Newsletter

DATA

Opinion du Comité européen de la protection des données sur la création de l'Espace européen des données de santé

EDPB / Espace européen des données de santé / Opinion

SYNTHÈSE - Le 17 novembre 2020, le Comité européen de la protection des données a publié une opinion préliminaire concernant la création de l'Espace européen des données de santé (ci-après « Espace européen ») présentée par la Commission dans sa communication sur la « Stratégie européenne pour les données » de février 2020. Cette opinion a pour objectif de mettre en lumière les éléments essentiels en matière de protection des données qui doivent être pris en compte dans le cadre de la création de cet espace.

FAITS - La création de l'Espace européen est envisagée par la Commission comme un outil essentiel de prévention, détection et de traitement des maladies mais également comme un outil permettant la prise de décisions informées, d'amélioration de l'efficacité, l'accessibilité et la pérennité des systèmes de santé.

À ce titre, le Comité européen de la protection des données s'est prononcé en faveur de la création d'un tel outil mais a souhaité souligner la nécessité de prévoir, dès la création de cet espace, des garanties de protection des données personnelles.

SOMMAIRE

Le Comité a alors précisé les éléments essentiels à considérer dans le cadre du développement de l'Espace européen des données de santé en ce qui concerne la protection des données.

D'abord, le Comité a appelé la Commission à prévoir une base légale de traitement dûment réfléchie dans le cadre de ce traitement. En effet, le Comité a rappelé que le traitement des données personnelles ne peut être légal que s'il repose sur une ou plus des six bases légales de traitement prévues par l'article 6 du RGPD. À ce titre, le Comité a précisé qu'il ne considérait pas le consentement comme une base légale appropriée. En revanche, au regard de l'objectif de l'Espace européen, le Comité a précisé que l'exécution d'une mission de d'intérêt public (article 6.1.e), pouvait constituer une base légale pertinente. Par ailleurs, les données traitées relevant de la catégorie des données particulières au sens du RGPD, le Comité a rappelé que leur traitement devait être en conformité avec les exigences prévues à l'article 9 du RGPD. Le Comité a rappelé que les motifs d'intérêt public dans le domaine de la santé (article 9.2.i RGPD) de même que la finalité de recherche scientifique (article 9.2.j RGPD) pouvaient constituer des bases légales de traitement pertinentes.

Par ailleurs, au regard de la sensibilité des données collectées et traitées, le Comité considère que la définition de ce que constitue un traitement licite de même qu'un traitement ultérieur autorisé doit être très claire pour toutes les parties prenantes. Il est alors primordial que ces informations soient accessibles au public de façon transparente.

Le Comité appelle également la Commission à clarifier le rôle et la responsabilité des parties impliquées dans cet espace afin notamment d'identifier les responsables de traitement auprès desquels les personnes concernées peuvent exercer leurs droits dans chaque État membre. Il est également demandé de préciser les catégories de données transmises à l'Espace européen.

S'agissant de la sécurité des données, le Comité appelle la Commission à prévoir des garanties ainsi que des mesures techniques et organisationnelles au sein de l'Espace européen. Par exemple, dans le cadre de la minimisation des données, l'utilisation de technologies de chiffrement peut être envisagée. La conduite d'une analyse d'impact peut également se révéler utile afin d'identifier les risques existants et les mesures de sécurité appropriées devant être adoptées.

Par ailleurs, le Comité met en garde sur l'utilisation éthique des données. À ce titre, l'avis de comités éthique nationaux doit être pris en compte.

S'agissant de la gouvernance des données, le Comité affirme que le succès de l'Espace européen des données de santé repose sur un mécanisme de gouvernance des données présentant l'assurance d'une gestion légale, responsable et éthique des données. Ce mécanisme devrait notamment prévoir les entités autorisées à transmettre les données à l'Espace européen, les utilisateurs de l'Espace européen, les points de contrôle au sein des États membres. Le Comité considère que les autorités nationales de protection des données doivent être impliquées dans le contrôle et la conformité des traitements dans le cadre de l'Espace européen.

Enfin, le Comité appelle les États membres à garantir l'effectivité du droit à la portabilité des données ainsi que d'assurer la mise en place d'autres mesures techniques nécessaires à l'exercice des droits des personnes concernées dans le cadre de l'Espace européen.

