contenu ou dans son interprétation ?

A suivre…

Source : ici

SANCTIONS CNIL : BILAN 2022

Comme chaque année, la CNIL a publié le bilan annuel de son action répressive. Elle y indique une « confirmation des tendances de 2021 », que ce soit par le nombre de sanctions et de mises en demeure, ou par le montant cumulé des amendes.

Dans son bilan de l'année 2022, publié le 31 janvier 2023, la CNIL indique avoir prononcé 21 sanctions, dont 13 ont été rendues publiques et 19 ont donné lieu à des amendes, représentant la somme totale de 101.277.900 euros. Pour mémoire, en 2021, la CNIL avait prononcé 18 sanctions, pour un montant total cumulé de 214.106.000 euros d'amendes, cette somme représentant, alors, une progression de +55% par rapport à l'année 2020.

La CNIL a adressé 147 mises en demeure au cours de l'année 2022, nombre en progression par rapport à 2021 (135 mises en demeure). Ces mises en demeure ont notamment concerné des manquements en matière de désignation de DPO, de prospection commerciale, de transferts de données vers les Etats-Unis (via Google Analytics), ou encore de sécurité des sites internet.

La CNIL a également dressé un bilan plus global : depuis l'entrée en application du RGPD, les autorités de contrôle européennes ont prononcé des amendes dont le montant total dépasse 2,5 milliards d'euros.

Parmi celles-ci :

- les amendes prononcées par l'autorité irlandaise à l'encontre de Facebook (475 millions d'euros), et d'Instagram (585 millions d'euros) ;
- l'amende prononcée en 2021 par l'autorité luxembourgeoise à l'encontre d'Amazon (746 millions d'euros) ;
- les amendes prononcées par la CNIL, elle-même, qui représentent, pour leur part, un peu plus d'un demi-milliard d'euros au total, dont la majeure partie concerne les GAFAM.

Source : ici

ENTREPÔTS DE DONNEES DE SANTE HOSPITALIERS EN FRANCE : UN RAPPORT DE LA HAS

A la fin de l'année 2022, la Haute Autorité de Santé (« HAS ») a rendu public un rapport sur les entrepôts de données de santé hospitaliers en France. Ce rapport met en exergue à la fois le développement et l'hétérogénéité de ces entrepôts de données, mais également les points à améliorer pour favoriser leur utilisation au niveau national.

C'est dans le cadre de « *sa stratégie data* », axée sur l'usage « *des données de vie réelle* », que la HAS a établi ce panorama des entrepôts de données de santé hospitaliers.

Les entrepôts de données de santé hospitaliers (« EDSH ») sont, selon la HAS, une catégorie d'entrepôts de données de santé (« EDS »), ces derniers étant définis comme « *la mise en commun des données d'un ou plusieurs systèmes d'information médicaux, sous un format homogène pour des réutilisations à des fins de pilotage, de recherche ou dans le cadre des soins* ».

La HAS a fait le constat du « *développement rapide sur le territoire français* » de tels entrepôts et de leur « *potentiel important pour tous les acteurs de la santé* » qui va « *au-delà de l'usage primaire du soin* ». Sont ainsi également visées les « *utilisations secondaires* » telles que, par exemple, la recherche ou la réalisation d'études de faisabilité.

Dans son rapport, la HAS a recensé 22 entrepôts de données de santé hospitaliers dont 17 de CHU et 5 d'autres établissements hospitaliers. Pour chacun d'entre eux, la HAS a analysé différents critères : la gouvernance, la transparence, les données, les usages, l'architecture technique et la qualité des données.

Partant de cette analyse, la HAS a identifié plusieurs axes d'amélioration pour une pleine et efficace utilisation des données de ces entrepôts de données.

