MARS 2023 : #15

L'ACTUALITÉ RGPD

By Tchérylène MAIRET - DPO AGS RECORDS MANAGEMENT

L'EDITO DU DPO

Cocher et ricochet

Le 2 février 2023, le service désinfox de l'AFP – ayant pour mission de débusquer et confondre la désinformation - a publié un article relatif à une rumeur selon laquelle les services d'hospitalisation français avaient mis en œuvre un fichage des patients opposés au vaccin Covid 19 identifiés sous le Code Z281 : « Vaccination non-faite pour raison de conviction ou de pression sociale ». De fait, il existe bien plusieurs « étiquettes » à disposition du médecin pour catégoriser un patient dont les vaccins n'ont pas été réalisés en lien avec sa prise en charge et ce… quelle que soit la nature du vaccin. Ce code est utilisé à des fins de statistiques internes pour l'activité publique hospitalière mises en œuvre par l'Athi et n'alimentent pas le DMP : une telle information n'alimente que le dossier patient de l'hôpital.

Néanmoins, du point de vue du RGPD, il est intéressant d'examiner cette situation sous le prisme de l'exercice du droit à la limitation. En effet la formulation « pression sociale » de ce code pose question : cette catégorie suggèrerait-elle que le patient est un individu sous influence et incapable de discernement ?

En cochant cette case, le médecin est-il certain de la fiabilité et de la pertinence de cette information tel que l'impose l'article 5 aux paragraphes c) et d) du RGPD ? Le médecin réalise-t-il le traitement sur des données objectives ? Et de quels vaccins parlons-nous exactement puisque le cocktail d'injections obligatoires des Boomers n'a rien de comparable avec la génération Z par exemple ?

Demander l'exercice du droit à la limitation (article 18 du RGPD) est une requête complexe à exécuter pour le Responsable de traitement. La plupart des non-conformités sont consécutives à la volonté de mettre en œuvre des indicateurs sur des statistiques très fins ou de collecter trop d'informations sans que la finalité ait été clairement identifiée au départ. L'argument de collecter « au cas où » n'est pas une finalité prévue au RGPD.

Dans le cas présent, le médecin dispose de plusieurs choix concernant la situation vaccinale du patient :

- Z280 : vaccination non-faite en raison d'une contre-indication
- Z281 : Vaccination non-faite pour raison de conviction ou de pression sociale
- Z282 : Vaccination non faite par décision du sujet pour des raisons autres et non précisées
- ….
- Z289 : Vaccination non faite, sans précision

Puisque l'objectif de libérer du temps médical est une des revendications des médecins libéraux justifiant l'augmentation du tarif de consultation, nous pouvons apprécier les tourments induits par ce formulaire : le médecin est englué dans ces choix cornéliens et le patient est rangé dans une case susceptible de révéler (ou de présumer) un comportement face à la vaccination dont la finalité du traitement reste à éclaircir tant la formulation semble maladroite. Quel serait par exemple l'objectif de réaliser des statistiques sur le silence d'un patient (raisons non précisées) ?

En pratique, une bonne case à cocher n'a qu'une vertu : faciliter la mise en œuvre du principe de minimisation par la réduction des libertés d'un champ de texte libre où l'on est susceptible d'en raconter plus que nécessaire. Si le formulaire accouche d'une usine à gaz, il faut se poser la question de l'intérêt et de la transparence de ce traitement auprès de la personne concernée.

EN BREF

DES MOUCHARDS DANS LA MOITIÉ DES EMAILS

Selon le média l'Informaticien.com et sur la base d'une étude de l'éditeur de messagerie Proto Mail, **50%** des e-mails envoyés chaque jour contiennent des traqueurs. Ils collectent et partagent secrètement avec des entreprises et spécialistes du marketing des informations sur les utilisateurs, dont des données sur la localisation, les appareils et les usages, preuve que « *la plupart des expéditeurs veulent savoir si ou quand vous ouvrez leurs e-mails et construire un profil sur vous sans votre consentement.* »

En savoir +

SUR LE DARK WEB, ON BRADE LES DONNÉES PERSONNELLES

Un article de Numérama de janvier 2023 et de Visual Capitalist exposent que la multiplication des fuites de données conduit à une perte de valeur commerciale de ces dernières. Sur le Dark Web, les fichiers de données personnelles s'échangent à des prix ridicules, voire gratuitement. De nos jours, les sites du Dark Web se font concurrence sur leur sécurité et la qualité de leur service client. Il n'est donc pas surprenant qu'ils utilisent désormais également des tactiques de marketing traditionnelles :

- Les remises (pour 2 cartes de crédit clonées, 1 gratuite),
- Les coupons,
- Les avis, évaluations et commentaires des acheteurs.

