NEWSLETTER RGPD/DATA

NUMÉRO 56 ● 2023

SOMMAIRE

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

EN BREF

BCR

- Le CEPD a adopté, le 20 juin 2023, la version finale de ses recommandations en matière de règles d'entreprise contraignantes (ou binding corporate rules, « BCR ») « responsable du traitement ». Ce document énumère de manière détaillée les éléments devant figurer respectivement dans le formulaire de soumission, ainsi que dans les BCR elles-mêmes, et clarifie certains aspects procéduraux. Ces recommandations prennent en compte les retours issus de la consultation publique qui s'est déroulée entre novembre 2022 et janvier 2023. Ainsi, certains aspects procéduraux ont été clarifiés, tels que l'applicabilité des recommandations ou encore la notification annuelle à transmettre à l'autorité de contrôle en charge de l'instruction. Ces recommandations sont d'ores et déjà applicables à toute entité partie à des BCR « responsable du traitement.

CERTIFICATION DPO

- Quelques changements ont été apportés, mais ils concernent principalement les modalités d'obtention, par les organismes certificateurs, de leur agrément. « Les fondamentaux de la certification demeurent inchangés pour les candidats à la certification », précise la CNIL. Ainsi, les prérequis et les conditions d'obtention de la certification pour les candidats restent inchangés : il faut justifier de deux ans d'expérience professionnelle dans le domaine de la protection des données ou de deux ans d'expérience professionnelle dans tout domaine complétée de trente-cinq heures de formation en protection des données. Bonne nouvelle : il est désormais possible pour un organisme certificateur de proposer aux candidats de passer l'épreuve de certification à distance.

DPO SOUS PRESSION

- Une enquête récente de l'AFCDP démontre que les DPO sont de plus en plus sous pression. En cause, le cadre relatif aux échanges de données avec les Etats-Unis toujours flou, l'inflation des règles et recommandations, et surtout le prononcé de sanctions de plus en plus en sévères par la CNIL.

ACTUALITE

MISE A JOUR DU REFERENTIEL CNIL « ALERTES PROFESSIONNELLES »

Le 6 juillet dernier, la CNIL a mis à jour son référentiel « alertes professionnelles », à la suite de la transposition par la France de la directive européenne sur la protection des personnes qui signalent des violations du droit de l'Union.

Quels sont les principaux changements :

- Un élargissement des catégories des personnes auxquelles l'accès au dispositif d'alertes professionnelles doit être garanti par l'organisme mettant en place un tel dispositif ;
- Un élargissement des finalités du traitement des données collectées ;
- La description des différentes phases de traitement de l'alerte ;
- La durée de conservation des alertes (concernant notamment la liste des finalités pouvant justifier la conservation des données d'alerte) ;
- Le traitement des signalements anonymes (notion propre à la loi Sapin 2 et qui doit être distinguée de celle d'« anonymisation des données » au sens du RGPD);
- La possibilité de confier la gestion de certaines opérations de traitement à des tiers (avec une distinction entre l'« externalisation » et la « mise en commun des ressources »).

La CNIL rappelle que ce référentiel n'a pas de valeur contraignante et que, par conséquent, les organismes peuvent s'en écarter. Toutefois, « il leur appartient (…) de justifier et de documenter ce besoin et les mesures mises en œuvre afin de garantir la conformité des traitements à la réglementation en matière de protection des données à caractère personnel. »

Source : ici

LE PRINCIPE DE MINIMISATION CEDE-T-IL FACE AU DROIT A LA PREUVE D'UNE DISCRIMINATION ?

Dans un arrêt du 6 juillet 2023, la Cour d'appel de Paris a fait application du principe de minimisation pour déterminer dans quelle mesure un employeur peut communiquer les données personnelles de ses salariés à un autre salarié qui s'estime victime de discrimination.

Un salarié, embauché en 2009 par la société Franfinance et dont le contrat a été transféré en 2015 à la Société Générale, a constaté que, depuis son embauche, sa carrière n'avait pas évolué, pas plus que sa rémunération.