DÉCISION – Cliquez ici pour en savoir plus

(*EDPB, Preliminary opinion 8/2020 on the European Health Data Space du 17 novembre 2020*)

Une amende de 20.000 euros prononcée par la CNIL à l'encontre de la société Nestor en raison de ses activités de prospection commerciale

CNIL / Prospection commerciale / Sanction

SYNTHÈSE - Le 8 décembre 2020 la CNIL a prononcé une amende de 20.000 euros à l'encontre de la société Nestor en raison de plusieurs manquements constatés dans le cadre de ses opérations de prospection commerciale en ligne, notamment l'obligation de recueillir le consentement et différents manquement relatifs aux droits de personnes concernées.

FAITS - Nestor est une société qui a pour activité la préparation et la livraison de repas à destination d'employés de bureaux, commandés à partir de son site internet/application. Entre fin 2018 et début 2019, la CNIL a été saisie de plaintes de personnes non-clientes de la société indiquant avoir reçu des emails de prospection commerciale de la part de Nestor sans qu'elles aient préalablement fourni leur consentement.

La CNIL a constaté quatre manquements à la règlementation applicable en matière de protection des données personnelles :

- Un manquement à l'obligation de recueillir le consentent des personnes concernées par une opération de prospection commerciale en ligne au titre de l'article L. 34-5 du CPCE.
  En effet, l'enquête de la CNIL a révélé que depuis 2017, environ 654.000 prospects avaient reçu des emails de prospection commerciale de la part de Nestor sans y avoir préalablement consenti. Ces emails de prospection visaient deux catégories de personnes. D'abord, des personnes dont les données personnelles sont recueillies sur internet (à partir du format de l'adresse de l'entreprise et des données diffusées par l'entreprise sur Internet), et d'autre part des personnes ayant créé un compte sur le site ou l'application sans avoir passé commande. Pour ces dernières, aucune disposition n'était prise pour recueillir leur consentement à l'envoi d'emails de prospection.
  Durant la procédure, Nestor a mis en place des mesures afin de mettre ses pratiques en conformité avec l'article L.34-5 du CPCE, notamment un système de recueil du consentement à l'envoi d'emails de prospection au moment de la création du compte.
  Néanmoins, la CNIL a prononcé une injonction contre Nestor afin de justifier de la suppression de l'ensemble des données personnelles collectées sans le consentement.
- Un manquement à l'obligation d'information des personnes en application des articles 12 et 13 du RGPD.
  La CNIL a en effet constaté que l'ensemble des informations exigées par le RGPD ne figuraient pas dans le formulaire de collecte de données permettant de s'inscrire et ce dernier ne renvoyait pas non plus vers une page dédiée contenant ces informations (notamment s'agissant de la base légale des traitements ni de l'intérêt légitime du responsable de traitement). Par ailleurs, la CNIL a relevé que la politique de confidentialité de Nestor était incomplète, trop générale et imprécise s'agissant par exemple des destinataires des données personnelles collectées. Enfin, aucune information relative à la protection des données n'était fournie aux personnes créant un compte sur l'application.
  Au cours de la procédure, Nestor a néanmoins mis en œuvre les mesures nécessaires pour assurer sa conformité au RGPD.
- Un manquement à l'obligation de respecter le droit d'accès au titre de l'article 15 du RGPD. La CNIL a en effet constaté que la société avait manqué à son obligation de fournir une copie des données personnelles ainsi qu'une information relative à la source des données à la suite de demandes de deux personnes. Ces réponses partielles constituent des manquements.

La CNIL a enjoint Nestor à satisfaire pleinement aux demandes d'exercice du droit d'accès des personnes concernées.

- Enfin, la CNIL a constaté un manquement à l'obligation de sécurité des données imposé par l'article 32 du RGPD. Nestor n'imposait pas l'utilisation d'un mot de passe robuste lors de la création d'un compte. La société a depuis pris des mesures.

SANCTION - La CNIL a prononcé une sanction de 20.000 euros mais également une injonction sous astreinte de 500 euros par jour de retard imposant à Nestor de mettre ses traitements en conformité avec le CPCE et le RGPD sous un délai de 3 mois à compter de la notification de la délibération.

DÉCISION – Cliquez ici pour en savoir plus

(*Délibération SAN-2020-018 du 8 décembre 2020*)

Une amende de 12,5 millions d'euros prononcée par l'Autorité italienne à l'encontre de Vodafone en raison de ses pratiques agressives de télémarketing

RGPD / Italie / Télémarketing / Sanction

SYNTHÈSE - L'Autorité italienne de protection des données personnelles a eu l'occasion de prononcer une amende 12,5 millions d'euros à l'encontre de Vodafone à la suite à de pratiques agressives de télémarketing conduisant au traitement illicite de données de millions d'utilisateurs.