Privacyaffairs.com analyse ainsi régulièrement la publication de données sur le Dark Web, et note qu'un fichier de 10 millions d'adresses mail est généralement vendu autour de 100 euros. En conclusion, les effets conjugués des réseaux sociaux, des « data brokers », de la multiplication des comptes sur le Web, conjugués au « laxisme de toutes ces entreprises pour la sécurité ont tout simplement fait perdre toute notion d'intimité à certaines informations. »

CAMPAGNE DE SENSIBILISATION À LA CYBERSÉCURITÉ PAR LES VIDEONAUTES

Une campagne de sensibilisation au randsomware a été mise à disposition sur le site internet des Vidéonautes, l'objectif est de promouvoir leur travail et d'aborder la sensibilisation à la cybersécurité sous un angle original.

Voici le scénario :
Cette entreprise subit une CYBERATTAQUE en direct !
Notre Patrick national fait son grand retour pour vanter la sécurité et la fiabilité de son système d'information.

Et pas de bol pour lui… Son entreprise, si bien protégée, subit une cyberattaque ! Ils sont victimes d'un ransomware. Tous les fichiers de la société sont chiffrés et ils sont complètement à l'arrêt !
😨Mais qui peut les attaquer de la sorte ?

Pour Patou, il n'y a aucun doute. Il s'agit d'un coup des "hackers russes". Et ils sont assez faciles à reconnaître :
☢ Ils portent des capuches
☢ Ils se rassemblent dans des caves ou des hangars sombres
☢ Ils disposent de moyens ultra sophistiqués…

Sauf que …

Le coupable c'est lui

LE NUMÉRO 27 DE CYBERUN EST EN LIGNE

Cyberun est un magazine gratuit dédié aux stratégies de cybersécurité relayant beaucoup de témoignages. Le n°27 est dédié aux processus d'automatisation. Pour recevoir ce N° et tous les numéros antérieurs il suffit de vous abonner avec votre adresse e-mail.

La note du DPO

Votre DPO apprécie très particulièrement la rubrique « Les grognements de Cy ». Cyberun n'utilise aucun cookie publicitaire.

ENTREPRISES : LE BUDGET CLOUD PAS DANS LES CLOUS

Selon une étude de Veritas Technologies, réalisée par le cabinet Vanson la quasi-totalité des entreprises semblent avoir une mauvaise lecture de la répartition des responsabilités entre le fournisseur Cloud et l'entreprise notamment autour de la protection des données. En effet, 51 % des entreprises interrogées supposent que leur fournisseur de service cloud protège certains de leurs actifs dans le cloud. En réalité, la majorité de ces derniers précisent qu'ils sont « tenus de garantir la résilience du service en lui-même », mais que c'est au client d'assumer « la responsabilité de la protection des données et des applications qui y sont déployées ».
Résultats, 87 % des répondants ont déjà subi une attaque par ransomware sur leurs environnements cloud parce qu'ils n'ont pas fait appel à des compétences dédiées pour sécuriser leurs données critiques, les laissant ainsi « vulnérables à des attaques par ransomware », faute d'avoir budgétisé cette sécurité dans les dépenses.

En savoir +

ARRÊT DE LA CJUE : EVOLUTION MAJEURE DE L'APPRÉCIATION DES DONNÉES SENSIBLES

Le média Le journal du net.com revient sur un arrêt de la Cour de justice de l'Union européenne (CJUE) rendu le 1er août 2022 aux implications potentielles considérables en matière de protection des données à caractère personnel. Par cette décision, la Cour tranche une question fondamentale ayant fait l'objet d'interprétations divergentes, relative à la qualification juridique du traitement de données à caractère personnel pouvant indirectement permettre de déduire des informations considérées comme sensibles au sens du RGPD. Désormais doit être considéré comme un traitement de données sensibles "*un traitement portant non seulement sur des données intrinsèquement sensibles, mais également sur des données* ***dévoilant indirectement****, au terme d'une* ***opération intellectuelle de déduction*** *ou de recoupement, des informations de cette nature*"

La note du DPO

Cet arrêt de la CJUE a donc des répercutions considérables sur les plateformes de prises de rendez-vous médicaux en ligne. Ainsi le rendez-vous serait (enfin) considéré comme une donnée de santé.