Considérant justifier d'un motif légitime, le salarié, sur le fondement de l'article 145 du Code de procédure civile qui permet d'obtenir en référé la production d'éléments permettant d'établir « avant le procès, la preuve de faits laissant présumer l'existence d'une discrimination ou d'une inégalité de traitement », a saisi le Conseil de prud'homme de Paris aux fins de voir ordonner « la communication d'un certain nombre de pièces ».

Face au rejet de sa demande par le Conseil de prudhommes, le salarié a interjeté appel de cette ordonnance devant la Cour d'appel de Paris.

Devant la Cour, et toujours sur le même fondement, le salarié sollicitait la communication de deux tableaux :

Un premier répertoriant les éléments de carrière de tous les salariés occupant ou ayant occupé un poste similaire au sien depuis 2015 (date de transfert du contrat) et indiquant le genre, l'année de naissance, les diplômes, le poste d'affectation, la rémunération ainsi que l'évolution des salariés sur les dernières années

Un second répertoriant les mêmes éléments, mais cette fois-ci s'appliquant à tous les salariés embauchés entre 2008 et 2010.

En défense, la Société Générale considérait que la demande du salarié, en plus de n'être fondée sur aucun motif légitime, est contraire au RGPD car il n'est pas démontré en quoi il est nécessaire de porter atteinte à la vie privée des salariés concernés par la demande. Subsidiairement elle sollicitait, a minima, l'anonymisation desdites informations.

La Cour d'appel a considéré qu'il découlait du principe de minimisation posé par le RGPD, que, lorsque seule une partie des données est nécessaire à des fins probatoires, il peut être envisagé des mesures supplémentaires en matière de protection des données telles que la pseudonymisation des noms des personnes concernées ou toute autre mesure destinée à minimiser l'entrave au droit à la protection des données à caractère personnel.

En l'espèce, cependant, relevant que la demande du salarié concerne essentiellement « l'identité, la carrière, la qualification et la rémunération des salariés » et exclut la communication de données telles que « l'adresse personnelle et des données bancaires ou fiscales », la Cour a considéré que la communication de listes nominatives de salariés comportant leur patronyme, âge, genre, carrière, qualification et rémunération est indispensable pour permettre d'apprécier l'existence et la cause de la discrimination alléguée.

Compte tenu de ce qui précède, la Cour d'appel a infirmé l'ordonnance du Conseil de prud'hommes et fait droit à la demande du salarié en condamnant la Société Générale à fournir le premier tableau, sans qu'il soit nécessaire d'anonymiser les données. En revanche, du fait du transfert du contrat en 2015, la Cour d'appel a considéré que la communication du second tableau n'était pas justifiée.

Source : ici

L'AVIS CNIL SUR LE DECRET DEDIE A LA VIDEOPROTECTION DANS LE CADRE DES JO

Le 15 juin 2023, la CNIL a rendu un avis portant sur le projet de décret organisant les traitements algorithmiques des images qui seront collectées par les caméras installées sur des aéronefs, dans le cadre des jeux Olympiques.

La loi n° 2023-380 relative aux Jeux Olympiques et Paralympiques de 2024 a été promulguée le 19 mai 2023. Celle-ci instaure un cadre expérimental permettant la mise en œuvre de traitements algorithmiques d'analyse automatisée des images provenant des dispositifs de vidéoprotection et de caméras installées sur des aéronefs afin de détecter et de signaler en temps réel des évènements prédéterminés.

Les traitements prévus par cette loi, mis en œuvre par les forces de l'ordre, ont pour objet d'assurer la sécurité des manifestations sportives, récréatives ou culturelles exposées à des risques d'actes de terrorisme ou d'atteinte grave à la sécurité des personnes.

Un projet de décret a été pris en application de cette loi. Il vise à fixer les caractéristiques des traitements et à indiquer les évènements que les traitements ont pour objet de signaler.

L'avis rendu par la CNIL au sujet de ce décret comprend une recommandation « qu'aucun transfert de données hors de l'UE ou accès aux données par des autorités étrangères ne puisse avoir lieu, autant en phase de conception [de l'algorithme] que d'exploitation ».

Cette recommandation tient compte « du caractère novateur et de la haute technicité de ces traitements algorithmiques, des risques qu'il peuvent impliquer par nature pour les libertés individuelles et de leur déploiement inédit et en conditions réelles ».