EN PRATIQUE - Suivant la réception de centaines de plaintes et d'alertes d'utilisateurs de Vodafone reprochant à l'opérateur de nombreux appels non sollicités, l'Autorité italienne de protection des données a mené une enquête sur ses pratiques.

Aux termes de cette enquête, l'Autorité italienne a relevé des nombreuses violations de principes clés du RGPD, notamment de l'obligation de recueillir le consentement, du principe de responsabilité ainsi que du principe de *privacy by design*.

Particulièrement, l'autorité italienne a relevé que Vodafone utilisait de faux numéros de téléphones ou des numéros non enregistrés afin d'effectuer des appels marketings depuis des centres d'appel non autorisés. Au surplus, ces appels étaient réalisés en violation de la règlementation applicable en matière de protection des données personnelles.

En outre, il a été constaté que les listes de contacts de Vodafone acquises auprès de tiers étaient transférées à Vodafone par ses partenaires commerciaux au mépris des droits des personnes concernées. En effet, le consentement spécifique, libre et éclairé de ces personnes au transfert de leurs données personnelles à Vodafone n'avait pas été préalablement recueilli.

Enfin, la gestion des mesures de sécurité a été considérée inadéquate en raison de plusieurs plaintes faisant état d'opérateurs se faisant passer pour Vodafone et demandant la fourniture de données personnelles auprès des utilisateurs dans le cadre de pratiques malveillantes.

SANCTION - Les pratiques de Vodafone ont conduit l'Autorité italienne de protection des données à prononcer une amende d'un montant de 12,5 millions d'euros ainsi qu'une injonction de cesser les traitements à des fins promotionnelles ou commerciales effectuées après acquisition de listes de données personnelles auprès de tiers, sans que le tiers en question ait obtenu le consentement libre, spécifique et éclairé des personnes concernées.

DÉCISION – Cliquez ici pour en savoir plus

(*Décision de l'Autorité italienne de protection des données du 16 novembre 2020*)

Sanction d'un responsable de traitement et de son sous-traitant pour l'absence de mesures correctives face aux attaques de *credential stuffing*

CNIL / *Credential stuffing* / Cybersécurité / Sous-traitant / Sanction

SYNTHÈSE - Fin janvier 2021 la CNIL a sanctionné d'une part un responsable de traitement et d'autre part son sous-traitant pour ne pas avoir pris assez rapidement des mesures de sécurité adéquates pour faire face à des attaques de *credential stuffing* sur le site Internet du responsable de traitement.

FAITS - A la suite de plusieurs notifications de violations de données personnelles relatives à un site Internet, sur lequel il est notamment possible de faire des achats, la CNIL a décidé de mener une enquête auprès du responsable de traitement et son sous-traitant, en charge de la gestion du site.

La CNIL a alors constaté le site Internet avait fait l'objet de plusieurs vagues d'attaques de type *credential stuffing*.

Le *credential stuffing* est une attaque dans laquelle un attaquant récupère une série d'identifiants et mots de passe librement accessibles sur Internet, en général à la suite d'une fuite de données personnelles. Puis, considérant que la vaste majorité des utilisateurs se servent des mêmes identifiants et mots de passe pour différents services, l'attaquant va utiliser des robots pour tenter massivement de se connecter sur différents sites et, en cas de succès d'authentification, accéder aux informations associées aux comptes.

Lors des attaques répétées sur le site Internet en question, la CNIL a constaté que les attaquants avaient pu avoir accès aux noms, prénoms, adresses email notamment mais surtout aux numéros et soldes des cartes de fidélité des clients ainsi que des informations liées à leurs achats.

La CNIL a considéré que le responsable de traitement et le sous-traitant avaient manqué à leur obligation d'assurer la sécurité des données personnelles traitées en vertu de l'article 32 du RGPD.

Les deux sociétés ont en effet tardé à mettre en place des mesures de sécurité adéquates. En effet, si les sociétés avaient entrepris de développer un outil permettant de bloquer les attaques, le développement de cet outil a pris un an. Or, dans cet intervalle, aucune autre mesure n'a été adoptée malgré la persistance des attaques. La CNIL a alors considéré que des mesures, notamment techniques, auraient pu être adoptées afin d'assurer la sécurité des données comme :

- La limitation du nombre de requêtes autorisées par adresse IP ;
- L'utilisation d'un CAPTCHA dès la première tentative d'authentification des utilisateurs à leur compte (particulièrement efficace contre les robots).

