NEWSLETTER RGPD/DATA

NUMÉRO 57 ● 2023

SOMMAIRE

ACTUALITE

SANCTION DE SAF LOGISTICS PAR LA CNIL : UN FORMULAIRE DE MOBILITE INTERNE UN PEU TROP ETOFFE

Le 18 septembre 2023, la CNIL a sanctionné la société SAF LOGISTICS, qui traitait, dans le cadre d'opérations de mobilités internes, des données personnelles de salariés allant au-delà des besoins du traitement.

Un salarié de SAF LOGISTICS, société de fret aérien et filiale française d'une société chinoise, a alerté la CNIL quant aux données personnelles collectées dans le cadre d'un processus de recrutement interne au groupe, destiné aux salariés en France souhaitant travailler en Chine, pour l'entité chinoise.

Sur la base de ce signalement, la CNIL a procédé à un contrôle sur place.

Tout d'abord, la CNIL a relevé un manquement au principe de minimisation, SAF LOGISTICS collectant l'identité, les coordonnées, les fonctions, l'identité de l'employeur et la situation maritales des membres de la famille des salariés concernés. Pour la CNIL, cette collecte allait bien au-delà de ce qui était nécessaire dans le cadre du traitement, dont l'objet était de pouvoir contacter les proches du salarié concerné en cas d'urgence.

Dans la même veine, la CNIL a constaté que SAF LOGISTICS collectait le groupe sanguin, l'appartenance ethnique et l'affiliation politique des salariés, ce qui constitue un manquement au principe d'interdiction de traiter des données sensibles, dans la mesure où SAF LOGISTICS ne justifie d'une quelconque exception à ce principe.

Par ailleurs, sans que cela ne soit directement lié aux opérations de mobilités internes, SAF LOGISTICS conservait les extraits de casier judiciaires (bulletin n°3) de ses salariés, alors même que ceux-ci faisaient déjà l'objet d'une habilitation délivrée par les autorités compétentes après enquête administrative. La CNIL a donc considéré que SAF LOGISTICS ne remplit pas les conditions nécessaires pour consulter ou conserver les casiers judiciaires de ses salariés, caractérisant un manquement à l'interdiction de traiter les données relatives aux infractions, condamnations et mesures de sûreté.

Enfin, il a été relevé un manquement à l'obligation de coopération avec la CNIL. En effet, le formulaire de mobilité interne utilisé par SAF LOGISTICS lui avait été fourni par sa société mère et était donc rédigé en langue chinoise. Pour satisfaire la demande de la CNIL d'obtenir un formulaire en langue française, SAF LOGISTICS avait procédé à sa traduction, mais de façon incomplète, effaçant sciemment les champs relatifs aux données sensibles.

L'ensemble de ces manquements a conduit la CNIL à prononcer une amende administrative de 200.000 € à l'encontre de SAF LOGISTICS.

Source : ici

DEREFERENCEMENT : QUAND LE CONSEIL D'ETAT DEJUGE LA CNIL

Par une décision du 20 avril 2023, le Conseil d'Etat a enjoint à la CNIL à mettre en demeure Google de déréférencer un article relatant la condamnation pénale d'un homme.

Le 20 janvier 2017, le journal « La Montagne » publiait un article sur son site internet relatant la condamnation d'un homme, quelques jours plus tôt, à trois ans de prison pour, notamment, des faits d'escroquerie.

L'homme, constatant, en saisissant son nom sur le moteur de recherche Google, que ledit article apparaissait dans les résultats, a mis en demeure Google de déréférencer l'article, puis, face au refus de ce dernier, a saisi, en vain, la CNIL afin qu'elle enjoigne à Google de procéder audit déréférencement. Dans ce contexte, l'homme a formé un recours en excès de pouvoir contre la décision de la CNIL.

