NOVEMBRE 2021 : #10

ACTUALITÉS RGPD

By Tchérylène MAIRET - DPO PRO ARCHIVES SYSTEMES

L'EDITO DU DPO

Que ce soit pour la sanction de la CNIL à l'encontre de FranceTest sur la base de dénonciation anonyme le 14 octobre 2021 ou la fuite de 500.000 données personnelles issues de 28 laboratoires d'analyses médicales en mars 2021 sur la base d'une alerte de Médiapart après la découverte de ces fichiers en vente sur le DarkWeb, les conséquences sur la vie privée des personnes concernées sont très graves s'agissant de données de santé.

Or, ces deux faits divers ont en commun que les entreprises elles-mêmes n'ont pas fait la démarche d'avertir dans les meilleurs délais des conséquences pour la vie privée des personnes concernées (art.34 du RGPD), de manière individuelle quand cela est possible, par communication générale quand l'effort est évalué disproportionné.
Un élément extérieur à l'organisation a donc donné l'alerte.
Deux cas de figure sont possibles qui pourraient expliquer cette inertie des organisations : soit elles avaient méconnaissance de cette fuite. Il est donc important de disposer d'outils permettant de monitorer les activités anormales sur les Systèmes d'Informations. Soit les organisations ont craint pour leur image et leur crédibilité vis-à-vis de leurs clients en communicant à leur attention sur l'incident, comme un aveu de faiblesse.

Qu'y a-t-il de pire pour la réputation que l'avis de mise en demeure de la CNIL placardé sur son site, dont les concurrents de ces organisations se délectent ?

Croire à tort que les cyberpirates n'oseraient pas s'attaquer aux hôpitaux ou aux établissements de santé sur la base d'une présumée éthique, c'est sous-évaluer la valeur des données de santé sur le Dark Web:

- Les données de santé renseignent sur le niveau de protection sanitaire d'une population pour un état étranger,
- Les données de santé intéressent les laboratoires pharmaceutiques pour ajuster leur recherche & développement.

Une fuite de données de santé a donc des conséquences pour les personnes concernées et à l'échelle de la nation.

EN BREF

CONSERVATION DES DURÉES DE CONNEXION : PUBLICATION DU DÉCRET 2021-1362

20 octobre 2021 : Publication du décret 2021-1362 encadrant la durée de conservation des données de connexion en application du (II) de l'article 6 de la Loi 2004-575 du 21 juin 2004 pour la Confiance dans l'Economie Numérique.
Cette évolution du régime juridique était rendue nécessaire par la décision de la CJUE du 6 octobre 2020 (C623/17) et celle du Conseil d'Etat du 21 avril 2021 et l'imbroglio juridique quant au conflit entre durée de conservation et protection de la vie privée d'une part et moyens de lutte contre le terrorisme les crimes et délits d'autre part.
Désormais les fournisseurs d'accès internet et plateformes de contenus en ligne doivent, selon les cas, conserver ces données de connexion entre 1 à 5 ans en fonction de leur nature.

Lire l'article

TÉLÉSURVEILLANCE DES SALARIÉS

Un arrêt de la Cour de Cassation du 21 juin 2021 rappelle les conditions d'installation de la vidéosurveillance sur le lieu de travail des salariés. Un tel dispositif est possible pour des finalités de sécurité et non pour le contrôle de l'activité du salarié (hors manipulation de fonds). La preuve à l'appui d'un dispositif de vidéosurveillance ne peut être produite pour une sanction disciplinaire.

Lire l'article

DÉLIBÉRATION PORTANT RECOMMANDATIONS DE LA CNIL CONCERNANT LA JOURNALISATION DES ACTIONS SUR LES SYSTÈMES D'INFORMATION.

Le 14 octobre 2021, la CNIL a publié sa délibération 2021-122 portant adoption d'une recommandation relative à la journalisation. Les dispositifs de journalisation sont définis comme des dispositifs qui permettent d'assurer une traçabilité des accès et des actions des différents utilisateurs habilités à accéder aux systèmes d'information (et donc aux traitements de données à caractère personnel que sont susceptibles de constituer ces systèmes). Ces dispositifs peuvent être adossés soit à des applications (qui sont les briques logicielles spécifiques au traitement mis en œuvre et sont donc sujettes à la mise en œuvre de journaux dits applicatifs), soit à des équipements spécifiques (qui sont des équipements informatiques associés à des logiciels embarqués, sujets à la mise en œuvre de journaux dits périmétriques).