On peut notamment relever :

- En termes de gouvernance, la constitution d'une « *équipe dédiée, pluridisciplinaire et transverse* » et un travail à trois niveaux (local, interrégional et national) – excluant, de fait, les petites structures hospitalières ;
- En termes de données (dépendantes des SI hospitaliers), la mise en place de modèles standards de données et de nomenclature restreints ;
- En termes d'usage, la résolution des problématiques juridiques posées par des demandes d'autorisation auprès de la CNIL portant sur des EDSH à des fins d'utilisation primaire (soin), mais aussi secondaire (recherche) avec séparation des systèmes d'information (notamment la question de la pseudonymisation ou non de certaines données) ;
- En termes d'architecture technique en ayant recours à un nombre limite de plateformes techniques selon un modèle « open source » (pour des raisons de transparence et d'indépendance vis-à-vis d'un éditeur) et opéré par des « experts internes ».

L'objectif est clair : améliorer l'exploitation des données de santé hospitalières, y compris au service des missions de la HAS.

Source : ici

ACTUALITE

DONNEES BIOMETRIQUES ET GENETIQUES : PAS DE COLLECTE SYSTEMATIQUE DE TOUTE PERSONNE MISE EN EXAMEN

Dans un arrêt du 26 janvier dernier, la CJUE s'est prononcée sur la légalité de la collecte de données biométriques et génétiques dans le cadre d'une procédure pénale et, plus particulièrement, s'agissant de personnes mises en examen.

L'affaire concernait une procédure pénale pour fraude fiscale en Bulgarie. Une personne mise en examen pour participation à un groupe criminel organisé a refusé (i) la collecte de ses empreintes digitales, aux fins de leur enregistrement, et (ii) un prélèvement en vue d'établir son ADN. Les autorités de police ont alors demandé à la juridiction pénale une autorisation d'exécution forcée d'une telle collecte au motif qu'une disposition nationale prévoit l'« enregistrement policier » de personnes mises en examen pour une infraction pénale intentionnelle poursuivie d'office.

La juridiction pénale s'est interrogée sur la légalité d'une telle règle au regard du droit européen, en particulier de la directive « Police-Justice »[1] et de la Charte des droits fondamentaux. Elle s'est ainsi tournée vers la CJUE afin d'avoir des éclairages.

En premier lieu, la Cour a jugé que le droit de l'Union ne s'oppose pas à une législation nationale autorisant une mesure d'exécution forcée de la collecte de données biométriques et génétiques en cas de refus de coopération de la personne mise en examen pour une infraction intentionnelle poursuivie d'office. La Cour a, toutefois, précisé la nécessité que *« le droit national garantisse ultérieurement le contrôle juridictionnel effectif des conditions de cette mise en examen, dont découle l'autorisation de procéder à ladite collecte* ».

En second lieu, la Cour a apporté une limite à une telle possibilité de « collecte forcée » : elle ne peut être systématique pour toute personne mise en examen pour ce type d'infraction. Sur ce point, la CJUE a, en effet, estimé que « *la notion d'« infraction pénale intentionnelle poursuivie d'office » revêt un caractère particulièrement général (…) susceptible de s'appliquer à un grand nombre d'infractions pénales, indépendamment de leur nature et de leur gravité* ». La Cour a également souligné l'exigence de « *protection accrue des personnes à l'égard du traitement de données sensibles* » que constituent les données en cause. En conséquence, « *l'autorité compétente »* a l'obligation *« de vérifier et de démontrer, d'une part, si cette collecte est absolument nécessaire à la réalisation des objectifs concrets poursuivis et, d'autre part, si ces objectifs ne peuvent pas être atteints par des mesures constituant une ingérence de moindre gravité pour les droits et les libertés de la personne concernée.* ».

Ce nouvel arrêt de la CJUE illustre encore une fois l'enjeu de la règlementation relative à la protection de la vie privée dans l'avancement, voire la régularité, d'une procédure pénale.

Source : ici

DOCTRINE

RGPD

Sécurité : limiter les risques d'accès non autorisés aux données

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 problématique des mesures de sécurité qu'un hôpital doit mettre en œuvre pour éviter une divulgation du dossier médical de patients à des membres du personnel qui n'exercent aucune activité de soins à l'égard de tels patients.