Le Conseil d'Etat, après avoir rappelé le contenu du droit à l'effacement de l'article 17 du RGPD, a fait application de la jurisprudence de la CJUE (C-136/17), en considérant que :

- « *Lorsque des liens accessibles depuis un moteur de recherche mènent vers des pages web contenant des données à caractère personnel relatives à des procédures pénales […], l'ingérence dans les droits […] de la personne concernée est susceptible d'être particulièrement grave en raison de la sensibilité de ces données.*

- *Il s'ensuit qu'il appartient en principe à la CNIL, saisie d'une demande tendant à ce qu'elle mette l'exploitant d'un moteur de recherche en demeure de procéder au déréférencement de liens renvoyant vers de telles pages web, publiées par des tiers et contenant de telles données, de faire droit à cette demande.*

- *Il n'en va autrement que s'il apparaît, compte tenu du droit à la liberté d'information, que l'accès à une telle information à partir d'une recherche portant sur le nom de la personne concernée est strictement nécessaire à l'information du public.* »

La Conseil d'Etat a ajouté que :

« *Pour apprécier s'il peut être légalement fait échec au droit au déréférencement au motif que l'accès à des données à caractère personnel [est] strictement nécessaire à l'information du public, il incombe à la CNIL de tenir notamment compte,*

- *d'une part, de la nature des données en cause, de leur contenu, de leur caractère plus ou moins objectif, de leur exactitude, de leur source, des conditions et de la date de leur mise en ligne et des répercussions que leur référencement est susceptible d'avoir pour la personne concernée et,*

- *d'autre part, de la notoriété de cette personne, de son rôle dans la vie publique et de sa fonction dans la société. Il lui incombe également de prendre en compte la possibilité d'accéder aux mêmes informations à partir d'une recherche portant sur des mots-clés ne mentionnant pas le nom de la personne concernée* ».

Compte tenu de ce qui précède, le Conseil d'Etat a constaté que :

- d'une part, l'article de presse litigieux (i) se rapporte « *à des faits antérieurs à 2014* » (mais à une condamnation de 2017) (ii) relate « *de façon factuelle le procès et la condamnation* » ; (iii) ne comporte pas « *d'analyses ou de commentaires de nature à nourrir un débat d'intérêt public* », (iv) n'est « *pas accessible en ligne à partir d'autres informations que le nom* » de l'homme et (v) ne peut plus « *être regardé comme reflétant la situation judiciaire [réelle] dès lors que, par un arrêt du 14 mars 2018, la cour d'appel de Riom a réduit la peine infligée* » ;

- d'autre part, le requérant (i) est « *âgé de 68 ans* », (ii) ne peut plus avoir la qualité de dirigeant en raison de la « *peine d'interdiction de gérer* » et (iii) ne jouit pas d'une « *notoriété particulière* », et ;

- enfin, l'affaire n'a « *pas fait l'objet d'autres commentaires publics* » et « *la décision d'appel n'a pas donné lieu à un article de presse référencé par Google* ».

Dans ces conditions, le Conseil d'Etat a considéré que « *eu égard aux répercussions que le référencement de cet article est susceptible d'avoir sur la situation personnelle du requérant, l'accès à ce contenu en ligne à partir du nom de ce dernier ne peut plus être regardé, à la date de la présente décision, comme strictement nécessaire à l'information du public* », et a enjoint la CNIL de mettre en demeure la société Google de procéder au déréférencement demandé.

Source : ici

PROSPECTION COMMERCIALE, INFORMATION DES PERSONNES, VIOLATION DE DONNEES : GROUPE CANAL + SANCTIONNE PAR LA CNIL A UNE AMENDE DE 600.000 €

La CNIL a sanctionné la société GROUPE CANAL + pour divers manquements relatifs à la prospection commerciale, à l'information des personnes et aux obligations en matière de violation de données.

A la suite d'une trentaine de plaintes, la CNIL a procédé à un contrôle en ligne, sur le site web www.canalplus.com, suivi d'un contrôle sur pièces, qui ont mis en lumière un certain nombre de manquements.

