Newsletter

DATA

SOMMAIRE

Protection insuffisante des données de santé en accès libre sur Internet : deux médecins libéraux sanctionnés 1

Prospection commerciale et consentement des personnes concernées 2

Brexit et transfert de données : période transitoire et fin du « guichet unique » européen.... 3

Sanction de l'Autorité espagnole pour l'envoi de données personnelles à un tiers en l'absence d'autorisation de la personne concernée..... 4

Un candidat a le droit d'accéder aux évaluations de sa performance dans le cadre d'un processus de sélection 5

Protection insuffisante des données de santé en accès libre sur Internet : deux médecins libéraux sanctionnés

RGPD/CNIL/Médecins/Données de santé/Sanction

SYNTHÈSE - Par deux décisions du 7 décembre 2020 la CNIL a sanctionné deux médecins libéraux pour avoir insuffisamment protégé les données de santé de leurs patients et pour défaut de notification d'une violation de données.

FAITS - À la suite du signalement émanant d'une société de sécurité informatique, la CNIL a constaté que des milliers d'images médicales et données à caractère personnel de patients hébergées sur les serveurs de deux médecins libéraux étaient en accès libre sur Internet.

En raison d'un mauvais choix de configuration de leur box Internet et du logiciel d'imagerie médicale, il était possible de consulter et de télécharger librement les images médicales accompagnées de données à caractère personnel appartenant aux patients. Lors de son contrôle la CNIL a par ailleurs pu constater que les images médicales n'étaient pas systématiquement chiffrées.

Dans ce contexte, la CNIL sanctionne les deux médecins pour plusieurs motifs :

- D'une part, la CNIL a estimé que les deux médecins avaient manqué à leur obligation de sécurité des données en tant que responsables de traitement en ne mettant pas en œuvre les mesures techniques de sécurité appropriées – les données ont été exposées environ 5 ans ;
- D'autre part, elle a également considéré que les deux médecins avaient manqué à leur obligation de notifier les violations de données suite à leur connaissance de l'accès libre aux données à caractère personnel de leurs patients sur Internet.

La CNIL considère que les deux médecins ont ainsi manqué à des exigences élémentaires en matière de sécurité informatique, à savoir le chiffrement des données ainsi que la protection des réseaux informatiques. Compte tenu du caractère particulier des données de santé au titre de l'article 9 du RGPD, les deux médecins auraient dû être particulièrement vigilants. La CNIL considère à ce propos que les professionnels de la santé doivent être d'une vigilance particulière et être conduits à choisir des solutions présentant le maximum de garanties en matière de sécurité informatique et protection des données. Selon la CNIL, cette vigilance particulière doit inciter ces professionnels à être prudents lors du paramétrage de leur système informatique et si nécessaire à s'entourer de prestataires compétents, contrairement aux deux médecins qui avaient procédé seuls à ce paramétrage.

Par ailleurs, la CNIL précise que la circonstance selon laquelle la violation de données est portée à la connaissance du responsable de traitement par les services de contrôle de la CNIL ne le décharge pas de son obligation de notification.

SANCTION - Les amendes infligées aux médecins pour violation des articles 32 et 33 du RGPD s'élèvent à 6 000€ pour l'un et 3 000€ pour l'autre. Si la CNIL n'a pas considéré nécessaire de révéler l'identité des médecins, elle a néanmoins souhaité assurer la publicité de la délibération afin d'alerter les professionnels de santé sur la nécessité de vigilance s'agissant des mesures de sécurité adoptées dans leur traitement des données personnelles.

DÉCISION – Cliquez ici et ici pour en savoir plus

(*Délibération n°SAN-2020-015 du 7 décembre 2020 concernant Monsieur [...]* et *Délibération de la formation restreinte n° SAN-2020-014 du 7 décembre 2020 concernant Monsieur [...]*)

Prospection commerciale et consentement des personnes concernées

RGPD / CNIL/Prospection commerciale/Consentement/Sanction

SYNTHÈSE - Par une décision du 7 décembre 2020, la CNIL a prononcé des sanctions à l'encontre de Performeclic pour avoir notamment adressé des courriers électroniques de prospection commerciale sans preuve du consentement préalable des personnes et sans information satisfaisante.

FAITS - La société Performeclic (TPE d'1 à 2 salariés), ayant pour activité l'envoi de prospection commerciale par courrier électronique pour le compte d'annonceurs, a fait l'objet d'un signalement auprès de la CNIL par une association recueillant les signalements des internautes relatifs à la réception de courriers électroniques non sollicités. Ce signalement indiquait que Performeclic apparaissait régulièrement en tête du classement des sociétés émettant le plus de messages signalés comme spams par les internautes français.

