DATACTU JURIDIQUE

NOVEMBRE 2022

HOUDART
& ASSOCIÉS
AVOCATS

SOMMAIRE

Pages

LES RECO CNIL DU MOIS

LA NOUVELLE RECOMMANDATION DE LA CNIL RELATIVE AUX MOTS DE PASSE 2

Par une délibération du 21 juillet 2022, la CNIL a adopté une recommandation relative aux mots de passe dans l'objectif d'actualiser sa précédente recommandation de 2017 en la matière (...)

ACTU CYBER SÉCURITÉ

L'ADOPTION DÉFINITIVE DES LIGNES DIRECTRICES DU CEPD SUR LA NOTIFICATION DES VIOLATIONS DE DONNÉES PERSONNELLES 3

Le Comité européen à la protection des données (CEPD) a publié la version définitive de ses lignes directrices sur la notification des violations de données personnelles en application du RGPD (...)

POUR ALLER + LOIN

ACTU SANTÉ NUMÉRIQUE

LES PRÉCISIONS DU CONSEIL D'ÉTAT SUR L'INDÉPENDANCE FONCTIONNELLE DU DÉLÉGUÉ À LA PROTECTION DES DONNÉES 4

Dans un arrêt en date du 21 octobre 2022, le Conseil d'Etat a apporté des précisions sur l'indépendance fonctionnelle du délégué à la protection des données. (...)

UNE CONSULTATION PUBLIQUE AU SUJET DE LA NOUVELLE VERSION DE LA DOCTRINE DU NUMÉRIQUE EN SANTÉ 5

Dans un communiqué de presse publié sur son site internet le 12 octobre dernier, l'Agence du Numérique en Santé (ANS) a mis en ligne une consultation publique (...)

PERSPECTIVES & CHANGEMENTS

LES PRÉCISIONS DE LA CNIL SUR LES ÉLECTIONS PROFESSIONNELLES ORGANISÉS PAR LES EMPLOYEURS PUBLICS OU PRIVÉS 6

Par une publication sur son site internet le 24 octobre dernier, la CNIL a apporté quelques précisions sur le déroulement des élections professionnelles organisées par (...)

PERSPECTIVES & CHANGEMENTS

UNE DÉCISION DU TRIBUNAL ADMINISTRATIF DE PARIS ENJOINT LE HEALTH DATA HUB À CHANGER SA DÉNOMINATION 7

Dans une décision du 20 octobre 2022, le tribunal administratif de Paris a fait droit à la demande de l'association Francophonie Avenir tendant à changer la dénomination du « Health Data Hub »,(...)

PERSPECTIVES & CHANGEMENTS

JOE BIDEN SIGNE UN DÉCRET PRÉSIDENTIEL POUR PERMETTRE LES NÉGOCIATIONS SUR UN NOUVEL ACCORD TRANSATLANTIQUE DE TRANSFERT DE DONNÉES 8

Le président américain Joe Biden a récemment signé un décret présidentiel dans l'objectif de reprendre les négociations sur un nouvel accord transatlantique.

DÉCRYPTAGE SANCTION

LA CNIL CONDAMNE LA SOCIÉTÉ CLEARVIEW AI À UNE SANCTION DE 20 MILLIONS D'EUROS 9

La société Clearview AI a été condamnée par la CNIL dans une délibération SAN-2022-019 du 17 octobre 2022 à une sanction de 20 millions d'euros (...)

LA NOUVELLE RECOMMANDATION DE LA CNIL RELATIVE AUX MOTS DE PASSE

Par une délibération du 21 juillet 2022, la CNIL a adopté une recommandation relative aux mots de passe dans l'objectif d'actualiser sa précédente recommandation de 2017 en la matière.
En effet, 81% des violations de données mondiales sont liées à un problème de mot de passe : ce constat alarmant a conduit la CNIL à lancer une consultation publique en octobre 2021 au sujet de cette mise à jour.
La nouvelle recommandation vise ainsi à permettre tant aux professionnels qu'aux particuliers de disposer d'outils pratiques sur lesquels tout responsable de traitement peut s'appuyer dans le cadre des obligations posées par le RGPD.