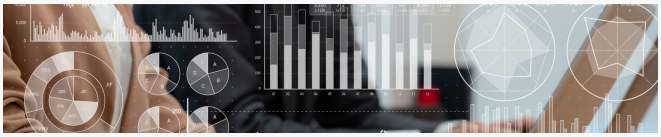
Lire l'article

MICROSOFT VISE UN CLOUD 100% UE POUR LES CLIENTS EUROPÉENS

A partir de Janvier 2023, Microsoft proposera à ses clients européens de circonscrire le stockage et le traitement Cloud au sein de l'Union européenne, afin de « *respecter les valeurs européennes et les besoins de souveraineté* ». Son nouveau programme « *EU Data Boundary* » concernera dans un premier temps les données gérées avec les services Microsoft 365, Azure, Power Platform et Dynamics 365, et s'étendra progressivement à d'autres catégories de données. S'il permet de rassurer les clients et les régulateurs européens, ce programme ne règle pourtant pas les effets extraterritoriaux du Cloud Act américain.

C'est la raison pour laquelle, pour le secteur public, le comité européen à la protection des données dans son rapport du 17 janvier 2023 fixe les actions à mener en faveur d'un Cloud européen souverain et insiste, pour que soit analysée l'exposition du fournisseur au droit d'un pays tiers, même s'il héberge les données en Europe, pour éviter l'accès aux données personnelles par les autorités de ces pays.

Voir le rapport



JOURNÉE DE LA PROTECTION DES DONNÉES : PUBLICATION DU BAROMÈTRE

À l'occasion de la journée de la protection des données le 28 janvier 2023, Qwant, Proton, Olvid et Murena (entreprises du numérique privé en Europe) se sont réunies pour étudier le rapport des Français avec la protection de la confidentialité de leurs données personnelles numériques. Outre la présentation graphique de leur étude, elles proposent un guide intitulé « *Comment protéger votre vie privée sur Internet* ». Il ressort de cette étude que « ***72 %*** *des Français ont conscience de divulguer des informations personnelles lors de leur navigation sur Internet* » tandis que « ***86 %*** *d'entre eux aimeraient être accompagnés pour mettre en place des solutions pour protéger leurs données.* »

Voir le guide

L'AGENCE DU NUMÉRIQUE EN SANTÉ SOUHAITE MUSCLER LA CERTIFICATION HDS VERS PLUS DE SOUVERAINETÉ

L'Agence du numérique en santé a publié fin décembre 2022 sa Feuille de route du numérique en santé 2023 – 2027. Le projet publié précise (page 14) que « *pour renforcer notre souveraineté, le cadre règlementaire sur l'hébergement devra être renforcé* ». Dans ce cadre, « *la nouvelle certification hébergement de données de santé (HDS) évoluera en 2023 pour intégrer un hébergement systématique des données de santé dans l'Espace économique européen (ou dans un pays offrant un niveau de protection adéquat au sens du RGPD) avec des mesures juridiques ou techniques de réduction du risque de transfert extraterritorial des données. Dès qu'une offre suffisamment large sera disponible, les acteurs devront systématiquement opter puis* ***migrer vers des solutions qui ne dépendent pas de droits et capitaux extraeuropéens*** ».

LE REFUS DE COMMUNIQUER LE CODE PIN D'UN TÉLÉPHONE PORTABLE PEUT CONSTITUER UN DÉLIT

Dans une décision du 7 novembre 2022 de la Cour de cassation expose que le refus de communiquer le code de déverrouillage d'un téléphone portable en garde à vue peut constituer un délit.
Même si cette disposition semble pouvoir porter atteinte au droit au silence et au droit de ne pas contribuer à sa propre incrimination le nombre et la diversité des infractions commises par l'intermédiaire de systèmes d'information pose de nombreuses difficultés à la Justice, l'identification et la localisation des auteurs étant rendue difficiles, comme le recueil des preuves numériques, ce qui incite les magistrats à vouloir consulter des preuves sur les téléphones mobiles. Dans ce contexte, le refus de communiquer les codes de déverrouillage d'un téléphone sur réquisition des autorités constitue une infraction pénalement répréhensible.