En application de l'article 32 du RGPD, le responsable du traitement doit, en tenant compte « *de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques* », mettre en œuvre « *les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque* ».
Autrement dit, tout organisme, qui traite des données personnelles, est tenu à une obligation de sécurité : il doit prendre les mesures nécessaires pour garantir la sécurité des données qu'il a collectées et empêcher notamment leur divulgation à des tiers non autorisés.

C'est ce qu'indique également l'article 5.1.f du RGPD qui souligne que les données personnelles doivent être traitées « *de façon à garantir une sécurité appropriée des données* », et ce « *à l'aide de mesures techniques ou organisationnelles appropriées (intégrité et confidentialité)* ».

L'AFFAIRE[1]

Dans le cas d'espèce, la plaignante, membre du personnel d'un hôpital, avait déposé une plainte auprès de sa direction au motif qu'une de ses collègues, infirmière, avait eu accès au contenu de son dossier médical pendant le temps où elle était soignée par le service des urgences.

Les faits, qui n'étaient aucunement contestés par l'infirmière fautive, avaient par ailleurs été confirmés dans le cadre d'une enquête interne. Selon la plaignante, cet accès était inapproprié dès lors que sa collègue, affectée au bloc opératoire, n'était pas responsable du traitement de son dossier. C'est dans ce contexte que l'autorité espagnole de protection des données (l'AEPD) a été saisie.

Selon cette dernière, il s'agissait de déterminer si les mesures mises en place par l'hôpital étaient « *suffisantes* » pour prévenir ce type d'incident, qualifié de violation de données.

En application de la procédure de sécurité en vigueur dans l'établissement, plusieurs mesures étaient en place au moment des faits, et notamment : la journalisation des accès dans le système ; la réalisation d'audit mensuels ; la ségrégation des profils en fonction des postes afin de limiter les accès au strict minimum ; la signature d'un accord de confidentialité rappelant les devoirs du personnel en termes de sécurité.

« *Seule la segmentation des profils pour l'accès aux dossiers médicaux pourrait être considérée comme une mesure valable et efficace pour éviter des évènements tels que ceux objets du litige* », a considéré l'AEPD.

Et si l'hôpital a fourni une annexe qui détaille les profils de chacun, en différenciant le personnel administratif et le personnel de santé, et, au sein de cette dernière catégorie, en distinguant le personnel par type et par spécialisation, l'autorité de protection des données a considéré qu'une mesure essentielle faisait toutefois défaut : celle selon laquelle un professionnel de santé « *ne devrait avoir accès qu'aux seuls dossiers médicaux des patients sur lesquels il exerce son activité de soins* » et ce, conformément aux dispositions de la loi espagnole du 14 novembre 2002 sur l'autonomie du patient et les droits et obligations en matière d'information et de documentation médicale[2].

Ainsi, s'il est établi que le dossier médical est l'instrument essentiel de la prestation de soins au patient, « *il est également clair que l'accès au dossier clinique ne peut être accordé qu'aux professionnels qui assistent le patient, non pas de manière générale, mais de manière particulière, en effectuant le diagnostic ou le traitement du patient.* »

En conséquence, il appartenait à l'établissement de santé de mettre en place des mesures garantissant que chaque membre de son personnel n'ait accès qu'aux seules données médicales relatives à ses propres patients. De telles mesures faisaient défaut dans le cas d'espèce, dès lors que l'infirmière en cause, qui n'était pas responsable de la plaignante, a pu accéder à son dossier médical, ainsi qu'à son historique clinique.