Par ailleurs, s'agissant de l'information des personnes quant à la collecte de leur image par des caméras « augmentées », la CNIL « insiste fortement sur la nécessité de prévoir systématiquement des modalités d'information directement sur les lieux de captation des images et sur des supports adaptés (panneaux d'information dédiés, vidéos, codes QR, marquage au sol, annonces sonores, etc.) ».

La CNIL prévoit que la fourniture de cette information n'est pas toujours possible et indique que « l'information des personnes ne sera exclue que dans les seuls cas où des aéronefs seraient eux-mêmes déployés dans des conditions qui excluent l'information des personnes ».

S'agissant spécifiquement de la phase de « conception » de l'algorithme, la CNIL demande que les données traitées dans le cadre de cette phase « fassent systématiquement l'objet d'opérations de pseudonymisation ou de floutage lorsque de telles opérations ne compromettent pas la qualité technique du traitement ».

Source : ici

RGPD

Application aux traitements réalisés par des particuliers

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 l'application du RGPD aux traitements « domestiques » réalisés par des personnes physiques.

Il ressort des termes des articles 2.1 et 2.2 du RGPD que la règlementation en matière de protection des données personnelles s'applique à tous les traitements de données à caractère personnel, automatisés ou non.
Il est toutefois précisé que le règlement ne s'applique pas aux traitements effectués par une personne physique « *dans le cadre d'une activité strictement personnelle ou domestique* »[1]. Si le RGPD ne donne pas de définition de ce type d'activités, il précise, dans son considérant 18, qu'il s'agit des traitements « *sans lien avec une activité professionnelle ou commerciale* », comme par exemple : « *l'échange de correspondance* », « *la tenue d'un carnet d'adresses* », « *l'utilisation de réseaux sociaux* » et « *les activités en ligne qui ont lieu dans le cadre de ces activités* ».

Cette dérogation n'est pas nouvelle. Elle était déjà inscrite dans la directive 95/46/CE (que le RGPD a abrogé) qui, dans son article 3.2, excluait de son champ d'application les traitements effectués par une personne physique « *pour l'exercice d'activités exclusivement personnelles ou domestiques* ».

La CJUE avait eu l'occasion, à deux reprises, d'en délimiter les contours. D'abord dans une affaire, dans laquelle il était reproché à une formatrice de communiants d'une paroisse d'avoir publié sur les pages de son site internet personnel (renvoyant vers celui de l'église) des données personnelles concernant d'autres collègues (nom, prénom, coordonnées, situation familiale, etc.).

La CJUE avait considéré que l'exception de l'article 3.2 ne pouvait être invoquée pour faire échec à l'application de la directive car l'exception devait être interprétée « *comme visant uniquement les activités qui s'insèrent dans le cadre de la vie privée ou familiale des individus* », ce qui n'était pas le cas en l'espèce en raison de la publication sur internet de données « *rendues accessibles à un nombre indéfini de personnes* »[2].

L'autre affaire concernait un particulier qui avait installé, au niveau du toit de sa maison, plusieurs caméras filmant à la fois l'entrée de celle-ci, mais aussi la voie publique et la demeure d'en face[3].

La CJUE avait considéré que la dérogation ne n'appliquait pas au cas d'espèce puisque le traitement s'étendait à l'espace public, le dispositif étant dirigé « *vers l'extérieur de la sphère privée* » de celui qui réalisait le traitement.

À la lumière de ce qui précède, on peut s'interroger sur les contours de cette dérogation. Est-ce qu'il faut limiter son champ d'application aux seuls traitements « *sans lien avec une activité professionnelle ou commerciale* » (comme semble l'indiquer le considérant 18 du RGPD) ou l'étendre à des traitements mis en œuvre, certes, dans le cadre d'une activité personnelle (c'est-à-dire « *sans lien avec une activité professionnelle ou commerciale* ») mais qui déborderait de la sphère privée (comme semble l'indiquer la CJUE) ?

Les affaires

Plusieurs autorités nationales de protection des données ont été amenées à se prononcer sur la problématique de l'application du RGPD aux traitements mis en œuvre par des particuliers. Dans deux affaires, il a été fait application du RGPD. Dans deux autres, il a été écarté.