Suite à des contrôles, la CNIL sanctionne alors la société Performeclic en se fondant sur les manquements suivants :

- Un manquement à l'obligation de recueillir le consentement des personnes concernées par l'envoi de courriers électroniques de prospection commerciale directe en vertu de l'article L.34-5 du Code des postes et des communications électroniques. En effet, il ressort des

contrôles de la CNIL que la société Performeclic ne dispose d'aucun élément permettant de matérialiser ni le recueil ni l'existence du consentement valable des personnes concernées par les courriers électroniques de prospection. Or, l'envoi de courriers électroniques de prospection commerciale constitue le cœur de l'activité de la société, qui s'engage envers ses cocontractants à disposer d'une base d'adresses de personnes ayant consenti à recevoir de tels courriers ;

- Un manquement au principe de minimisation des données en vertu de l'article 5.1.c du RGPD notamment par la conservation des numéros de téléphone des personnes concernées, données non nécessaires à l'activité de la société (la prospection est réalisée uniquement par courriers électroniques) ;
- Un manquement en matière de durée de conservation des données à caractère personnel par la conservation des données d'environ 5 millions de prospects pendant plus de 3 ans après la simple ouverture d'un courrier électronique sans autre action de la part des personnes concernées. La CNIL considère que la société n'aurait pas dû prendre en compte la simple ouverture d'un courrier comme dernier contact émanant du prospect. La CNIL recommande de prendre en compte une action manifestant un intérêt de la personne concernée comme un clic sur un lien hypertexte ;
- Un manquement à l'obligation d'information des personnes concernées notamment en ne fournissant pas une information conforme à l'article 14 du RGPD aux personnes dont les données ont été collectées de manière – notamment en ne fournissant pas d'information sur l'identité du responsable de traitement, sa base légale, les catégories de données concernées, les droits des personnes concernées. Par ailleurs, aucune modalité d'information complémentaire n'est mise en place ;
- Un manquement au droit d'opposition des personnes au titre de l'article 21 du RGPD. En effet, la société Performeclic ne permettait pas aux personnes concernées de s'opposer de manière simple et effective à l'utilisation de leurs données – nécessité de se désabonner de chaque compte sans être informé de l'existence de canaux permettant de se désinscrire de l'ensemble des comptes ;
- Enfin, un manquement à l'obligation d'encadrement contractuel du sous-traitant au titre de l'article 28 du RGPD par l'absence de certaines clauses obligatoires dans le contrat conclu entre la société Performeclic et son prestataire d'hébergement.

SANCTION - Sur la base de ces manquements, la CNIL a prononcé une amende de 7 300€ à l'encontre de Performeclic ainsi qu'une injonction de se mettre en conformité dans un délai de 2 mois sous astreinte de 1 000€ par jour de retard.

DÉCISION – Cliquez ici pour en savoir plus

(*Délibération de la formation restreinte n° SAN-2020-016 du 7 décembre 2020 concernant la société PERFORMECLIC*)

Brexit et transfert de données : période transitoire et fin du « guichet unique » européen

BREXIT / RGPD / Transfert de données / Guichet unique

SYNTHÈSE - Dans le cadre de l'accord de commerce et de coopération conclu entre le Royaume-Uni et l'Union européenne le 24 décembre 2020, il a été convenu que le RGPD demeurerait applicable au Royaume-Uni jusqu'au mois de juillet 2021. Néanmoins, le mécanisme du « guichet unique européen » n'est plus applicable depuis le 1er janvier 2021.

EN PRATIQUE - L'accord conclu entre le Royaume-Uni et l'Union européenne le 24 décembre dernier prévoit que le RGPD restera applicable de manière transitoire au Royaume-

Uni jusqu'au 1er juillet 2021. Ainsi, jusqu'à cette date, les transferts de données avec le Royaume-Uni ne seront pas considérés comme des transferts de données vers un pays tiers.

Aucune formalité n'est donc nécessaire aujourd'hui. En revanche, à l'issue de la période transitoire de 6 mois, plusieurs hypothèses de transferts sont à envisager.

- S'agissant des transferts de l'Union européenne vers le Royaume Uni, en l'absence d'une décision d'adéquation de la Commission européenne, autorisant de façon générale les transferts de données vers le Royaume-Uni, ces transferts seront considérés comme effectués vers un pays tiers au sens du RGPD. Ils ne pourront alors être effectués qu'avec la mise en place de garanties appropriées telles que des clauses contractuelles types, des BCR etc.
- S'agissant des transferts de données du Royaume-Uni vers l'Union européenne, il existe pour l'instant une décision d'adéquation britannique visant l'Espace économique européen. De tels transferts peuvent donc être réalisés sans autre formalité pour l'instant.
- Dans l'hypothèse où le Royaume-Uni déciderait de révoquer sa décision d'adéquation concernant l'Union européenne, les transferts de données seront considérés comme des transferts vers un pays tiers. Il faudra alors mettre en place les garanties appropriées prévues par le UK Data Protection Act (BCR - dans leur version proposée par l'Union européenne adaptée au Royaume-Uni ou en utilisant les BCR éditées par l'ICO -, clauses contractuelles types).