« *Il ressort de ce qui précède que le défendeur [l'hôpital], en tant que responsable du traitement, n'a pas fait preuve de la diligence requise pour établir les mesures de sécurité nécessaires et éviter la diffusion des données à un tiers, en a conclu l'AEPD. En ce sens, la configuration des mesures techniques et organisationnelles doit être effectuée de manière à ce que, avant le traitement des données personnelles, il soit garanti que seul le personnel qui exerce son activité de soins sur la personne concernée puisse avoir accès aux dossiers. Si l'application informatique contrôlant l'accès aux dossiers médicaux était correctement programmée, elle serait en mesure de déterminer, au moment où l'accès est accordé, si la personne qui le demande (en fonction de sa spécialité, de son poste ou de son activité à ce moment-là) devrait être autorisée à y accéder.* ».

Dans ces conditions, l'autorité espagnole de protection des données a considéré que l'établissement de santé a manqué à son obligation de sécurité, telle que visée aux articles 5.1.f) et 32 du RGPD.

QUELLES RECOMMANDATIONS ?

Afin de limiter les risques que des personnes non autorisées accèdent aux données à caractère personnel, il convient de mettre en place une politique de gestion des privilèges des utilisateurs sur les données. Il s'agit ainsi de définir, comme le recommande la Cnil, « *un ou plusieurs profils d'utilisateurs de façon centralisée (avec des privilèges spécifiques d'utilisation des fonctionnalités, de création, d'accès, de modification, de transfert et de suppression des données)* » et de faire rattacher « *chaque personne à un des profils définis en début de contrat ou de changement d'emploi* ».

Il est également recommandé de prendre les mesures complémentaires suivantes : (i) identifier tout utilisateur ayant un accès légitime aux données par un identifiant unique ; (ii) limiter les utilisateurs/profils disposant de privilèges élevés aux opérations qui le nécessitent ; (iii) chaque utilisateur, et d'autant plus s'il a des privilèges élevés, doit avoir un mot de passe propre ; (iv) journaliser les informations liées à l'utilisation des privilèges et (v) enfin, réaliser un audit semestriel ou annuel des privilèges afin d'identifier et de supprimer les comptes non utilisés et de réaligner les privilèges sur les fonctions de chaque utilisateur.

Alexandre FIEVEE
Avocat Associé
DERRIENNIC ASSOCIES

Notes

(1) **AEPD, Décision n° PS/00587/2021.**

(2) Loi 41/2002 du 14 novembre 2002, **article** 16 : « 1. Le dossier clinique est un instrument **conçu fondamentalement pour garantir des soins adéquats au patient. Les professionnels de santé du centre qui effectuent le diagnostic ou le traitement du patient ont accès à l'histoire clinique du patient en tant qu'instrument** fondamental pour sa prise en charge appro**priée. 2. Chaque centre établit les modalités qui permettent l'accès à tout moment à l'histoire clinique de chaque patient par les professionnels de santé qui l'assistent.** »

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

DOCTRINE

RGPD

Sécuriser les données de santé, c'est déjà sécuriser leur envoi…

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 problématique de la sécurité des communications dans le cadre des envois électroniques et postaux contenant des données de santé à caractère personnel.

Selon la Cnil, la notion de données de santé à caractère personnel doit être entendue très largement. Il s'agit de toutes les données « *relatives à la santé physique ou mentale, passée, présente ou future, 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* »[1].

Entrent donc dans cette catégorie de données sensibles : (i) celles qui sont des données de santé par nature (antécédents médicaux, maladies, prestations de soins réalisés, résultats d'examens, traitements, handicap(s), etc.) ; (ii) celles, qui, du fait de leur croisement avec d'autres données, deviennent des données de santé en ce qu'elles permettent de tirer une conclusion sur l'état de santé ou le risque pour la santé d'une personne ; et (iii) celles qui deviennent des données de santé en raison de leur destination, c'est-à-dire de l'utilisation qui en est faite au plan médical.

Compte tenu de leur sensibilité, les données de santé à caractère personnel bénéficient d'un régime juridique très protecteur (RGPD, article 9). L'organisme qui les traite et qui, comme tout responsable du traitement, est tenu à une obligation de sécurité, doit mettre en œuvre toutes les mesures techniques et organisationnelles qui s'imposent pour préserver leur intégrité, leur disponibilité et leur confidentialité.