En Italie, une plainte avait été déposée contre un particulier qui - lui aussi - avait installé un dispositif de vidéosurveillance à des fins de sécurité et de protection de sa propriété privée. Mais comme l'angle de vue de deux des caméras utilisées comprenait le passage municipal adjacent au bâtiment,

mais aussi quelques propriétés privées voisines, la question de la licéité de ce dispositif au RGPD s'est posée[4].

Après avoir rappelé que l'utilisation de ce type de dispositif doit être considérée, en principe, comme exclue du champ d'application matérielle du RGPD, l'autorité de protection des données italienne (la « *GPDP* ») a rappelé que cette exclusion suppose que « *la portée de la communication des données ne dépasse pas la sphère familiale du propriétaire et que les images ne sont pas communiquées à des tiers ou diffusées et que le traitement ne s'étende pas au-delà des domaines de stricte pertinence du propriétaire, en prenant des images dans des espaces communs (tels que escaliers, halls d'entrée, parkings), les lieux recevant du public (rues ou places)* ».

Compte tenu de l'angle de vue du dispositif ainsi installé, la GPDP a fait application du RGPD et a infligé une amende au propriétaire en raison du non-respect des articles 5.1. a) (principe de licéité) et 6 (absence de base légale) du RGPD. Dans une affaire plus ancienne, l'autorité de protection des données belge avait - elle aussi - repris le raisonnement de la CJUE pour estimer que le RGPD devait s'appliquer à un système de vidéosurveillance installé par un particulier, comprenant plusieurs caméras orientées vers l'extérieur de la propriété : « *Lorsque le système de vidéosurveillance couvre par exemple l'espace public ou le domaine privé d'autres personnes, même en partie, et qu'il dépasse ainsi la sphère privée des personnes qui traitent des données au moyen de ce système, on ne peut considérer qu'il s'agit d'une activité réalisée exclusivement à des fins personnelles ou domestiques* »[5].

Dans une affaire dans laquelle il était reproché à une voisine d'avoir refusé de supprimer des enregistrements qu'elle faisait des conversations privées de la plaignante, l'autorité de protection des données islandaise n'a pas fait application du RGPD au motif qu'il n'était pas démontré que les enregistrements litigieux avaient été communiqués à d'autres personnes que la plaignante elle-même[6].

Ainsi, il était possible de considérer que le traitement des données personnelles était uniquement destiné à un usage personnel et qu'il était donc en dehors du champ d'application matériel de la règlementation sur la protection des données. Une décision similaire a été rendue par l'autorité de protection des données belge, dans une affaire dans laquelle le plaignant reprochait à son ex-épouse d'avoir obligé ses enfants à installer une application sur un smartphone qu'elle détenait lui permettant ainsi d'accéder à l'historique des conversations entre ses enfants et son ex-mari, afin d'utiliser tout ou partie de ces éléments dans le cadre de la procédure de divorce[7].

Selon l'autorité de contrôle, il convient, pour déterminer si le RGPD s'applique, de rechercher si les données en question ont été ou non rendues accessibles à « *un grand nombre de personnes manifestement étrangères à la sphère privée des personnes concernées* ». Considérant que les conversations litigieuses s'inscrivaient dans « *un cadre strictement privé et limité* », la chambre contentieuse a estimé que les traitements en cause ont eu lieu dans le cadre d'activités strictement personnelles ou domestiques, et que le RGPD ne s'applique pas.

Quelles recommandations ?

À la lumière des décisions susvisées, force est de constater que les autorités de protection des données ne se contentent pas de rechercher si le traitement présente un lien ou non avec « *une activité professionnelle ou commerciale* ». Tout comme la CJUE, dans des décisions qu'elle avait rendu sous l'empire de la directive 95/46/CE, elles vont rechercher si le traitement en cause dépasse ou non la sphère purement personnelle et donc faire application du RGPD chaque fois que 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).

