Lettre AFCDP – L'actualité des Données Personnelles

Cette édition regroupe plusieurs « news » récemment diffusées dans la lettre de veille de l'AFCDP (Association Française des Correspondants à la protection des Données à caractère Personne).

➲ Vous souhaitez recevoir gratuitement la newsletter mensuelle « L'Actualité des données personnelles » au format électronique ? Il vous suffit de le demander par email à delegue.general@afcdp.net, en indiquant vos coordonnées professionnelles.

L'actualité des Données personnelles (France) :

Un employeur « piégé » par son propre Règlement intérieur

Un dirigeant d'entreprise avait accédé aux emails de l'un de ses salariés hors sa présence. Or le règlement intérieur de l'entreprise prévoyait que les messageries électroniques des salariés ne pouvaient être consultées par la direction qu'en présence du salarié, peu importe leur caractère personnel ou professionnel. La chambre sociale de la Cour de cassation a confirmé, dans un arrêt rendu le 26 juin 2012, la décision de la Cour d'appel de Rouen.

Cloud Computing : résultats de la consultation publique de la CNIL

Comme nous vous l'avons annoncé, la CNIL a publié la synthèse des réponses à sa consultation…On y parle de PLA, d'obfuscation, de responsabilité partagée, de BCR sous-traitants… La Chef du Service International de la CNIL viendra présenter ces résultats devant le groupe AFCDP « Flux transfrontières » courant septembre. Signalons également la publication d'une opinion du Groupe Article 29 sur ce même sujet (WP 196).

Interdits de stade à tort ?

«*Je vais écrire au club pour savoir ce qu'on me reproche. Si je n'ai pas de réponse, je réfléchirai à aller au tribunal. Je trouve cela dégradant… J'ai toujours été irréprochable* »... certains supporters du PSG sont surpris de figurer sur ce qui ressemble à une liste noire de personnes auxquelles le club refuserait de vendre des places, et évoquent un dépôt de auprès de la CNIL. La Commission serait d'ailleurs « en cours d'intervention ».

Patriot Act : et si la société mère américaine envoie ses auditeurs à Paris ?

Parmi les questions intéressantes que soulève cet article, on relève une hypothèse selon laquelle les autorités américaines pourraient avoir accès aux données d'une société française utilisant un Cloud : « *On donne ainsi l'exemple d'une société mère de droit américain qui enverrait, dans ses filiales à l'étranger, une équipe de contrôleurs de nationalité américaine. Ces citoyens américains sont soumis aux dispositions du Patriot Act, en tant qu'Américains, et ce même lorsqu'ils sont à l'étranger. Ces personnes pourraient faire l'objet d'une demande de communication des données conservées par la filiale et auquel le contrôleur aurait eu accès.* »

Dictaphone : la salariée aurait dû être appelée

Elle enregistrait les conversations se déroulant au sein de l'entreprise, à l'insu des intéressés, grâce à un dictaphone caché sous l'écran de son ordinateur. Elle est licenciée pour faute grave, décision confirmée en appel. La Cour de cassation en décide autrement, considérant que…

La CNIL contrôle à nouveau le fichier de police STIC

La Commission lance une nouvelle campagne de contrôle du Système de traitement des infractions constatées, qui comprendra dix visites « sur place » (commissariats et tribunaux) et 34 contrôles « sur pièces ». Les conclusions devraient être publiées début 2013.

Consultation de sites pornographiques

Deux affaires viennent d'être jugées. Dans un cas, la Cour de cassation a considéré que la faute grave n'était pas caractérisée, dans la seconde elle a confirmé le licenciement pour faute grave.

Elle avait informé la CNIL : 175.000 € d'indemnités

Commerciale dans une entreprise de fruits et légumes du Vaucluse, Simone a fait appel au défenseur des droits pour contester son licenciement. « *J'avais d'abord subi d'énormes pressions de la part de mon patron pour avoir informé la CNIL d'une surveillance abusive des employés via des caméras et des micros. Mais c'est après avoir décidé d'organiser des élections syndicales que j'ai reçu une lettre de licenciement, que l'inspection du travail a ensuite refusée.* ». L'employeur a été

condamné pour licenciement discriminatoire, lié à l'engagement syndical de Simone, par le conseil des prud'hommes d'Avignon. Il devra lui verser 175 000 € d'indemnités.

Phising utilisant le logo de la CNIL

Depuis le mois de juillet, une campagne d'emails frauduleux usurpant le nom et le logo de la CNIL vise à récupérer des données personnelles contre rémunération.