Il doit ainsi prendre toutes les précautions utiles, au regard des risques présentés, pour empêcher qu'elles ne soient déformées, endommagées ou que des tiers non autorisés y aient accès, et ce notamment au moment de leur collecte, lors de leur conservation, mais aussi durant leur transmission (RGPD, articles 5 et 32).

Les affaires

Dans deux affaires récentes – l'une qui se déroule en Italie l'autre en Suède – le responsable du traitement a fait l'objet d'une sanction pour ne pas avoir suffisamment protégé les données de santé contenues dans les correspondances adressées aux patients destinataires.

Dans la première affaire[2], il était reproché à un organisme d'avoir, dans le cadre d'une campagne d'information concernant la distribution en Italie d'Eversense XL – « *un système de surveillance continue du glucose pour les personnes souffrant de diabète* » –, saisi, dans le champ « *cc* », les adresses électroniques de tous les patients concernés par le dispositif, permettant ainsi à tous les destinataires de connaître l'identité des autres patients. Le courriel litigieux n'ayant été adressé qu'aux seuls utilisateurs du système de surveillance susvisé, l'autorité italienne de protection des données en a conclu que les informations contenues dans ce courriel devaient de facto s'analyser comme des données à caractère personnel relatives à la santé. Dans ce contexte, elle a estimé que les mesures techniques et organisationnelles mises en œuvre étaient insuffisantes et que l'organisme avait, par une telle communication, « *divulgué aux destinataires des données relatives à l'état de santé des autres patients* » caractérisant ainsi un manquement aux dispositions des articles 5 paragraphe 1, point a) et f), et 9 du RGPD.

Dans la seconde affaire[3], un organisme a été épinglé pour avoir envoyé par voie postale à des patients des convocations à des visites de soins, en utilisant des enveloppes à fenêtre laissant apparaître, outre le nom et

l'adresse des patients, le nom des établissements de soins concernés. Selon l'autorité de contrôle suédoise, « *les données relatives à ces établissements de santé (...) constituent des données de santé au sens de l'article 4(15) du RGPD* ». Par conséquent, et dans la mesure où, du fait de l'utilisation des enveloppes à fenêtre, des données personnelles sensibles étaient « *entièrement visibles* » par tous ceux qui ont été en contact avec les lettres litigieuses, l'autorité de contrôle a prononcé une amende administrative à l'encontre de l'organisme pour manquement caractérisé à l'obligation de sécurité.

Quelles recommandations ?

Pour rappel et au risque de se répéter, le professionnel de santé est tenu de prendre toutes les précautions utiles - au regard des risques présentés par son traitement - pour préserver la sécurité des données. Cela passe notamment par : la sensibilisation du personnel accédant aux données, la gestion des habilitations et des authentifications, la sécurisation des postes de travail, la protection du réseau informatique interne, la sécurisation des serveurs, ou encore la protection des locaux

Il ne faut pas oublier la sécurisation des échanges, qui est tout aussi indispensable que les mesures précédemment citées, et ce qu'il s'agisse d'échanges entre professionnels intervenant dans la prise en charge du patient ou entre un professionnel et un patient. Dans ce cadre, plusieurs mesures sont recommandées par la Cnil : (i) procéder au chiffrement des données avant leur envoi sur une messagerie électronique standard et transmettre le secret par un envoi distinct et via un canal différent ; (ii) utiliser un protocole de transfert garantissant la confidentialité des messages et l'authentification du serveur de messagerie ; (iii) choisir une messagerie hébergeant les données dans un pays ou auprès d'un prestataire garantissant la protection des données conformément aux règles européennes. N'oublions pas l'essentiel : pour les envois postaux, protéger les données par l'utilisation d'une enveloppe adaptée (qui ne rend pas visible le contenu du courrier) et, pour les envois électroniques, vérifier la liste des destinataires en copie afin de ne pas porter atteinte à la confidentialité des données. Sécuriser les données de santé, c'est aussi sécuriser leur envoi...