La CNIL rappelle au préalable que si les acteurs peuvent mettre en place d'autres mesures de sécurité que celles décrites dans cette recommandation, c'est à la condition qu'ils puissent démontrer qu'est garanti un niveau de sécurité au moins équivalent.
Afin de compléter cette nouvelle recommandation, la CNIL renvoie vers le guide de l'ANSSI relatif aux recommandations relatives à l'authentification multifacteur et aux mots de passe.

La CNIL recommande de nouveau dans cette nouvelle version l'utilisation d'un mot de passe complexe et long pour diminuer le risque de réussite d'une attaque informatique par force brute, c'est-à-dire une attaque consistant à tester successivement de nombreux mots de passe. Parmi les nouvelles recommandations, la CNIL introduit ainsi de nouvelles notions pour évaluer la robustesse d'un mot de passe :

- La notion d'entropie qui vise à comparer la robustesse des politiques de mot de passe et qui peut être définie comme la « quantité de hasard », c'est-à-dire son degré d'imprédictibilité théorique et sa capacité de résistance à une attaque par force brute ;
- La notion de « devinabilité » qui consiste à évaluer, au moyen de traitements algorithmiques dédiés, la facilité pour un adversaire de retrouver un mot de passe donné. Les outils pour mettre en œuvre cette nouvelle méthode n'étant toutefois pas encore disponibles, la CNIL entend ainsi rester attentive aux nouveaux développements dans ce domaine.

Par ailleurs, la CNIL recommande notamment :

- L'arrêt du renouvellement périodique des mots de passe. Plusieurs études ont en effet démontré que forcer l'utilisateur à changer son mot de passe régulièrement ne constitue pas une mesure efficace. La CNIL recommande ainsi désormais de ne demander une telle modification qu'aux comptes d'administration ;
- De ne jamais stocker les mots de passe en clair, ces derniers devant être transformés au moyen d'une fonction cryptographique non réversible et sure ;
- Une procédure à suivre pour les responsables de traitement en cas de détection d'une violation de données en rapport avec le mot de passe d'une personne.

Enfin, prenant en compte l'avis de la majorité des répondants à la consultation publique, la CNIL a supprimé l'utilisation d'un mot de passe renforcé par une information complémentaire, recommandation qui était prévue dans la version de 2017 et laisse en conséquent aux responsables de traitement recourant à de tels mots de passe un délai d'adaptation pour faire évoluer leur politique en la matière.

ACTU CYBER SÉCURITÉ

L'ADOPTION DÉFINITIVE DES LIGNES DIRECTRICES DU CEPD SUR LA NOTIFICATION DES VIOLATIONS DE DONNÉES PERSONNELLES

Le Comité européen à la protection des données (CEPD) a publié la version définitive de ses lignes directrices sur la notification des violations de données personnelles en application du RGPD :

Sans modifier l'ensemble de ses précédentes lignes directrices en la matière datant de 2017 qui contiennent une description des étapes de la procédure de notification à l'autorité de contrôle compétente conformément à l'article 33 du RGPD, des exemples de violations ou encore les mesures à prendre pour un responsable de traitement, le CEPD souhaitait cependant clarifier dans cette nouvelle version la procédure de notification lorsque des violations de données surviennent à la suite de flux transfrontières.

En effet, en cas de flux transfrontière, une violation de données à caractère personnel au sens de l'article 4 du RGPD, peut affecter des personnes concernées situées dans plusieurs Etats membres de l'Union européenne. Dans un tel cas de figure, un responsable de traitement doit notifier cette violation à l'autorité chef de file, c'est-à-dire l'autorité d'un Etat membre compétente en matière de protection des données à caractère personnel qui est l'interlocuteur unique d'un responsable de traitement ou d'un sous-traitant pour le traitement transfrontalier effectué par ce responsable de traitement ou par ce sous-traitant. Il se peut aussi que cette violation provienne d'un responsable de traitement qui n'est pas établi sur le territoire de l'Union européenne, mais qui en vertu du champ d'application prévu à l'article 3 paragraphe 2 du RGPD, est soumis également à cette obligation de notifier une violation de données à caractère personnel. Le cas échéant, ce dernier doit désigner un représentant dans l'UE, conformément à l'article 27 du RGPD.

Dans leurs versions définitives, les lignes directrices du CEPD précisent désormais que la violation devra toutefois être notifiée aux autorités de chaque Etat membre dans lesquels des personnes concernées impactées par la violation de données résident. Par ailleurs, cette notification devra être effectuée conformément au mandat donné par le responsable du traitement à son représentant et sous sa responsabilité.