Manquements commis dans le cadre des activités de prospection commerciale

En premier lieu, la CNIL a relevé que GROUPE CANAL + faisait appel à des prestataires collectant, pour son compte, des données personnelles, en vue de réaliser des opérations de prospection par voie électronique.

La CNIL a observé que, si le formulaire de collecte utilisé par ces prestataires comprenait bien une case à cocher permettant de formaliser le consentement de la personne concernée à la réception de prospection commerciale, ce formulaire ne mentionnait pas, néanmoins, que ces messages de prospection commerciale étaient adressés de la part de GROUPE CANAL +. Ainsi, le consentement, à défaut d'être éclairé, ne pouvait être considéré comme valablement recueilli.

Par ailleurs, les prestataires de GROUPE CANAL +, lors des appels téléphoniques passés auprès des prospects, ne délivraient pas d'information « RGPD » satisfaisante.

De surcroit, certains sous-traitants ne disposaient pas d'un contrat signé répondant aux exigences de l'article 28 du RGPD.

Manquements à l'obligation d'information des personnes

La CNIL s'est également intéressée à l'information des personnes procédant à la création d'un compte pour le service MyCanal, proposé par GROUPE CANAL +. Elle a relevé que la durée de conservation des données faisait l'objet de développements dans la politique de confidentialité, sans être, toutefois, suffisamment définies, traduisant une information des personnes insuffisante.

Manquements aux obligations en matière de violation de données

Enfin, GROUPE CANAL + a omis de notifier à la CNIL une violation de données, constituée par un dysfonctionnement de l'espace client CANAL + ayant permis à des abonnés accédant à leur compte, de visualiser les informations relatives à d'autres abonnés, telles que leur adresse postale et leur numéro de téléphone, ce pendant un peu plus de 5h.

En raison de ces manquements, la CNIL a prononcé une amende administrative d'un montant de 600.000 € à l'encontre de GROUPE CANAL +.

Source : ici

DOCTRINE

RGPD

Diffusion sur les réseaux sociaux d'une vidéo non consentie

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 nationales et européennes. Ce mois-ci, il se penche sur la problématique de la diffusion de vidéos sur les réseaux sociaux, enregistrées et publiées sans le consentement de la personne concernée.

Le mois dernier, nous avons traité la question de l'application du RGPD aux traitements réalisés par les particuliers[1].

À la lumière de plusieurs décisions[2], nous avons constaté que les autorités de protection des données et la CJUE avaient tendance à faire application de la règlementation sur la protection des données chaque fois que le traitement réalisé par un particulier dépasse la sphère strictement privée. En d'autres termes, il est fait application du RGPD si la sphère publique est impactée, soit parce que les données enregistrées concernent des personnes extérieures à la sphère privée de la personne qui réalise le traitement (exemple des caméras qui filment l'espace public), soit parce que les données ont été rendues accessibles à un nombre indéfini de personnes (exemple de la publication de données sur internet). Nous avons alors fait le constat d'un champ d'application matériel du RGPD particulièrement large et avons soulevé quelques questions : un particulier qui filmerait ses amis sur la voie publique et donc qui, par la même occasion, capterait l'image des passants, serait-il contraint de respecter toutes les obligations qui pèsent sur un responsable du traitement (minimisation, transparence, etc.) ? Qu'en serait-il également d'une publication sur les réseaux sociaux d'un « *selfie* » pris dans un lieu privé sur lequel apparaitraient des personnes autres que la personne concernée ? Ce mois-ci, nous allons tenter de répondre à ces différentes questions.

En application de l'article 6 du RGPD, le traitement de données personnelles n'est licite que sous réserve qu'il repose sur une des six bases légales qu'il énumère : le consentement (la personne concernées a consenti au traitement de ses données) ; le contrat (le traitement est nécessaire à l'exécution ou à la préparation d'un contrat avec la personne concernée) ; l'obligation légale (le traitement est imposé par un texte légal) ; la mission d'intérêt public (le traitement est nécessaire à l'exécution d'une mission d'intérêt public) ; l'intérêt légitime (le traitement est nécessaire à la poursuite d'intérêts légitimes de l'organisme qui traite les données, dans le strict respect des droits et intérêts des personnes dont les données sont traitées) ; la sauvegarde des intérêts vitaux (le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée, ou d'un tiers). Autrement dit, le traitement est illicite s'il ne repose sur aucune de ces bases légales.