Le champ d'application matériel du RGPD est donc particulièrement large et semble s'étendre à des situations plus nombreuses qu'on n'aurait pu l'imaginer. Un particulier qui filmerait ses amis sur la voie publique, et donc qui filmerait par la même occasion 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 un réseau social d'un « *selfie* » pris dans un lieu privé sur lequel apparaitrait des personnes autres que la personne concernée ? Nous n'avons pas fini de parler du RGPD...

Alexandre FIEVEE
Avocat associé
DERRIENNIC Associés

Notes

(1) Voir également l'article 2 de la loi n°78-17 du 6 janvier 1978 modifiée.

(2) CJUE, 6 novembre 2003, C-101/01.

(3) CJUE, 11 décembre 2014, C-212/13.

(4) GPDP, 27 avril 2023, n° 9896468.

(5) Autorité de protection des données belge, 24 novembre 2020, DOS-2019-04412.

(6) Autorité de protection des données islandaise, 14 juin 2023, affaire n° 2022030544.

(7) Autorité de protection des données belge, 20 mars 2023, DOS-2022-00945.

QUELLES MODALITES DE SECURITE POUR LES TRAITEMENTS CRITIQUES DANS LE DOMAINE DE LA SANTE ?

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 ».

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 ».

La nécessité d'une préparation active à d'éventuels incidents de sécurité ou violation de données

La CNIL recommande que les traitements critiques fassent l'objet de « mesures de traçabilité particulièrement poussées, mises en place dès l'intégration du traitement de données au système d'information et couvrant tous les équipements impliqués dans le traitement de données à caractère personnel ». Elle ajoute que ces mesures de traçabilité devraient s'accompagner de « mesures d'analyse automatique des journaux afin de faciliter la détection des éventuels incidents de sécurité et violations de données ».

Le responsable du traitement devrait, par exemple au moyen d'une procédure dédiée, préciser les critères conduisant à qualifier un incident de sécurité en tant que violation de données à caractère personnel. Par ailleurs, les organismes devraient être dotées d'un centre opérationnel de sécurité (COS ou SOC) disposant d'outils dédiés à l'analyse des journaux et à la détection d'incidents, et notamment d'un système de gestion des informations et des événements de sécurité. En fonction des risques pesant sur le traitement critique, le responsable devrait envisager que l'équipe de détection d'incident soit opérationnelle à tout instant.

La nécessité d'une maîtrise des relations avec les tiers

En plus d'un encadrement contractuel conforme aux exigences des articles 28 du RGPD et 122 de la loi « informatique et libertés », la CNIL estime que des exigences de sécurité devraient être formalisées et détaillées, notamment sous la forme de niveau de service attendu (SLA), « à la hauteur des exigences que le responsable du traitement a identifiées pour le traitement ». De plus, la CNIL recommande qu'en fonction de la criticité de la prestation rendue par le sous-traitant, le responsable du traitement « déploie des efforts proportionnés pour s'assurer du respect des obligations du contrat », en particulier sous la forme d'audits réguliers.

Ce projet est soumis à la consultation jusqu'au 8 octobre 2023 avec pour objectif la confirmation, d'une part, de la notion de « traitements critiques » et, d'autre part, des mesures de sécurité associées. Il est prévu que cette recommandation soit publiée au début de l'année 2024.

[1]https://www.cnil.fr/sites/cnil/files/202308/recommandation_relative_aux_traitements_critiques.pdf

Source : ici

PANORAMA EUROPÉEN

PANORAMA DE QUELQUES DECISIONS RENDUES PAR DES AUTORITÉS NATIONALES DE CONTRÔLE

Sanction d'un laboratoire d'analyses médicales

APD (Belgique), 19 août 2022

En sanctionnant un laboratoire d'analyses médicales, l'autorité de contrôle belge est venue clarifier ou rappeler certains principes du RGPD.

Après avoir réalisé une analyse médicale au sein d'un laboratoire, un patient a découvert que son médecin traitant avait accès à ses résultats par l'intermédiaire du site internet non sécurisé du laboratoire. Constatant également qu'il n'avait pas été informé du traitement de ses données personnelles et soupçonnant le laboratoire de n'avoir pas réalisé d'analyse d'impact, le patient a déposé une plainte auprès de l'autorité de contrôle belge.