POUR ALLER + LOIN

LES PRÉCISIONS DU CONSEIL D'ÉTAT SUR L'INDÉPENDANCE FONCTIONNELLE DU DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Dans un arrêt en date du 21 octobre 2022, le Conseil d'Etat a apporté des précisions sur l'indépendance fonctionnelle du délégué à la protection des données.

En l'espèce, une DPO licenciée par une société agissant en qualité de responsable de traitement de données à caractère personnel, avait déposé plainte auprès de la CNIL sur le fondement de l'article 8 de la loi « informatique et libertés » du 6 janvier 1978. Elle contestait les conditions dans lesquelles elle avait exercé ses fonctions de DPO au sein de la société et faisait valoir également la méconnaissance de son droit d'accès à ses données personnelles.

La CNIL ayant clôturé sa plainte, l'ancienne DPO a demandé au Conseil d'Etat l'annulation pour excès de pouvoir de cette décision.

S'agissant de l'exercice du droit d'accès de la requérante à ses données personnelles prévu par l'article 15 du RGPD, le Conseil d'Etat rappelle que la CNIL doit motiver une décision lorsqu'elle refuse de donner suite à une plainte fondée sur la méconnaissance de ce droit, puisque c'est une décision administrative individuelle défavorable refusant un avantage dont l'attribution constitue un droit pour les personnes, au sens de l'article L 211-2 du Code des relations entre le public et l'administration (CRPA). Le Conseil d'Etat estime cependant que la décision de la CNIL à cet égard a été suffisamment motivée.

S'agissant surtout de la question du respect par la société des dispositions relatives aux missions d'un DPO et notamment son indépendance fonctionnelle le protégeant contre toute décision qui mettrait fin à ses fonctions, lui ferait subir un désavantage, ou qui constituerait une sanction en vertu des articles 38 et 39 du RGPD, le Conseil d'Etat rappelle notamment l'éclairage apporté par la Cour de Justice de l'Union européenne (CJUE) dans son arrêt Leistritz AG c/ LH du 22 juin 2022 (C-534/20). Dans cet arrêt, la CJUE considère que bien que les dispositions de l'article 38 paragraphe 3 vise à préserver l'indépendance fonctionnelle du délégué à la protection des données, « elles ne font pas obstacle au licenciement d'un délégué qui ne posséderait plus les qualités professionnelles requises pour exercer ses missions ou qui ne s'acquitterait pas de celles-ci conformément aux dispositions du RGPD ».

En l'espèce, la société a exposé que le licenciement résultait de défaillances dans l'exercice de ses fonctions en invoquant notamment des alertes répétées de non-conformité non motivées et non documentées, une absence de réponse aux sollicitations des salariés de la société, une absence de disponibilité délibérée ainsi que le non-respect de processus internes à la société..., ajoutant que la DPO n'avait jamais fait l'objet de sanctions directes ou indirectes.

Le Conseil d'Etat considère ainsi que l'exigence de protection de l'indépendance fonctionnelle d'un DPO ne fait pas obstacle à ce que la société puisse reprocher à celui-ci des carences dans l'exercice de ses fonctions et le non-respect de règles internes à la société, en l'absence d'incompatibilité de ces règles avec son indépendance fonctionnelle. Dès lors, quand bien même la matérialité de certains des faits reprochés à la DPO ne serait pas établie avec certitude, la CNIL, bénéficiant d'un large pouvoir d'appréciation, pouvait valablement refuser d'engager des poursuites à l'encontre de la société.

Enfin, validant le raisonnement de la CNIL, le Conseil d'Etat confirme l'absence de manquement à l'obligation de fournir au DPO les ressources nécessaires à l'exercice de ses missions (article 38§2 RGPD) qui avait été invoquée à l'encontre de la société, relevant les importantes ressources humaines et opérationnelles octroyées en l'espèce à la DPO.