L'affaire[3]

Alors qu'une jeune femme, en état d'ébriété manifeste, titubait sur la voie publique tout en essayant de s'accrocher à une poubelle pour garder l'équilibre, une personne inconnue s'est approchée d'elle avec son véhicule et, avec son téléphone portable depuis le siège conducteur, a enregistré la scène pendant plus d'une minute. Le visionnage de la vidéo montrait que la personne, qui enregistrait, se moquait éperdument de la jeune femme, et ce sans aucune raison apparente et sans jamais chercher à lui porter assistance. Par la suite, la jeune femme découvrit que la vidéo en question – dans laquelle elle est parfaitement reconnaissable - a été diffusée par son auteur d'abord à quelques personnes par l'application Whatsapp, puis plus largement sur les réseaux sociaux Facebook, Instagram, Twitter et Youtube. C'est dans ce contexte que la jeune femme a déposé une plainte devant l'autorité espagnole de protection des données (l'AEPD).

Après avoir rappelé que l'image d'une personne physique identifiée ou identifiable est une donnée à caractère personnel et que sa diffusion sur internet s'analyse comme un traitement au sens du

RGPD, l'AEPD s'est intéressée à la question de la licéité d'un tel traitement : « *À la lumière des pièces du dossier administratif, il est clair que le mis en cause a diffusé via les réseaux sociaux, sans aucune base légale telle que prévue à l'article 6.1 du RGPD qui légitimerait le traitement de l'image (le plaignant indiquant expressément ne pas avoir donné son consentement), une vidéo dans laquelle la plaignante apparaît dans une situation délicate. Tout au long de la minute et trente-cinq secondes que dure la vidéo, le visage de la personne concernée est visible, ce qui permet de l'identifier clairement.* » Partant, l'autorité espagnole de protection des données, qui a estimé que les faits litigieux constituent une violation de l'article 6.1 du RGPD (le traitement étant dépourvu de base légale), a prononcé une amende de 10.000 euros à l'encontre de l'auteur de la vidéo.

Quelles recommandations ?

Le champ d'application du RGPD est finalement plus large qu'on pouvait l'imaginer initialement, puisqu'il ne s'applique pas qu'aux traitements réalisés par des professionnels. Il s'applique également aux traitements mis en œuvre par les particuliers, et ce chaque fois que ces traitements dépassent le cadre strictement privé de celui qui en est à l'origine. Tel est notamment le cas d'une publication par une personne sur un réseau social des données personnelles concernant une autre personne, comme l'image de cette dernière.

Le « *responsable* » d'un tel traitement doit donc respecter toutes les obligations du RGPD. À cet égard, il doit s'assurer que le traitement en question repose sur une base légale. Or, sauf à ce que la personne concernée ait consentie à la captation de son image et à sa diffusion sur internet, il est peu probable que le responsable du traitement puisse s'appuyer sur un autre fondement de l'article 6.1 pour justifier la licéité d'un tel traitement. Cela signifie donc que l'auteur d'une publication sur un réseau social, qui ne serait pas en mesure de démontrer le consentement des personnes figurant sur celle-ci, serait « *en infraction* » par rapport aux dispositions de la règlementation sur la protection des données personnelles. Ne sommes-nous pas, dans ces conditions, tous des délinquants du web ?

Alexandre FIEVEE
Avocat associé
Derriennic Associes

Notes

(1) Expertises, n° 493, septembre 2023, p. 282.