- En premier lieu, l'autorité de contrôle belge a précisé qu'un laboratoire d'analyses médicales doit être considéré comme un responsable du traitement. Effectivement, lors de la venue d'un patient, le laboratoire d'analyses médicales « détermine les finalités et les moyens du traitement » et ne reçoit pas d'instructions, nonobstant le fait que c'est un médecin qui prescrit l'analyse et « envoie » son patient réaliser lesdites analyses ;

- En second lieu, l'autorité de contrôle a considéré que l'utilisation d'une page web non chiffrée (protocole http) sur laquelle apparaissaient les résultats d'analyse, viole le principe d'intégrité et de confidentialité inscrit aux articles 5.1.f et 32 du RGPD ;

Autorité de protection des données
Gegevensbeschermingsautoriteit

- Enfin, l'autorité de contrôle a estimé que le fait de placer des « mentions RGPD » directement dans les centres de prélèvement n'est pas suffisant au titre de l'information des personnes concernées dès lors que le laboratoire d'analyses médicales est amené à procéder à des analyses de patients qui ne se sont pas déplacés dans les locaux. Ainsi, elle considère qu'il appartient au laboratoire de publier une politique de confidentialité sur son site, sauf à violer les articles 12 à 14 du RGPD.

Compte tenu de ce qui précède, l'autorité de contrôle a prononcé une amende de 20.000 € à l'encontre du laboratoire d'analyse médicales pour avoir violé les articles 5.1.f ; 12 ; 13 ; 14 ; 32 et 35 du RGPD.

Source : ici

Le principe d'exactitude permet de réexaminer une sanction disciplinaire

L'Ordre des pharmaciens belge a été sanctionné sur le fondement du principe d'exactitude pour n'avoir pas réexaminé une sanction disciplinaire

Le 22 décembre 2016, l'Ordre des pharmaciens belge a infligé à une pharmacienne une sanction disciplinaire pour avoir effectué des « pratiques commerciales » interdites en vertu du Code de déontologie des pharmaciens.

Considérant cette sanction infondée, la pharmacienne a introduit le 1er septembre 2017 une plainte auprès de l'autorité belge de la concurrence. A l'issue des débats, l'autorité de la concurrence a considéré que l'Ordre des pharmaciens avait procédé à une « interprétation restrictive » du Code de déontologie des pharmaciens et a enjoint l'Ordre des pharmaciens de réformer son Code de déontologie sur cette question des pratiques commerciales.

Par la suite, la pharmacienne a mis en demeure l'Ordre des pharmaciens de procéder à l'effacement de son « casier judiciaire » et plus largement de toute information en lien avec la sanction du 22 décembre 2016.

L'Ordre des pharmaciens n'a pas donné suite à cette mise en demeure, considérant (i) que la sanction disciplinaire n'avait pas été invalidée par l'autorité de la concurrence et (ii) que le traitement était conforme au RGPD. Face à ce refus, la pharmacienne a déposé une plainte auprès de l'autorité belge de contrôle.

Autorité de protection des données
Gegevensbeschermingsautoriteit

de ce principe est de lutter contre les données obsolètes dont l'usage qui en est fait peut être non pertinent, voire préjudiciable pour la personne concernée », l'autorité de contrôle a estimé que l'Ordre aurait dû mettre à jour le dossier disciplinaire « pour vérifier si les données conservées reflétaient toujours un statut disciplinaire exact » et donc vérifier « si les sanctions prononcées à l'encontre [de la pharmacienne] sur la base de l'ancienne édition du Code de déontologie seraient à nouveau prononcées en vertu [du] nouveau Code », ce qui n'a pas été fait.

En conclusion, l'autorité de contrôle belge a considéré que l'Ordre des pharmaciens n'avait « pas mobilisé suffisamment de moyens pour respecter le principe d'exactitude » et qu'en n'ayant « pas procédé au réexamen du dossier disciplinaire de la [pharmacienne] après l'adoption du nouveau Code de déontologie, malgré les préjudices soulevés par la plaignante et les indices sérieux du manque de bien fondé du maintien d'une telle sanction » l'Ordre des pharmaciens a violé l'article 5§1.d du RGPD justifiant le prononcé d'une amende de 30 000 € à son encontre.