La note du DPO

La journalisation des actions (accès et actions) des différents utilisateurs d'une application ou d'un système d'information permet de conserver la preuve en cas d'atteinte à la confidentialité, l'intégrité des données ou leur perte et d'établir les responsabilités. La journalisation est particulièrement intéressante en cas de contractualisation avec un sous-traitant ayant accès au système d'information.

En savoir +

LA CNIL ORGANISE UNE CONCERTATION SUR LE RÉFÉRENTIEL POUR LA GESTION DES PHARMACIES

Ce référentiel vise à faciliter la mise en conformité des traitements de données personnelles mis en œuvre au sein des officines de pharmacie dans le cadre de la prise en charge sanitaire et de la gestion administrative de leur patientèle/clientèle. Il s'adresse aux officines de pharmacie libérales et à leurs prestataires.
La conformité au référentiel peut être documentée dans le registre des activités de traitement tenu par le délégué à la protection des données, s'il existe.
Depuis l'entrée en application du règlement général sur la protection des données (RGPD), la norme simplifiée 52 adoptée par la CNIL pour encadrer les traitements de gestion des pharmacies n'est plus en vigueur.

La note du DPO

La collecte des données personnelles et de santé des clients des officines a pour finalité a priori la délivrance des médicaments. Certaines pharmacies revendent les données personnelles des clients à des data brokers une fois anonymisées. Si une telle pratique n'est pas considérée illicite en revanche, la pharmacie est tenue par une obligation d'information et la possibilité pour les clients d'exercer leur droit d'opposition. Tout manquement d'information sur cette finalité renverrait à de la collecte déloyale et serait sanctionnée.

En savoir +

LES FOURNISSEURS D'ACCÈS INTERNET (FAI) COMMENCENT À DÉPLOYER LA « PUBLICITÉ SEGMENTÉE »

Permettant aux annonceurs de proposer des campagnes adaptées aux caractéristiques des téléspectateurs, la publicité segmentée se développe peu à peu sur les équipements des fournisseurs d'accès français à l'exception de Free. D'après l'Association pour le développement de services multimédias et multi opérateurs (AF2M), près de 5 millions de foyers (18 %) auraient déjà consenti à l'utilisation de leurs données (âge, sexe, localisation, composition du foyer), soit 30 % des foyers équipés d'un téléviseur IPTV éligible.

La note du DPO

S'agissant de profilage, le consentement préalable des abonnés à l'utilisation de leurs données à des fins publicitaires est obligatoire.

En savoir +

L'ANSSI PUBLIE DES « RECOMMANDATIONS RELATIVES À L'AUTHENTIFICATION MULTI FACTEUR ET AUX MOTS DE PASSE »

L'authentification des utilisateurs accédant un système informatique est un des fondamentaux de la sécurité informatique.
Ce guide de portée très large, élaboré par l'ANSSI avec la contribution de la CNIL, constitue une référence pour l'élaboration de mesures d'authentification, essentielles pour garantir la sécurité des traitements de données personnelles, en application des articles 5 et 32 du RGPD. Il sera nécessaire d'adapter ces mesures aux risques propres à chaque application ou traitement selon le contexte, en étant particulièrement vigilant sur la biométrie, spécifiquement encadrée par le RGPD.
La CNIL s'appuiera sur ce guide pour recommander des bonnes pratiques en matière d'authentification et encourage tous les acteurs du numérique à s'en saisir afin de progresser dans leur conformité à l'obligation de sécurité du RGPD.
Dans ce cadre, une mise à jour de sa recommandation sur l'usage des mots de passe sera rendue publique en 2022.

Accédez au guide de l'ANSSI

FACEBOOK (META) RENONCE À LA RECONNAISSANCE FACIALE SUR LES PHOTOS/ VIDÉOS DE SES CLIENTS.

Facebook a annoncé dans un communiqué du 2 novembre 2021 qu'il abandonne les fonctions de reconnaissance faciale qui, depuis plus de 10 ans, permettent d'identifier les personnes présentes sur les photos mises en ligne par ses abonnés. Les données concernant l'identification faciale de plus d'un milliard d'utilisateurs vont également être définitivement supprimées. Estimant que la reconnaissance faciale peut être utile, Facebook reconnait que cette technologie soulève de nombreuses inquiétudes, en l'absence de règles claires de la part des autorités.