Alexandre FIEVEE
Avocat associé
DERRIENNIC Associés

Notes

(1) https://www.cnil.fr/fr/quest-ce-ce-quune-donnee-de-sante

(2) GPDP, 7 juillet 2022, n° 9809998

(3) IMY, 17 janvier 2023, 2022-695.

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

PANORAMA EUROPÉEN

PANORAMA DE QUELQUES DECISIONS RENDUES PAR DES AUTORITÉS NATIONALES DE CONTRÔLE

Transfert d'un rapport médical au mauvais destinataire par le sous-traitant

GPDP (Italie), 20 octobre 2022

L'autorité de contrôle italienne a sanctionné un hôpital pour avoir transféré un rapport médical au mauvais destinataire.

A la suite d'une erreur humaine, un hôpital a transmis par courriel un « *rapport d'anatomie pathologique* » en intervertissant deux patients.
L'un des patients a immédiatement signalé cette erreur et a déposé une plainte auprès de l'autorité de contrôle italienne.
L'enquête initialement dirigée contre l'hôpital a été étendue à « *l'institut d'étude et de prévention du cancer* », ce dernier étant, selon l'hôpital et l'autorité de contrôle, le responsable du traitement, l'hôpital n'étant que sous-traitant au sens du RGPD.

Bien que constatant l'existence d'une violation de données, l'autorité de contrôle n'a pas sanctionné le responsable du traitement, considérant que le contrat conclu et que les instructions confiées au sous-traitant étaient satisfaisantes, et surtout qu'à la suite de l'incident, « *l'institut avait mis en œuvre des mesures visant à minimiser le risque de survenance d'évènements similaires* ».
En revanche, l'autorité de contrôle a considéré que l'hôpital, sous-traitant, avait réalisé un traitement de données à caractère personnel en violation des obligations de sécurité imposées par le RGPD.
En conséquence, l'autorité de contrôle italienne a infligé à l'hôpital une amende de 9000 €.

Source : ici

Non-conformité au RGPD d'un enregistrement obtenu de manière illicite

GPDP (Italie), 10 novembre 2022

L'autorité de contrôle italienne a sanctionné un conservatoire national pour avoir utilisé, dans le cadre d'une procédure disciplinaire, un enregistrement obtenu de manière illicite.

Une association d'étudiants d'un conservatoire national de musique a organisé, sur Zoom, une assemblée d'étudiants au cours de laquelle l'un d'eux aurait tenu des propos litigieux envers le conservatoire.

Le conservatoire, qui n'a ni convoqué ni participé à l'assemblé, a indiqué avoir « *trouvé une clé USB contenant le fichier de l'enregistrement vidéo de l'assemblée* », puis, après l'avoir consulté, a fait appel à un expert afin de retranscrire l'enregistrement vidéo.

Considérant que les propos tenus, ainsi retranscrits, étaient pénalement répréhensibles et portaient « *fortement atteinte à la dignité et à l'image du conservatoire* », ce dernier a engagé une procédure à l'encontre de l'étudiant et lui a infligé une sanction disciplinaire.

L'étudiant sanctionné a déposé une plainte auprès de l'autorité de contrôle italienne considérant que le traitement de ses données personnelles était illégal, notamment car il n'avait pas été informé que l'assemblée était enregistrée.

Au cours de son enquête, l'autorité de contrôle, après avoir rappelé que les données à caractère personnel doivent être traitées de manière licite et en respectant le principe de limitation des finalités, a considéré que les données à caractère personnel avaient été traitées en violation des articles 5 et 6 du RGPD.

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

En effet, puisque l'enregistrement avait été acquis de manière « accidentelle », l'autorité de contrôle a estimé que le traitement ultérieur (i) portait sur des données personnelles initialement traitées sans base légale et (ii) était incompatible avec les finalités initiales du traitement.