ACTU SANTÉ NUMÉRIQUE

LES PRÉCISIONS DU CONSEIL D'ÉTAT SUR L'INDÉPENDANCE FONCTIONNELLE DU DÉLÉGUÉ À LA PROTECTION DES DONNÉES

Dans un communiqué de presse publié sur son site internet le 12 octobre dernier, l'Agence du Numérique en Santé (ANS) a mis en ligne une consultation publique au sujet de la version réactualisée de la doctrine du numérique en santé. Cette consultation publique est disponible jusqu'au 30 novembre 2022.

Dans l'objectif d'en améliorer la lisibilité, un travail de simplification sur la forme de la doctrine a été réalisé. Deux chapitres traitent ainsi dans cette nouvelle version des plateformes de santé et des référentiels et services socles et présentent les services associés ainsi que les outils pour en faciliter leur mise en œuvre.

La nouvelle version met également tout particulièrement l'accent sur l'éthique, la sécurité et l'interopérabilité, règles fondamentales pour les services numériques en santé. Elle introduit également deux nouveautés importantes, le service ViaTrajectoire et le service d'accès aux soins (SAS).

Pour participer à cette consultation publique, c'est ici !

PERSPECTIVES
& CHANGEMENTS

LES PRÉCISIONS DE LA CNIL SUR LES ÉLECTIONS PROFESSIONNELLES ORGANISÉS PAR LES EMPLOYEURS PUBLICS OU PRIVÉS

Par une publication sur son site internet le 24 octobre dernier, la CNIL a apporté quelques précisions sur le déroulement des élections professionnelles organisées par les employeurs publics ou privés.

Ces derniers étant en effet amenés à cette occasion à collecter et utiliser les données personnelles des électeurs, la CNIL répond aux questions les plus fréquemment posées en profitant de cette occasion pour rappeler plusieurs principes importants.

Sont notamment abordées la question des mentions que l'employeur peut faire figurer sur la liste électorale concernant ses agents ou salariés ; les formalités du vote par correspondance électronique ; les modalités d'information des électeurs concernés de l'utilisation de leurs données personnelles ; la sécurisation de l'authentification des électeurs en cas de vote électronique...

Pour trouver les réponses à ces questions, c'est par ici !

PERSPECTIVES
& CHANGEMENTS

UNE DÉCISION DU TRIBUNAL ADMINISTRATIF DE PARIS ENJOINT LE HEALTH DATA HUB À CHANGER SA DÉNOMINATION

Dans une décision du 20 octobre 2022, le tribunal administratif de Paris a fait droit à la demande de l'association Francophonie Avenir tendant à changer la dénomination du « Health Data Hub », en se fondant sur la loi du 4 août 1994 relative à l'emploi de la langue française.

En premier lieu, le tribunal administratif de Paris considère que l'utilisation d'une marque anglophone « Health Data Hub » méconnait l'article 14 de la loi précitée disposant que l'emploi d'une marque constituée d'une expression en des termes étrangers est interdit aux personnes morales de droit public dès lors qu'il existait des expressions françaises de même sens approuvées par la commission d'enrichissement de la langue française. Le Health Data Hub entrant bien, dès lors, dans le champ de cette interdiction.

La dénomination « Health Data Hub » a bénéficié d'un enregistrement à titre de marque verbale auprès de l'Institut National de la Propriété Industrielle (INPI) en 2019 et dont son dépôt aurait été retiré par l'Etat français. A ce titre, le tribunal administratif de Paris rappelle que quand bien même les termes « Health Data Hub » ne pourraient être regardés comme une marque déposée mais uniquement comme une simple expression et contrairement à ce que soutient le ministre des solidarités et de la santé, l'expression n'est « pas seulement utilisée dans les activités de promotion de la plateforme des données de santé à l'étranger, mais également dans les supports de communication disponibles sur le territoire français et à destination de la population française, en français, dans de nombreuses manifestations publiques » et méconnait dès lors l'obligation d'utiliser la langue française posée par les articles 3 et 6 de la loi du 4 août 1994.

En conséquence, le tribunal administratif de Paris a enjoint au ministre de la santé et de la prévention de procéder au retrait de l'expression « Health Date Hub » et du sigle « HDT » de l'ensemble des supports de communication destinés au public français sur le territoire national d'ici le 20 avril 2023.