Terra Nova propose de transformer la CNIL en APLIN

Le *think tank* proche du Parti socialiste a publié le 15 octobre un rapport contenant 123 propositions pour le développement du numérique en France. Parmi celles-ci figure le transfert d'une partie des missions de l'Hadopi à la CNIL, notamment le suivi de l'usage des œuvres (comptage anonyme des échanges ou téléchargement). Terra Nova prône aussi la « transformation » de la CNIL en pôle de régulation articulé autour de la protection des libertés (proposition n°30). La CNIL serait transformée en Autorité de protection des libertés numériques (APLIN) et récupérerait aussi certaines des attributions du CSA.

Elle avait informé la CNIL : 175.000 € d'indemnités

Commerciale dans une entreprise de fruits et légumes du Vaucluse, Simone a fait appel au défenseur des droits pour contester son licenciement. « *J'avais d'abord subi d'énormes pressions de la part de mon patron pour avoir informé la CNIL d'une surveillance abusive des employés via des caméras et des micros. Mais c'est après avoir décidé d'organiser des élections syndicales que j'ai reçu une lettre de licenciement, que l'inspection du travail a ensuite refusée.* ». L'employeur a été condamné pour licenciement discriminatoire, lié à l'engagement syndical de Simone, par le conseil des prud'hommes d'Avignon. Il devra lui verser 175 000 € d'indemnités.

Spam par SMS : un député apostrophe le gouvernement

Ces dernières années, le nombre de messages indésirables envoyés par SMS a nettement progressé. Une question écrite a été adressée par le député Philippe Meunier à Benoît Hamon, Ministre en charge de la consommation. Il demande quel est le plan d'action de l'exécutif face à cette « véritable nuisance » pour les usagers. Début Octobre l'ICO (Autorité de contrôle britannique) a infligé une sanction financière de 250.000 £ à deux diffuseurs de SMS « non-désirés ».

Le Conseil d'Etat confirme l'avertissement public de la CNIL à Acadomia

L'avertissement public que la CNIL avait infligé à Acadomia pour avoir traité des données non pertinentes, excessives et inadéquates sur les enseignants employés et sur ses clients parents ou enfants constituait une sanction proportionnelle aux manquements constatés, a considéré le Conseil d'Etat dans un arrêt du 27 juillet 2012.

Le prestataire qui a découvert la fuite et qui propose un audit placé en garde à vue

Une clinique de l'Est de la France laisse « fuir » des dossiers médicaux qui se retrouvent indexés sur le Web. Le PDG de la clinique en est averti par un prestataire qui lui propose ses services pour la réalisation d'un audit de sécurité. Or, ce même prestataire est intervenu dans l'établissement un mois auparavant pour installer un anti-virus. Le PDG de la clinique fait appel à la police. D'après le responsable, le prestataire, « dossier médical en mains » lui aurait réclamé rapidement 10.000 €.

Avertissement de la Cnil au moteur de recherche Yatedo

Visé par une trentaine de plaintes d'internautes, Yatedo a reçu un avertissement public de la part de la CNIL. Parmi les motifs de mécontentement, l'incapacité pour les plaignants, malgré des demandes réitérées, d'obtenir la suppression des données les concernant et le « défaut de coopération » de l'entreprise. Découvrez l'interview du responsable de Yatedo, qui indique avoir récemment bénéficié d'une levée de fonds d'1,2 millions d'euros.

L'actualité des Données personnelles (Monde) :

Les députés allemands profitent d'un match de foot pour faire passer une loi sur les données personnelles

Il aura suffi de 57 secondes, en pleine demi-finale de l'Euro 2012 Allemagne-Italie, à une trentaine de députés de la majorité gouvernementale pour voter en première lecture, sans débat, une loi autorisant les services municipaux à communiquer des données privées concernant leurs citoyens à des tiers, à des fins éventuellement commerciales.

Google Analytics : La Norvège fronce les sourcils

L'autorité de contrôle norvégienne pointe du doigt l'utilisation que font l'administration fiscale et une entité du Ministère de l'éducation de *Google Analytics* sans prendre la précaution de flouter les adresses IP avant leur transfert à Google.

British Airways a-t-il été trop loin avec son programme « Know Me » ?

L'initiative prise par la compagnie aérienne britannique a provoqué de multiples réactions. British Airways créé un « dossier » sur chacun de ses passagers, alimenté par des recherches Google. De cette façon, le personnel de bord peut, par exemple, disposer de la photo des passagers avant même qu'il ne pénètre dans l'appareil.