(2) CJUE, 6 novembre 2003, C-101/01 ; CJUE, 11 décembre 2014, C-212/13 ; GPDP, 27 avril 2023, n° 9896468 ; autorité de protection des données belge, 24 novembre 2020, DOS-2019-04412 ; autorité de protection des données islandaise, 14 juin 2023, affaire n° 2022030544 ; autorité de protection des données belge, 20 mars 2023, DOS-2022-00945.

(3) AEPD, EXP202204530, 28 août 2023.

RGPD : UN LABORATOIRE D'ANALYSES MEDICALES INVOQUE SA QUALITE DE SOUS-TRAITANT POUR SE DEDOUANER DE TOUTE RESPONSABILITE

Parce que certains traitements présentent des risques « d'une ampleur particulièrement importante » (les traitements dits « critiques ») et qu'ils sont la cible « des attaquants qui disposent de fortes capacités ou de fortes motivations », la CNIL a rédigé un projet de recommandation relative aux modalités de sécurisation de ces traitements[1].

C'est quoi un traitement critique ?

C'est un traitement qui répond aux deux conditions suivantes :

- Il est réalisé « *à grande échelle* » au sens du RGPD ;
- Il est celui pour lequel une violation de données pourrait soit entraîner des conséquences très importantes pour les personnes concernées, soit entraîner des conséquences pour la sûreté de l'État ou pour la société dans son ensemble (en raison de la perte de confidentialité, d'intégrité ou de disponibilité des données).

Parmi les exemples de traitements critiques, la CNIL vise « *les traitements de santé à grande échelle, aussi bien dans le cadre du soin, de la gestion des épidémies, de la recherche ou des mutuelles* ».

La nécessité d'une gouvernance de la protection des données personnelles

Selon la CNIL, la protection des données personnelles concernées par des traitements critiques devrait se traduire par la mise en place d'une gouvernance dédiée. A ce titre, l'autorité précise que la protection de telles données devrait être un « *enjeu* » porté par la direction générale de l'organisme, qui devrait s'assurer que les moyens suffisants sont mobilisés pour garantir la sécurité de ces traitements.

Par ailleurs, la CNIL estime que chaque organisme devrait désigner un référent en matière de protection des données personnelles et de sécurité pour le traitement concerné et se fixer des objectifs, (i) traduits en règles de fonctionnement et (ii) formalisés dans une politique de sécurité. Elle ajoute que la sécurité devrait faire l'objet d'une « *démarche d'amélioration continue* », afin de permettre une « *progression constante* ». Un bilan de sécurité pourrait être réalisé de manière annuelle pour « *tirer les leçons des éventuels incidents de sécurité* » et « *identifier et mettre en œuvre, sous la forme d'un plan d'action, les axes de progression* ».

La nécessité d'une démarche de gestion des risques

Pour la CNIL, les traitements critiques devraient « *systématiquement* » faire l'objet d'une analyse d'impact, avec une mise à jour régulière pour une prise en compte de l'évolution des risques. Par ailleurs, la CNIL recommande que ces traitements fassent l'objet d'une homologation de sécurité avant leur mise en œuvre. Cela consisterait à « *faire valider par la personne sous l'autorité de laquelle le traitement est mis en œuvre (par exemple, le directeur général dans une entreprise ou la personne délégataire du pouvoir de décision) le niveau de sécurité du traitement, les risques résiduels identifiés et le plan d'action visant à maintenir et à améliorer le niveau de sécurité du traitement dans le temps* ».

Sur l'absence d'analyse d'impact

Après avoir un moment soutenu, comme indiqué supra, qu'il n'était pas tenu de réaliser une analyse d'impact compte tenu de sa qualification de sous-traitant, le laboratoire a, une fois sa qualité de responsable du traitement reconnue, justifié l'absence d'un tel document au motif qu'il n'était pas contraint d'en rédiger un dès lors qu'au moment de la plainte, il ne traitait pas de données personnelles « à grande échelle ». Il reconnaissait, en revanche, que, depuis le COVID-19, le nombre d'analyses avait sensiblement augmenté et qu'il rentrait désormais dans les conditions d'un traitement de données de santé à grande échelle, expliquant ainsi qu'il ait bien réalisé, depuis, une analyse d'impact.