Compte tenu de ce qui précède, l'autorité de contrôle italienne a infligé au conservatoire une amende de 6.000 €

Source : ici

L'utilisation illégale de données de santé dans un article de blog spécialisé

ANSPDCP (Roumanie), 31 janvier 2023

L'autorité de contrôle roumaine a condamné un cabinet dentaire pour avoir publié, dans un article de blog spécialisé, les données de santé de l'un de ses patients sans son consentement.

Le patient d'un cabinet dentaire a constaté que ses données de santé relatives à son traitement orthodontique (à savoir un ensemble de radiographies et de photographies), avaient été publiées sur un article de blog spécialisé sans son consentement.

Le patient a alerté le cabinet dentaire, qui, bien qu'ayant connaissance de l'existence d'une violation de données de santé, ne l'a pas notifié à l'autorité de contrôle compétente.
Face à l'inaction du cabinet dentaire, le patient a déposé une plainte.

Au cours de son enquête, l'autorité de contrôle a considéré, d'une part, que faute de pouvoir apporter la preuve de l'obtention du consentement du patient, le traitement opéré par le cabinet dentaire n'était fondé sur aucune base légale, méconnaissant ainsi les articles 6 et 9 du RGPD.

L'autorité a constaté, d'autre part, que le cabinet médical, pourtant alerté, n'avait pas notifié la violation de données à l'autorité de contrôle dans les 72 heures, manquant ainsi aux dispositions de l'article 33 du RGPD.

Elle a rappelé, enfin, que dès lors qu'un cabinet dentaire traite des données de santé dans le cadre de la fourniture de soins, l'utilisation de telles données à d'autres fins nécessite (i) de se fonder sur une base légale valide, (ii) d'informer la personne concernée et, (iii) selon les circonstances, de prendre les mesures techniques et organisationnelles adaptées, en particulier d'anonymisation ou de pseudonymisation, ce que le cabinet dentaire n'avait pas fait en l'espèce.

Compte tenu de ces manquements, l'autorité de contrôle a infligé au cabinet médical une amende d'environ 1.000 €.

Source : ici

WhatsApp : interdiction d'inviter un tiers dans un groupe de discussion sans le recueil préalable de son consentement

AEPD (Espagne), 28 décembre 2022

L'autorité de contrôle espagnole a sanctionné un syndicat de copropriétaires pour avoir ajouté un agent d'entretien à un groupe WhatsApp sans son consentement.

Un agent d'entretien a été embauché pour effectuer des travaux de nettoyage dans une copropriété.

Sans que l'agent en soit informé et sans qu'il y ait consenti, son employeur a transmis son numéro de téléphone mobile au syndicat de copropriétaires.

L'agent a, par la suite, été intégré dans un groupe WhatsApp par l'un des membres du syndicat afin qu'il puisse envoyer, en fin de journée, des photos des tâches réalisées.

L'agent s'est plaint auprès de son employeur de la transmission de son numéro de téléphone et a refusé de participer à ce groupe WhatsApp qui n'avait d'autres finalités que de le surveiller. Face à ce refus, l'employeur a licencié l'agent.
Après avoir exercé une demande de droit d'accès auprès du syndicat, restée sans réponse, l'agent d'entretien a déposé une plainte devant l'autorité de contrôle espagnole.

L'autorité de contrôle a considéré que les données personnelles de l'agent d'entretien étaient traitées par le syndicat sans base légale dès lors (i) qu'aucun contrat n'a été signé entre le syndicat et l'agent, (ii) que l'agent n'a pas donné son consentement et (iii) que les droits et intérêt de l'agent prévalaient sur l'intérêt légitime du syndicat.

L'autorité de contrôle a également constaté que le syndicat était dans l'incapacité de prouver qu'il avait répondu à la demande de droit d'accès.

Compte tenu des manquements constatés, l'autorité de contrôle a infligé au syndicat une amende de 2000 €, décomposée comme suit : 1500 € pour absence de base légale et 500 € pour non-réponse au droit d'accès.

Source : ici

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* » (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 2023 :
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