Lire l'article

DES POSTS FACEBOOK DÉNONÇANT LES AUTEURS DE VOLS PRÉSUMÉS DEVIENNENT VIRAUX : POURQUOI C'EST ILLÉGAL

Des publications montrant des auteurs de vols présumés sont partagées des centaines de fois sur les réseaux sociaux. Leur but semble clair : se passer des services de gendarmerie et de la justice et faire appel au plus grand nombre pour retrouver les soi-disant responsables. Mais est-ce bien légal ?
Après avoir rappelé les risques juridiques de cette pratique, le journal régional en ligne Lepays.fr alerte sur le risque de voir se développer un « Far West numérique », et signale des commentaires en ligne proches de l'incitation à la violence.

La note du DPO

Ce n'est pas parce que des données personnelles sont publiques et librement accessibles sur le web que la collecte et le traitement sont autorisés. Cela reviendrait à une collecte déloyale. Le consentement de la personne concernée est obligatoire.
Mis à part les pouvoirs de lutte contre les crimes et délits et le terrorisme des autorités françaises, la collecte d'informations librement accessibles sur le web est autorisée depuis la loi de finances 2020 pour le fisc français pour une durée d'expérimentation de 3 ans.

En savoir +

LA SANCTION DU MOIS

COVID-19 : MISE EN DEMEURE DE LA SOCIÉTÉ FRANCETEST POUR SÉCURISATION INSUFFISANTE DES DONNÉES DE SANTÉ

La présidente de la CNIL a mis en demeure la société privée Francetest de sécuriser les données de santé qu'elle collecte pour le compte des pharmacies à l'occasion de tests de dépistage à la COVID-19. Elle s'est également rapprochée de plus de 300 pharmacies afin qu'elles vérifient leur conformité au RGPD et à l'obligation de sécurité.

Sur la base d'une dénonciation anonyme, la CNIL a mené des contrôles en ligne et dans les locaux de la société afin d'enquêter sur les circonstances de cette violation de données et vérifier les mesures prises pour assurer la sécurité des données. La base de données exposée concernait 386 970 personnes uniques et comportait leur nom, prénom, adresse e-mail, numéro de téléphone, date de naissance, résultat du test (positif ou négatif) et numéro de sécurité sociale (NIR).
La CNIL a constaté que la société avait pris certaines mesures pour remédier à la vulnérabilité à l'origine de la violation de données. Cependant, le service Francetest présente toujours plusieurs insuffisances en matière de sécurité de données. Les données de santé sont hébergées chez un prestataire ne disposant pas d'un agrément HDS (hébergement de données de santé), les processus d'authentification ne sont pas assez robustes, les procédés cryptologiques employés sont faibles et la journalisation (enregistrement des actions des personnes accédant à l'outil) des activités des serveurs est lacunaire.
En conséquence, la présidente de la CNIL a décidé de mettre la société en demeure de prendre toutes les mesures nécessaires pour garantir la sécurité des données de santé qu'elle traite pour le compte de centaines de pharmacies.

En savoir +

LE SAVIEZ-VOUS ?

LA BELLE PROVINCE SE DOTE D'UN RGPD

Le 22 septembre 2021, le Québec a adopté la loi dite « 64 » de modernisation en matière de protection des renseignements personnels.
Largement inspirée du RGPD, qui lui-même s'est inspiré des dispositions de la Loi Informatique et Libertés de la France, le Québec entend moderniser l'encadrement applicable à la protection des renseignements personnels dans diverses lois, dont la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et la Loi sur la protection des renseignements personnels dans le secteur privé.
La loi « 64 » introduit à ces deux lois des règles concernant le traitement des incidents affectant la confidentialité des renseignements personnels par les organismes publics et les entreprises. De plus, la loi oblige ces organismes et ces entreprises à publier des règles encadrant la gouvernance à l'égard des renseignements personnels et, pour ceux qui recueillent ces renseignements par un moyen technologique, à publier et diffuser une politique de confidentialité. Elle y introduit aussi l'exigence qu'une évaluation des facteurs relatifs à la vie privée soit réalisée en certaines circonstances, notamment à l'égard de tout projet de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels.
La loi « 64 » précise diverses exigences relatives au consentement requis préalablement à une collecte, une utilisation ou une communication de renseignement personnel. Ainsi, la loi prévoit que les organismes publics et les entreprises doivent demander à la personne concernée son consentement distinctement de toute autre information communiquée à cette dernière. La loi prescrit que le consentement nécessaire à certaines utilisations ou communications d'un renseignement personnel sensible doit être manifesté de façon expresse. La loi exige également l'obtention du consentement du titulaire de l'autorité parentale pour une collecte, une utilisation ou une communication de renseignement personnel concernant un mineur de moins de 14 ans.

En savoir +