En savoir +

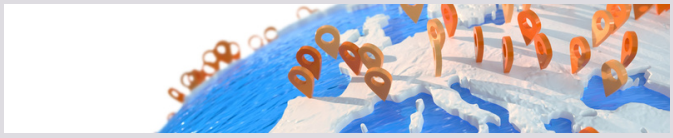
RESPECTE MES DATAS.FR CRÉE LA TEMPÊTE

En janvier 2023, l'association UFC Que Choisir a proposé un service en ligne clé-en-main afin de permettre d'exercer son droit d'accès à ses données personnelles auprès des entreprises accompagné d'une campagne de communication musclée. L'objectif de l'association est de frapper les esprits et de faciliter la reprise de contrôle sur leurs données des citoyens en exigeant la liste exhaustives des données détenues et traitées par ces entreprises ciblant particulièrement les GAFAM.

La note du DPO

Le droit d'accès est un droit commun aux 6 bases légales de traitement.
Néanmoins, l'enjeu de l'exercice des droits n'est pas pour but de satisfaire une simple curiosité. Derrière les probables milliers de demandes suite à l'ouverture de la plateforme, les services DPO des organisations seront probablement submergés. Comment vont-ils réussir à traiter cet afflux de demandes ?
La polémique a au moins le mérite de mettre en lumière que les usagers ont encore des difficultés pour trouver leur chemin jusqu'au DPO.

Découvrir le service



UN DISPOSITIF DE GÉOLOCALISATION DES ÉTUDIANTS FAIT POLÉMIQUE

Le Figaro étudiant.fr signale dans un article du 17 février 2023 que les étudiants de l'École de formation du Barreau de Paris doivent désormais activer leur géolocalisation pour le contrôle de présence et d'assiduité en cours via une application web. Cette géolocalisation complète la signature électronique d'émargement.
Auparavant, les étudiants devaient badger avant d'intégrer une salle pour indiquer leur présence en classe. Mais un trop grand nombre d'élèves profitaient de ce système pour confier leurs badges à un camarade pour signaler leur présence à leur place.
Depuis un mois, un contrôle d'émargement se réalisait aléatoirement par le biais de feuilles de présence classiques mais ne semblait pas satisfaire la Direction de l'établissement.

La note du DPO

Comme pour les dispositifs s'appuyant sur la biométrie dans les établissements scolaires (accès ou facturation des repas de cantine) la Cnil s'est systématiquement prononcée en faveur du dispositif le moins intrusif et le plus respectueux de l'équilibre entre le respect des libertés et droits fondamentaux et l'intérêt légitime du Responsable de traitement. Une fois encore l'Analyse d'Impact obligatoire dès lors qu'un traitement de données sensibles est mis en œuvre devra répondre à la question : est-il possible de faire autrement pour un meilleur respect de la vie privée des étudiants ? Or, le fournisseur Edusign met à disposition une palette de solutions d'émargement sans géolocalisation. Et quid des étudiants ne disposant pas de Smartphones ?

LE TINDER DES EMBOUTEILLAGES

Vous êtes coincé dans les embouteillages et vous apercevez une jolie inconnue au volant de sa voiture et vous ne pouvez pas l'aborder. Comment la retrouver ? Le gérant du site Carmmat propose de prendre en photo la plaque minéralogique du véhicule de la belle inconnue et de la renseigner dans son application. Si la jeune femme est également utilisatrice de l'application vous pouvez ainsi la retrouver grâce à son numéro d'immatriculation et proposer de prendre contact.

La note du DPO

A l'époque de ce reportage, le traitement posait un problème de durée de conservation des données. Si la belle inconnue n'est pas utilisatrice de cette application, son numéro de plaque d'immatriculation ainsi collectée – à son insu – pouvait rester sans limite de temps dans les bases de données. Une étude d'Impact menée au préalable de cette communication aurait suggéré de mieux encadrer projet au regard du RGPD...