Source : ici

SIM swapping : Orange sanctionnée pour défaut de base légale

AEPD (Espagne), 24 mars 2023

L'opérateur téléphonique Orange a été sanctionné pour avoir traité les données personnelles d'un client sans base légale, ce qui a engendré une usurpation d'identité de ce dernier.

Le SIM swapping est une technique de piratage par laquelle un pirate obtient d'un opérateur un duplicata d'une carte SIM. Le pirate est ainsi en mesure de détourner les appels et SMS et peut s'approprier les codes d'identification envoyés par les tiers, telles que les banques.

Le 17 janvier 2022, un pirate a déjoué les mesures de sécurité d'Orange et est parvenu à obtenir ledit duplicata d'un client. Ce faisant, il s'est identifié sur l'application bancaire du client et a effectué des virements frauduleux.

Constatant cette usurpation, le client a déposé une plainte pénale et a sollicité la copie de la demande de duplicata. Face au refus d'Orange de transmettre ladite copie, le client a déposé une plainte auprès de l'autorité de contrôle espagnole.

Au cours de son enquête, l'autorité de contrôle, après avoir rappelé qu'Orange est responsable du traitement et que la délivrance d'une carte SIM implique un traitement de données à caractère personnel, a rappelé les obligations qui pèsent sur les opérateurs téléphoniques.

Elle a considéré que « la diligence des opérateurs est essentielle pour éviter ce type d'escroqueries » et que ces « diligences se traduisent par la mise en place de mesures adéquates pour garantir que le traitement de données est conforme au RGPD ».

Or, en l'espèce, le simple fait d'avoir fourni une carte SIM à un tiers « prouve un manquement à l'obligation de protéger les informations des clients ».

Etonnamment, l'autorité de contrôle n'a pas considéré qu'Orange avait violé les articles 5§1.f et 32 du RGPD relatifs à la sécurité, mais qu'Orange a violé l'article 6§1 du RGPD, relatif à un défaut de base légale.

Pour expliquer un tel fondement, l'autorité a considéré qu'Orange « a fourni un duplicata de SIM du plaignant à un tiers sans son consentement et sans vérifier l'identité du tiers » et donc que le traitement a été effectué en dehors de toute base légale.

Compte tenu de ce qui précède, l'autorité de contrôle espagnole a infligé à Orange une amende de 70 000 €.

Source : ici

Messagerie électronique : lors du départ d'un salarié, l'employeur doit désactiver le compte

GPDP (Italie) 21 juillet 2022

L'autorité de contrôle italienne a sanctionné un employeur qui n'avait pas supprimé le compte de messagerie d'un ancien salarié.

Après son départ de l'entreprise, un salarié s'est rendu compte que son ancien employeur avait maintenu son adresse et le compte de messagerie professionnel actifs en redirigeant les communications entrantes vers des adresses électroniques attribuées à d'autres employés de la société.

L'autorité de contrôle italienne, saisie d'une plainte du salarié, a considéré, à l'issue de son enquête, que le fait de maintenir actif l'adresse de messagerie après le départ du salarié est contraire :

- Au principe de licéité, de loyauté et de transparence du traitement car cela permet à l'employeur « de reconstituer l'activité de son employé et d'effectuer un contrôle sur lui qui va au-delà des finalités pour lesquelles les données ont été traitées » ;

- Aux principes de minimisation et de limitation du stockage dès lors que :

  - le traitement des données à des fins de « continuité de l'activité de la société » supposait de « préparer le système de gestion de documents » afin d'identifier ceux qui doivent être archivés, ce que, par nature, les systèmes de courrier électronique ne permettent pas de faire ;

  - la société a activé le système de redirection automatique pendant une période considérable (près de 6 mois) sans indiquer les besoins concrets sous-jacents à cette décision ;

- A l'obligation de faire reposer un traitement sur une base légale, puisque, selon l'autorité : « après la fin de la relation de travail, [l'employeur] doit désactiver et supprimer le compte et adopter simultanément des systèmes automatiques visant à informer les tiers et à leur fournir des adresses alternatives ».

Compte tenu de tous ces manquements, l'autorité de contrôle a infligé à l'employeur une amende de 10 000 euros.

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