PERSPECTIVES
& CHANGEMENTS

JOE BIDEN SIGNE UN DÉCRET PRÉSIDENTIEL POUR PERMETTRE LES NÉGOCIATIONS SUR UN NOUVEL ACCORD TRANSATLANTIQUE DE TRANSFERT DE DONNÉES

Compte tenu des deux accords bilatéraux de transferts de données personnelles entre les Etats Unis et l'Union Européenne, le Safe Harbor et le Privacy Shield, ayant été invalidés par la Cour de Justice de l'Union européenne (CJUE) en 2016 et en 2020, le président américain Joe Biden a récemment signé un décret présidentiel dans l'objectif de reprendre les négociations sur un nouvel accord transatlantique.

Les suites de ces négociations méritent d'être suivies avec attention. L'avocat Maximilian Schrems a d'ores et déjà répondu dans un communiqué sur le site internet de son association None of Your Business (NOYB). Ce dernier précise par ailleurs qu'à la suite de la signature de ce décret, « la Commission européenne doit rédiger une "décision d'adéquation" en vertu de l'article 45 du GDPR. Une fois le projet de décision publié, la Commission doit entendre le Comité européen de protection des données (EDPB), mais n'est pas liée par ses conclusions. En outre, les États membres européens doivent être entendus et pourraient bloquer l'accord. Ce processus peut prendre quelques mois » et que cette décision n'est pas attendue avant le printemps 2023.

DÉCRYPTAGE SANCTION

LA CNIL CONDAMNE LA SOCIÉTÉ CLEARVIEW AI À UNE SANCTION DE 20 MILLIONS D'EUROS

La société Clearview AI a été condamnée par la CNIL dans une délibération SAN-2022-019 du 17 octobre 2022 à une sanction de 20 millions d'euros, sanction pécuniaire maximale en application de l'article 83 du RGPD. La CNIL n'est pas la seule autorité de contrôle compétente en matière de protection des données à caractère personnel à avoir sanctionné la société Clearview AI puisque cette dernière avait déjà condamnée à une amende de 20 millions d'euros par l'autorité italienne et à 8,85 millions d'euros par l'autorité britannique cette année.

En l'espèce, Clearview AI est une start up américaine collectant en masse des photographies de personnes physiques provenant de divers sites web et réseaux sociaux sans leur consentement. A partir de cette collecte, Cleaview AI a constitué une base d'images de ces personnes sous la forme d'un moteur de recherche, en vue d'une commercialisation. Ce service est ainsi notamment offert aux forces de l'ordre afin d'identifier des auteurs ou des victimes d'infraction.

Ayant reçu dès 2020 plusieurs plaintes de particuliers relatives au logiciel de reconnaissance faciale utilisé par la société, la CNIL a ouvert une enquête tout en coopérant avec ses homologues européens. Elle a ainsi constaté plusieurs manquements au RGPD :

- Un traitement illicite de données personnelles, celui-ci ne reposant sur aucune des bases légales visées à l'article 6 du RGPD. En effet, la société ne recueille pas le consentement des personnes concernées, et ne dispose pas non plus d'un intérêt légitime à collecter et traiter leurs photographies, en particulier eu égard au caractère particulièrement intrusif et massif du procédé (des millions d'internautes français étant concernés) ;
- L'absence de prise en compte satisfaisante et effective des droits des personnes concernées, en violation des articles 12, 15 et 17 du RGPD. La société limite en effet l'exercice du droit d'accès des personnes concernées aux données collectées, ne répond pas de manière effective aux demandes d'accès et d'effacement, et parfois en ne répondant pas du tout à ces demandes.

La présidente de la CNIL avait ainsi mis en demeure la société Clearview AI le 16 novembre 2021, dans un délai de deux mois, de cesser la collecte et l'usage des données de personnes se trouvant en France en l'absence de base légale et de faciliter l'exercice des droits des personnes concernées.

En l'absence de réponse de la part de Clearview IA à la mise en demeure, la CNIL a également relevé un manquement à l'article 31 du RGPD imposant une obligation de coopérer avec les services de la CNIL. La formation restreinte de la CNIL a ainsi été saisie et a prononcé une sanction de 20 millions d'euros. En outre, et au regard de la gravité du manquement pour les droits fondamentaux des personnes concernées, il a été enjoint à la société de ne pas procéder sans base légale à la collecte et l'usage des données des personnes en France et de supprimer les données déjà collectées, dans un délai de 2 mois et avec cette fois une astreinte de 100 000 euros par jour de retard.