« Quel est votre code postal ? »

Cette question anodine nous est souvent posée au passage à la caisse de certains magasins. Mais cette donnée (et sa collecte) pourrait s'avérer problématique si elle était « croisée » avec d'autres informations - comme les références de la carte de crédit utilisée pour régler l'achat. Une décision de jurisprudence très récente en Californie confirme l'interdiction faite aux commerçants de demander le ZIP code aux clients qui règlent par carte.

Une mairie forçait les chauffeurs de taxi à enregistrer les conversations tenues dans leur véhicule

L'Autorité de contrôle britannique exige que la ville de Southampton cesse d'imposer une telle pratique auprès des conducteurs de taxi, la trouvant disproportionnée. Par ailleurs la municipalité d'Islington est placée sous les projecteurs après avoir égaré des données personnels de personnes dont elle avait aidé au relogement. Parmi ces données figuraient les « préférences sexuelles » des bénéficiaires !

Téléphonie mobile : 6 millions de clients en danger ?

Un client s'est aperçu qu'il pouvait facilement « attaquer » son propre compte, protégé seulement par un mot de passe composé de 6 chiffres. Une attaque en force brute vient facilement à bout du million de possibilités. L'intrusion permet de lire le journal des appels et des SMS, de changer le téléphone associé au compte et donc recevoir les appels/SMS du compte, d'acheter un nouveau téléphone avec la carte bancaire associée au compte, de changer le mot de passe du compte ainsi que l'adresse mail du compte.

Faut-il s'assurer pour le risque « Data Breach » ?

Un débat se développe sur cette question aux Etats-Unis. Dans ce « billet d'humeur » il est évoqué le manque de recul et la grande variabilité des offres existantes. Une entreprise américaine, victime d'une Data Breach et qui s'était assurée contre ce type de risque, est en litige avec son assureur. Le contrat prévoyait une couverture allant jusqu'à 6,8 millions de dollars mais l'assureur arguait qu'il n'avait pas à couvrir les pertes liées « indirectement » à l'incident. Un juge en a décidé autrement.

Des balises GPS cachées dans ses barres chocolatées

La filiale anglaise de Nestlé lance un jeu qui permettra à six clients de gagner 10.000 £. Il suffira à ces derniers d'acheter par hasard l'une des barres chocolatées hébergeant un "mouchard" GPS qui s'activera à l'ouverture du déballage. La campagne est baptisée « We Will Find You ». Cette campagne n'est pas la première du genre. La lettre de veille AFCDP avait déjà fait état d'une opération similaire menée par un lessivier au Brésil.

Comment « détruire » des données personnelles ?

L'autorité de contrôle britannique, l'ICO, vient de publier une synthèse sur les différentes façons d'effacer des données d'un disque dur, d'un PC portable, etc.

Des ordinateurs proposés en location étaient équipés de logiciels espions

La FTC révèle que sept entreprises proposant des ordinateurs en location ainsi qu'un éditeur de logiciel avaient équipé les PC de logiciels espions. L'outil ne se limitait pas à l'activation de la Webcam mais est également capable d'enregistrer les frappes clavier et de prendre des copies d'écran.

Quelle est la valeur d'un profil public pour Facebook ou Google ?

Une nouvelle extension de protection de la vie privée pour les navigateurs Chrome et Firefox affiche une estimation des revenus que tirent des acteurs tels que Facebook ou Google des profils et des données personnelles. Un profil bien renseigné ne rapportait « que » 4,29 dollars par an à Facebook. En revanche, un utilisateur suisse rapporterait annuellement plus de 800 dollars à Google, selon l'extension. Selon un autre testeur, Facebook tracerait 87 % des sites qu'il visite, ce qui leur rapporterait 0,40 dollars par an.

Deux hôpitaux anglais écopent d'une sanction de 325.000 £ (400.000 €)

Les hôpitaux de Brighton et de l'Université du Sussex (gérés par la Sécurité sociale britannique, le NHS Trust) se sont vus infligés une sanction financière de 325.000 £ à la suite de "*serious breach of the Data Protection Act*" par l'ICO. Des données patients avaient été retrouvées dans des disques durs vendus aux enchères en octobre 2010. Les établissements ont fait appel.
L'ICO a également frappé le Belfast Health Trust d'une sanction de 225.000 £ : les dossiers de 20.000 patients avaient été retrouvés dans les bâtiments d'un hôpital fermé en 2006.

Ministère de la santé : Un cinquième employé licencié

La Ministre de la Santé du Canada vient de confirmer qu'elle avait pris cette décision cet été, suite à des fuites de données personnelles.