Selon la Chambre contentieuse, il ne fait aucun doute que la partie défenderesse aurait dû, bien avant le COVID-19 (et donc avant que la plainte ne soit introduite), réaliser une analyse d'impact. En tout de cause, elle aurait dû, ce qu'elle n'a pas fait, documenter les raisons pour lesquelles elle considérait ne pas être tenue de réaliser une telle analyse : « Elle estime qu'elle effectue dorénavant des traitements à grande échelle. La défenderesse aurait dû, sur la base du principe de responsabilité de l'article 24, clarifier son interprétation de la notion de « grande échelle » en indiquant les critères objectifs sur lesquels elle se base pour estimer que ses activités ont fini par entrer dans la catégorie des traitements à grande échelle, alors que selon elle, elles ne remplissaient pas ce critère au départ. »

Sur l'information des patients

Le dernier grief fait au laboratoire concernait l'absence de politique de protection des données disponible sur son site internet. Pour sa défense, le laboratoire a d'abord invoqué sa qualité de sous-traitant pour expliquer qu'il n'était pas tenu à la moindre obligation d'information à l'égard des patients.

Puis, après avoir reconnu l'évidence, il soutenait qu'aucun manquement ne pouvait lui être reproché dès lors qu'un affichage était réalisé dans les centres de prélèvement et que le RGPD n'impose pas qu'une information soit publiée sur le site web. Soulignant que le laboratoire ne rapportait pas la preuve que la politique de protection des données faisait l'objet d'un affichage dans ses centres de prélèvement, la Chambre contentieuse a considéré, qu'en ne publiant pas l'information requise sur son site internet, la partie défenderesse avait violé les articles 12, 13 et 14 du RGPD.

Malgré ces divers manquements, l'APD s'est montrée plutôt clémente en prononçant une amende administrative de 20.000 euros, correspondant à seulement 0,07% du chiffre d'affaires annuel du laboratoire pour l'année 2020[1].

[1] APD, 19 août 2022, 127/2022.

Lien vers l'article original : ici

PANORAMA EUROPÉEN

PANORAMA DE QUELQUES DECISIONS RENDUES PAR DES AUTORITÉS NATIONALES DE CONTRÔLE

Sanction du responsable du traitement qui n'a pas limité les accès aux données de santé aux seuls employés ayant besoin d'en connaître

Danemark, 13 octobre 2023

L'autorité de protection des données danoise a sanctionné la région du Sjælland pour n'avoir pas limité l'accès à des données de santé aux seuls employés ayant besoin d'en connaitre dans le cadre de leurs missions.

De nombreux employés de la région du Sjælland, au Danemark, avait accès à partir de 2017 à la « *liste des patients de tous les hôpitaux de la région* », ainsi qu'à leurs données personnelles telles que leur numéro de sécurité sociale ainsi que les diagnostics et soins reçus. La région considérait que cet accès, ouvert à plus de 16.000 employés, était nécessaire pour assurer la « *sécurité du traitement des patients* » et servait « *d'outil de travail interdisciplinaire entre les professionnels de santé* », raison pour laquelle toute personne disposant d'un accès à la « plateforme santé » avait la possibilité d'accéder à la liste des patients. L'un des salariés, considérant lesdits accès comme illicites, a déposé une plainte devant l'autorité de contrôle danoise.