De manière immédiate, la fin de la période transitoire prévue par l'accord de retrait a marqué la fin de l'application du mécanisme de « guichet unique » au Royaume-Uni dès le 1er janvier 2021. En vertu de ce mécanisme, les décisions concernant les traitements transfrontaliers sont facilitées pour les entreprises établies dans l'Union européennes : il s'agit d'un one-stop-shop permettant aux responsables de traitement établis dans l'Union européenne de n'avoir qu'un seul interlocuteur, l'autorité de protection des données du pays où se trouve l'établissement principal de l'entreprise, et une seule autorité auprès de laquelle accomplir leurs obligations en vertu du RGPD.

Ainsi, depuis le 1er janvier 2021 :

- Les responsables de traitement et les sous-traitants établis uniquement aux Royaume-Uni mais dont les activités de traitements sont soumises à l'application du RGPD doivent désigner un représentant au sein de l'Union européenne. En revanche, si le responsable de traitement ou le sous-traitant possède un établissement principal dans l'Espace économique européen, alors ces derniers peuvent continuer à bénéficier du mécanisme du guichet unique.
- De manière réciproque, les responsables de traitement et les sous-traitants sont les activités de traitement sont soumises à l'application du UK Data Protection Act sont tenus de désigner un représentant au Royaume-Uni.

Dans ce contexte il sera désormais possible d'avoir des investigations menées et des amendes prononcées par plus d'une autorité de protection des données.

INFORMATIONS – Cliquez ici pour en savoir plus. Voir également ICO Guidance

Sanction de l'Autorité espagnole pour l'envoi de données personnelles à un tiers en l'absence d'autorisation de la personne concernée

RGPD / Espagne / Confidentialité / Tiers / Autorisation

SYNTHÈSE - Le 27 novembre 2020, l'Autorité espagnole de protection des données a eu l'occasion de sanctionner une société pour l'envoi à un tiers d'un courrier électronique

contenant des données à caractère personnel sans l'autorisation de la personne concernée.

FAITS - Un ancien employé a saisi l'Autorité espagnole de protection des données suite à l'envoi par son ancien employeur d'un courrier électronique contenant des données à caractère personnel le concernant à un tiers sans son autorisation. L'envoi de ce courrier électronique et son contenu ont été porté à la connaissance de l'ancien employé au cours d'une audience devant les juridictions espagnoles à la suite d'une accusation de vol portée par son ancien employeur à son encontre.

L'ancien employeur a en effet envoyé un courrier électronique à une société de transport, contenant notamment des documents relatifs au licenciement dudit employé, de son indemnité de départ ainsi que d'une accusation de tentative de fraude le concernant. Ce courrier électronique comportant des données à caractère personnel, la société de transport a immédiatement notifié l'ancien employeur de son erreur en l'informant qu'elle n'aurait pas dû recevoir de telles informations.

L'Autorité espagnole a considéré que l'ancien employeur avait en effet violé le principe de confidentialité de l'article 5.1.f du RGPD par l'envoi d'un courrier électronique contenant des données à caractère personnel de son ancien employé à un tiers sans son consentement.

SANCTION - Une amende administrative de 10 000 euros a alors été imposée à l'ancien employeur.

DÉCISION – Cliquez ici pour en savoir plus

(AEPD, *Procedimiento Procedimiento nº PS/00324/2020, 27 novembre 2020*)

Un candidat a le droit d'accéder aux évaluations de sa performance dans le cadre d'un processus de sélection

RGPD / EDPB / Candidat / Institution UE / Droit d'accès

SYNTHÈSE - Le Comité européen de la protection des données personnelles a eu l'occasion de se prononcer en matière de droit d'accès d'un candidat lors d'une procédure de sélection.

FAITS - Un candidat exclu lors d'une procédure de sélection par une institution de l'Union européenne s'est vu refuser l'accès à aux évaluations de sa performance du Comité de sélection lors de sa participation à la première phase de sélection ainsi qu'aux fichiers logs et pistes d'audit concernant sa candidature.

L'institution a en effet considéré d'abord que la disqualification du candidat, due à un conflit d'intérêt, avait pour conséquence d'empêcher l'accès des candidats à de tels éléments d'évaluation ces derniers n'ayant pu être finalisés. Une telle communication aurait pour conséquence de porter atteinte à la confidentialité du processus du Comité de sélection.

Dans sa décision, le Comité européen de protection des données personnelles a considéré que l'évaluation de la performance d'un candidat, par des observations et suggestions de score sont des données à caractère personnel. Dès lors, il est nécessaire de donner un droit d'accès à ces données aux personnes concernées sans pour autant que ces documents identifient de façon directe ou indirecte un membre du Comité de sélection. Néanmoins, le Comité européen affirme que la nécessité de protection de l'anonymat du Comité de sélection ne peut être invoquée au détriment du droit fondamental des individus d'accéder à leurs données personnelles. Par ailleurs, le Comité européen souligne que l'élimination du candidat du processus de sélection ne constituait pas un fondement valable de refus d'accès.

SANCTION - Le Comité européen propose alors qu'une évaluation globale résumant les différents scores du candidat ainsi que les fichiers logs et pistes d'audit lui soit communiqués en prenant soin de ne pas révéler l'identité des membres du Comité de sélection ayant eu accès à ces données.

DÉCISION – Cliquez ici pour en savoir plus

(EDPB, *22 septembre* 2020)