Par ailleurs, la CNIL avait précédemment émis une recommandation à destination des professionnels conseillant de mettre en place des mesures de connexion multi-facteurs (envoi de SMS par exemple) et l'utilisation d'un couple identifiant/mot de passe ne correspondant pas à l'adresse email de l'utilisateur.

En raison du manque de diligence des deux sociétés, les données de 400 millions de clients ont été rendues accessibles à des tiers non autorisés entre 2018 et 2019.

Par ailleurs, il est assez rare qu'un sous-traitant soit condamné sur le fondement de l'article 32 du RGPD. La CNIL a cependant précisé que si le responsable de traitement doit décider de la mise en place de mesures et donner des instructions documentées à son sous-traitant, ce dernier doit aussi chercher des solutions techniques et organisationnelles appropriées et les proposer au responsable de traitement.

SANCTION - La CNIL a prononcé une sanction de 150.000 euros à l'égard du responsable de traitement et de 75.000 euros à l'égard du

sous-traitant. Si la décision n'a pas été rendue publique, la CNIL souhaite néanmoins attirer l'attention des professionnels sur ce type d'attaques qui est en outre le thème de la dernière « violation du trimestre », rendez-vous de la CNIL dédiés aux incidents de sécurité.

DÉCISION – Cliquez ici et ici pour en savoir plus

La ville de Rome et son sous-traitant sanctionné par l'Autorité italienne de protection des données pour le traitement illicite de données personnelles via un système de réservation

RGPD / Italie / Secteur Public / Sous-Traitant / Sanction

SYNTHÈSE - Le 17 décembre 2020, l'Autorité italienne de protection des données a eu l'occasion de sanctionner par deux décisions différentes, la Ville de Rome ainsi que son sous-traitant pour violation de l'obligation d'information et de la sécurité du traitement, mais également pour absence de conclusion d'un contrat de sous-traitance.

FAITS - Tupassi est un service de réservation et de prise de rendez-vous proposé par la société Miropass. Ce service est utilisé par la Ville de Rome, permettant aux utilisateurs de prendre des rendez-vous dans le cadre de différents services et notamment de services de santé.

Au terme d'une procédure d'investigation complexe qui a duré près de 3 ans, l'Autorité italienne de protection des données a sanctionné la Ville de Rome en raison des opérations illicites de traitement des données des utilisateurs et de ses employés via le service Tupassi.

En effet, l'Autorité a considéré que le service rendait possible la collecte et la conservation de données personnelles, et notamment de données sensibles liées à la santé des utilisateurs, mais également des employés (nom, date, type de service etc.). Or, ces opérations de traitement n'étaient pas réalisées de manière licite, loyale et transparente (article 5 (1) (a) du RGPD) en raison de l'absence d'information complète fournie aux employés et utilisateurs sur les activités de traitement réalisées.

Par ailleurs, l'Autorité a également considéré que les mesures de sécurité techniques et organisationnelles mises en place par la Ville de Rome étaient inadéquates.

Enfin, l'Autorité a considéré que la Ville de Rome avait manqué à son obligation en vertu de l'article 28 du RGPD faute d'avoir encadré par un contrat sa relation avec son sous-traitant Miropass.

Il est important de relever que l'Autorité italienne a également sanctionné Miropass pour violation de l'article 28 du RGPD. En effet, l'Autorité a considéré qu'en l'absence d'un contrat de sous-traitance, les opérations de traitement de données conduites par Miropass pour le compte de ses clients étaient réalisées en dehors d'une base légale appropriée. A ce titre, Miropass a été sanctionné pour violation de l'obligation de traitement des données de manière licite, loyale et transparente (article 5(1)(a)), illicéité du traitement (article 6) et illicéité du traitement de données sensibles (article 9). La sanction à l'encontre de Miropass a été prononcée dans une décision indépendante, dans laquelle Miropass a été sanctionnée à la fois pour ses activités en tant que responsable de traitement et en tant que sous-traitant.

SANCTION - L'Autorité italienne a donc prononcé une amende de 500.000 euros à l'encontre de la Ville de Rome et de 40.000 euros à l'encontre de Miropass.

Cette décision souligne l'importance à la fois pour les responsables de traitement et pour les sous-traitants d'encadrer leurs relations par un contrat. En effet, le risque de sanction en l'absence d'un tel encadrement ne pèse pas seulement sur le responsable de traitement mais également sur le sous-traitant.

DÉCISION – Cliquez ici et ici pour en savoir plus

(*Décision de l'Autorité italienne de protection des données du 17 décembre 2020 – Ville de Rome ; décision de l'Autorité italienne de protection des données du 17 décembre 2020 – Miropass*)