Les Chemins de Fer néerlandais sanctionnés à hauteur de 125.000 €

L'autorité de contrôle néerlandaise (CBP) a pris cette décision pour avoir conservé trop longtemps, malgré les rappels à l'ordre de la CBP, les données personnelles d'étudiants.

La résistance du mot de passe changerait avec l'âge

Une étude publiée par le chercheur Joseph Bonneau, vient établir que la résistance des mots de passe se renforcent avec l'âge, que la complexité n'est pas la même en fonction de la langue native des utilisateurs (ceux qui parlent allemand ou coréen ont en moyenne des mots de passe plus complexes) et les femmes utilisent globalement des séries de caractères plus complexes que les hommes. Reste tout de même que dans la très grande majorité des cas, les mots de passe sont bien trop faibles.

Un voleur d'iPhone localisé grâce à la fonction de géolocalisation

Le policier en charge de l'affaire a noté que sa propriétaire utilisait iCloud et l'application «Localiser mon iPhone ». Il ne lui aura pas fallu plus de quelques minutes pour retrouver la position du voleur, qui n'a pas eu la présence d'esprit d'éteindre l'appareil ou de désactiver iCloud.

Marketing comportemental basé sur les émotions ?

Microsoft vient de déposer une demande de brevet pour un dispositif qui vise à lier la publicité en ligne avec les émotions des internautes, sur base de la reconnaissance des expressions faciales et du statut Facebook. La demande donne pour exemple de personnes « *unhappy* » celles qui suivent un régime amaigrissant…

Le leader des « Credit Bureau » allemands envisage de récupérer des informations sur les réseaux sociaux

Des journalistes ont révélé que la société Schufa avait constitué un groupe de travail interne pour étudier la récupération d'informations personnelles sur les réseaux sociaux afin de déterminer l'assise financière d'une personne. Les associations de consommateurs, très puissantes outre Rhin, sont furieuses. Mais, selon cet autre article, ces pratiques ne seraient pas rares.

Biométrie : Un chercheur chinois propose d'utiliser le rythme cardiaque

Son équipe a construit un prototype fonctionnel qui permet de reconnaitre l'utilisateur grâce à l'enregistrement des battements via les paumes des mains.

Vie de l'Association :

Comment appliquer le guide « Diversité » sur le terrain ?

Pour répondre à cette question, les membres sont conviés à une nouvelle réunion du groupe de travail « Ressources Humaines » le jeudi 12 juillet 2012 matin. Nous décrypterons ensemble le guide « Mesurer pour progresser vers l'égalité des chances » publié conjointement par la CNIL et le Défenseurs des Droits, qui précise dans quel cadre légal peut être effectuée une mesure de la diversité (notamment de l'origine, dans les fichiers de ressources humaines en comparant les situations occupées par les salariés) et une enquête au sein d'une organisation en interrogeant le vécu et les perceptions des salariés sur les discriminations.

Quelle synergie entre RSSI et CIL ? Un RSSI peut-il être également CIL ?

La conférence organisée conjointement par le Clusif et l'AFCDP « RSSI - CIL, deux fonctions, un objectif commun » qui se tiendra le jeudi 25 octobre 2012 après-midi apportera des réponses concrètes à ces questions.

On recherche un « Data Privacy Leader »

Une grande entreprise recherche son responsable de la protection des données personnelles. La rubrique « Offres de stages et d'emplois » de l'AFCDP attend votre visite.

Les Membres de l'AFCDP ont eu la primeur de la nouvelle NS48 (prospect clients)

A l'occasion de la conférence-débat organisée le 22 juin sur le thème de la conformité des traitements de données « Prospects-Clients », le représentant de la CNIL a dévoilé ce que sera la nouvelle norme simplifiée. Quelques temps forts de cette manifestation : « *CIL : Faites des audits Cookies !* », « *Gestion des désinscriptions : Pensez à tenir une liste repoussoir à conserver au moins trois ans* », « *Arrêtons de travailler en silo ! Rien de vaut le dialogue pour une bonne compréhension mutuelle. Joignons nos efforts pour réaliser des opérations de sensibilisation…pas seulement réservées aux forces commerciales, mais aussi auprès l'encadrement* ».

Bilan annuel du CIL : Comment s'y prendre ?

Pour de nombreux CIL, la fin d'année est la période d'établissement de leur bilan annuel. Nous proposons aux personnes intéressées (CIL expérimentés ayant plusieurs bilans à leur actif et souhaitant "confronter" leur pratique et CIL récemment désignés se posant quelques questions sur cet exercice) de se réunir le jeudi 20 décembre matin, pour un échange informel et sympathique.