L'autorité de contrôle a considéré que :

- En premier lieu, « *si le secteur de la santé peut parfois avoir besoin d'un accès élargi aux données personnelles* », le responsable du traitement doit, en tout état de cause, « *veiller à ce que cet accès élargi ne soit accordé qu'aux salariés qui ont un besoin concret* » d'accéder auxdites données. A défaut d'avoir limité ledit accès, la région n'a, selon l'autorité de contrôle, pas mis en œuvre les mesures de sécurité appropriées ;
- En deuxième lieu, l'accès illicite à des données personnelles par des utilisateurs autorisés est un « *scénario réel et fréquent qui conduit à une violation de la sécurité des données personnelles* ». Qu'ainsi, en ne disposant pas de système de journalisation des accès permettant de suivre et documenter toute utilisation abusive des données, la région n'a pas mis en œuvre les mesures de sécurité appropriées

Compte tenu de ce qui précède, l'autorité de contrôle danoise (i) a prononcé un avertissement à l'encontre de la région et (ii) l'a enjoint, d'une part, à procéder à un audit de l'ensemble de son système informatique afin de s'assurer que seules les personnes qui ont un « *besoin concret* » puissent accéder aux données et, d'autre part, à instaurer un système de journalisation.

Source : ici

Droit d'accès : rejet d'une demande abusive

Un tribunal allemand a qualifié une demande de droit d'accès d'abusive, considérant que cette dernière n'avait pas pour objectif de vérifier la légalité du traitement, mais avait pour unique objectif de vérifier l'augmentation des cotisations d'un contrat d'assurance.

Dans le cadre d'un litige relatif à l'augmentation des cotisations d'un contrat d'assurance maladie, opposant un assureur à son assuré, ce dernier, considérant que son assureur avait augmenté illégalement et unilatéralement les cotisations, a sollicité de son assureur la transmission de nombreuses informations, telles que (i) le montant des ajustements des cotisations, (ii) les certificats d'assurance et (iii) les avenants d'assurance.

Considérant avoir droit au remboursement des primes payées en trop, l'assuré était cependant tributaire de la transmission desdites informations pour pouvoir procéder au calcul du trop payé.

Face au refus de l'assureur de transmettre lesdites informations, l'assuré a saisi les juridictions allemandes. Il considérait, notamment, que le refus de l'assureur était contraire au droit d'accès défini à l'article 15 du RGPD.

Le tribunal allemand a rejeté la demande de l'assuré.

Selon le tribunal, si, certes, certaines des informations demandées par l'assuré peuvent constituer des données personnelles au sens du RGPD, le tribunal a rappelé l'exception au droit d'accès posée à l'article 12 du RGPD, selon laquelle : « *Lorsque les demandes d'une personne concernée sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif, le responsable du traitement peut : […] b) refuser de donner suite à ces demandes*. »

Selon le tribunal, l'utilisation du mot «*notamment* » montre que la disposition vise également à couvrir d'autres demandes abusives.

Justement, rappelant conformément au considérant 63 du RGPD que la finalité du droit d'accès est « *de permettre à la personne concernée de prendre connaissance du traitement […] pour pouvoir en vérifier la légalité* », et constatant, selon les propres propos de l'assuré, que ce dernier n'a nullement pour ambition de vérifier la licéité du traitement mais a seulement pour objectif « *de vérifier d'éventuelles adaptations de cotisations effectuées par l'assureur* », le tribunal a considéré que la demande n'était pas fondée sur l'objectif de protection du RGPD.

Plus précisément, le tribunal, rappelant le principe selon lequel un demandeur au droit d'accès n'a pas à motiver sa demande d'accès, a considéré, (i) que ce dernier ne manifestait pas son intérêt à vérifier la légalité du traitement des données dans sa requête, mais plus encore que (ii) « *l'intérêt en matière de protection des données n'était manifestement pas poursuivi du tout* », justifiant le rejet de la demande.

Source : ici

La présence de données personnelles sur des panneaux d'information est contraire au RGPD

AEPD (Espagne), 24 mars 2023

L'autorité de contrôle italienne a sanctionné une autorité sanitaire qui, par inadvertance, avait laissé présentes des données personnelles sur un panneau d'information affiché à l'entrée d'un hôpital.

Une autorité sanitaire italienne a réalisé un panneau d'information qu'elle a affiché à l'entrée des urgences d'un hôpital.

Ce panneau, qui avait pour objectif d'informer les personnes sur l'interdiction d'accès des accompagnants et des visiteurs, comportait la photographie d'un professionnel de santé assis derrière son bureau et consultant le dossier médical d'un patient.

Malencontreusement, on pouvait distinctement voir sur la photographie les données personnelles du patient dont le dossier médical était ouvert, et notamment son nom, prénom, date et lieu de naissance, adresse, numéro de sécurité sociale, ainsi que des données relatives à son hospitalisation, son diagnostic et le traitement qui lui a été prescrit.

Le patient, alerté de l'existence de ce panneau d'information, a déposé une plainte auprès de l'autorité de contrôle italienne.
Cette dernière a considéré que le traitement de données personnelles, y compris de données de santé, était contraire :

- Au principe de licéité (article 5.1.a du RGPD)
- Au principe de minimisation des données (article 5.1.c du RGPD) ;
- Au principe d'intégrité et de confidentialité (article 5.1.f du RGPD) ;
- Au principe d'interdiction des traitements de données sensibles (article 9 du RGPD),
- Aux principes de protection des données dès la conception et protection des données par défaut (article 25 du RGPD).

GPDP | GARANTE PER LA PROTEZIONE DEI DATI PERSONALI

Compte tenu de ces violations, l'autorité de contrôle italienne a infligé à l'autorité sanitaire une amende de 20.000 €

Source : ici

Quand l'accessibilité l'emporte sur la sécurité des données

Un juge allemand a sanctionné un responsable du traitement qui invoquait des mesures de sécurité pour faire échec à une demande d'accessibilité.

Une personne aveugle, bénéficiaire d'une allocation auprès de l'organisme de « pôle emploi » allemand, a demandé à ce dernier de ne plus lui transmettre les différentes communications et formulaires par courrier postal, mais par courrier électronique ou, à défaut, sur un support de données numérique.

Effectivement, en raison de sa déficience visuelle, la personne concernée était difficilement capable de lire des documents papiers, mais disposait d'un logiciel de lecture lui permettant de lire les documents numériques au format word ou pdf.
Accusant réception de la demande de la personne concernée, l'organisme n'y a pas fait droit en considérant que la communication de tels documents sous forme électronique est contraire à l'obligation de sécurité qui pèse sur le responsable du traitement, conformément à l'article 32 du RGPD.

Plus précisément, selon l'organisme :

- l'utilisation de supports de données (clé usb ou CD) n'est pas autorisée au sein de l'organisme, et ;

- « *la communication par courriel n'est possible, pour des raisons de sécurité, que si les courriels peuvent être envoyés cryptés* ». Or, l'envoi de tels courriels (i) nécessitait que l'individu (i) possède un très haut niveau de savoir-faire technique, ce qu'il n'avait pas et (ii) supposait qu'il paye un certificat permettant le déchiffrement.

La personne concernée a donc saisi les tribunaux allemands qui ont considéré que, si l'article 32 du RGPD oblige le responsable du traitement à mettre en œuvre toutes les mesures appropriées afin de garantir un niveau de sécurité adapté, cet article «*n'exige pas à tout prix la sécurité des données* », mais, au contraire, suppose de « *trouver un équilibre* ».

Plus encore, le tribunal a considéré que les raisons invoquées par l'organisme pour refuser ladite transmission n'étaient pas valables puisque :

- elles ne prennent pas en compte la situation particulière de la personne concernée ;

- la personne concernée a consenti au traitement, et ;

- l'article 32 n'oblige pas la transmission de courriels cryptés, ou plus spécifiquement, l'organisme ne démontrait pas avoir procédé à « l'évaluation du niveau de sécurité approprié » et justifié en quoi une telle mesure de sécurité était indispensable.

Compte tenu de ce qui précède, le tribunal a considéré le refus du responsable du traitement comme illégal et a indiqué qu'un prestataire de services est tenu de transmettre à une personne handicapée, qui en fait la demande, les documents par voie électronique.

ACTUALITES DU CABINET

Matinale du 9 novembre 2023 présentée par le pôle RGPD et le pôle droit social du cabinet Derriennic Associés

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