Contrôle sur place : Avez-vous rédigé des procédures ?

Nous organisons une réunion d'échanges sur le thème des contrôles sur place de la CNIL le mercredi 9 janvier 2013 matin. L'objectif est de comparer les différentes procédures que nous avons chacun conçues (consignes pour les différents acteurs impliqués, notes de service, etc.) afin de les « mettre à l'épreuve ».

Voici quelques sujets abordés ces derniers jours sur AGORA AFCDP (réseau social réservé aux Membres) :

Pouvons-nous « piéger » nos bases de données ?
Comment inviter les Délégués du personnel à ne pas citer de nom de personnes ?
Gestion des délégations de pouvoirs et de signatures : Quel formalisme vis-à-vis de la CNIL ?
Gestion des indemnités de fin de Carrière : Peut-on la basculer en mode SaaS ?
Quelles informations du dossier du personnel papier d'un agent hospitalier public peut-on conserver au-delà de 5 ans ?
eMailing avec changement de finalité : Comment s'y prendre ?
Médecine professionnelle : Quelle déclaration ?
Zone de Libre Commentaire : Comment les maîtriser ?
Puis-je contacter un client via un réseau social ?
Données Locataires : Puis-je les transmettre aux communes ?
Détection d'images pédopornographiques – Quelles précautions prendre ?
Surveillance des appels passés depuis les portables professionnels
Promouvoir le covoiturage en diffusant la commune de résidence des collaborateurs ?
Réseaux Sociaux d'Entreprise : Et si les utilisateurs sont à l'étranger ?
Articulation entre lois CADA et Informatique et Libertés
Droit à l'image : Communication et inscription au registre des traitements ?
Mise en conformité d'un accueil d'établissement
Appels téléphoniques entrants : Comment informer les personnes ?
Enquêtes administratives et protection de la vie privée : qu'est ce qui est permis ?
Gestion de Réservation de Ressources : quelles formalités ?

Agenda des réunions AFCDP

10 juillet – Paris – Présentation du livrable AFCDP « Données personnelles de santé » à l'ASIP Santé
12 juillet – Paris – Repas mensuel entre membres
11 septembre – Rennes – Réunion Informatique et Libertés, avec visite du Musée Ferrié
11 octobre 2012 – Lyon – Réunion du groupe AFCDP « Lyon°+ »
15 octobre – Paris – Réunion du Groupe « Données Prospects et Clients »
25 octobre – Lille – Repas entre Membres et Sympathisants AFCDP
26 octobre – Toulouse – Réunion conjointe Club 27001/AFCDP Sud-Ouest
8 novembre– Limoges – Conférence « Informatique et Libertés » à la CCI
7 décembre – Marseille – Réunion de la section AFCDP Sud au Port Autonome de Marseille
14 décembre – Tours – Café juridique « Informatique et Libertés » à la Chambre de Métiers et de l'Artisanat d'Indre-et-Loire, Valérie Bel (l'AFCDP sera représentée par MmeValérie Bel, co-animatrice du groupe « Grand Ouest »)
18 décembre – Nantes – Réunion de la section AFCDP Grand Ouest
18 décembre – Toulouse – Réunion de la section AFCDP Sud-Ouest
19 décembre– Paris – Réunion du groupe « Données de santé »
20 décembre – Paris – Réunion « Comment établir son Bilan annuel ? »
9 janvier – Paris – Réunion « Procédures pour se préparer à un contrôle de la CNIL »
25 janvier – Paris – 7ème Université AFCDP des CIL

Directeur de la publication : Paul-Olivier Gibert, Président de l'AFCDP.
Afin que cette lettre soit à la fois un outil d'information mais également d'échanges, vous pouvez contacter pour toute réaction, commentaire et contribution, la rédaction : Bruno Rasle : delegue.general@afcdp.net
Si vous pensez que cette lettre peut intéresser des tiers, n'hésitez pas à leur signaler son existence.
Si vous ne souhaitez plus recevoir cette lettre d'informations, merci de le signaler par retour d'email (adresse delegue.general@afcdp.net)

Cette édition regroupe plusieurs « news » récemment diffusées dans la lettre de veille de l'AFCDP (Association Française des Correspondants à la protection des Données à caractère Personne).

➲ Vous souhaitez recevoir gratuitement la newsletter mensuelle « L'Actualité des données personnelles » au format électronique ? Il vous suffit de le demander par email à delegue.general@afcdp.net, en indiquant vos coordonnées professionnelles.