Futur Règlement européen sur la protection des données, qui est concerné ?

Futur Règlement européen sur la protection des données, qui est concerné ?

Le 25 février dernier, Arendt & Medernach organisait une conférence sur le futur Règlement européen sur la protection des données (ci-après « le Règlement »[1]afin de permettre aux entreprises de mieux comprendre les nouvelles obligations auxquelles elles seront prochainement soumises et leur procurer l'essentiel de ce qu'il faut retenir de ce nouveau texte.

Contexte

Après deux années riches en actualités en matière de données personnelles (droit à l'oubli consacré par la Cour de Justice de l'Union européenne (CJUE)[2], et invalidation du Safe Harbor[3] notamment), le nouveau Règlement arrive à point nommé pour remplacer le cadre juridique actuel adopté il y a plus de 20 ans[4].

4 ans de discussions et 4000 amendements ont été nécessaires pour parvenir à un accord autour de ce nouveau texte qui sera adopté en mai/juin prochain. Il sera applicable dans deux ans à compter de sa date d'entrée en vigueur, soit pour l'été 2018.
Si l'échéance semble lointaine, il est toutefois nécessaire d'envisager dès à présent les changements apportés par ce nouveau texte.

De nouvelles obligations pour les entreprises

Il résulte de ce Règlement diverses obligations pour les entreprises et notamment :

• De mettre en œuvre les principes de « privacy by design / privacy by default» afin d'assurer une protection des données dès leur conception et par défaut ;
• De tenir des registres des traitements de données personnelles sauf cas exceptionnels ;
• De notifier toute violation de données dans les 72h auprès de l'autorité de contrôle voire de la personne concernée le cas échéant ;
• De détailler/préciser l'information des personnes concernées ;
• D'adapter leurs contrats de sous-traitances ;
• D'assurer la portabilité des données ;
• De nommer un Délégué à la Protection des Données le cas échéant.
• Les entreprises doivent envisager ces obligations avec le plus grand sérieux puisque de nouvelles sanctions financières pourront désormais être prononcées par les autorités nationales de protection des données. En effet, selon le manquement, ces sanctions pourront atteindre de 2 à 4% du chiffre d'affaires mondial d'une entreprise ou de 10 à 20 millions d'euros, le montant le plus important devant être retenu.

Qu'est-ce qu'une donnée personnelle ?

"Les données à caractère personnel sont définies par le futur Règlement comme « toute information concernant une personne physique identifiée ou identifiable ; est réputée identifiable une personne qui peut être identifiée directement ou indirectement , notamment par référence à un identifiant, par exemple un nom, un numéro d'identification, des données de localisation ou un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, économique, culturelle ou sociale ».
Cette définition est identique à celle prévue actuellement dans la loi luxembourgeoise[7] mais elle ajoute quelques exemples. Il est notamment précisé qu'un identifiant en ligne, tel qu'une adresse IP, peut être qualifié de données à caractère personnel," explique Héloïse Bock, Partner Arendt & Medernach.

Est-ce qu'on peut dire que toutes les entreprises seront concernées par ce nouveau Règlement ?

"Le champ d'application du règlement est élargi puisque celui-ci aura vocation à s'appliquer à toutes les entreprises traitant des données personnelles dès lors qu'elles sont établies sur le territoire de l'Union européenne ou, lorsqu'elles sont établies hors de l'Union européenne si ces traitements ciblent des citoyens européens.
Un grand nombre d'entreprises seront ainsi concernées en pratique," poursuit-elle.

Des droits nouveaux et renforcés

Pour les personnes concernées, ce nouveau Règlement introduit le célèbre droit à l'oubli ou droit à l'effacement, déjà consacré par la CJUE en 2014[5] mais également, le droit à la portabilité des données qui permet de transférer les données d'un prestataire vers un autre. Les droits d'accès, d'opposition et de rectification des données ainsi que le droit à l'information, existants dans le cadre juridique actuel, sont maintenus et renforcés.

Les transferts de données hors de l'Union européenne

Concernant les transferts de données en dehors de l'Union européenne, le Règlement ajoute de nouvelles bases de légitimité ponctuelles/limitées sur lesquelles un responsable de traitement pourra se fonder en cas de transfert vers un pays n'assurant pas un niveau de protection adéquat.
Le sort des transferts de données réalisés vers les Etats-Unis n'est pas réglé par le Règlement, toutefois, une nouvelle décision d'adéquation est attendue très prochainement[6]. La Commission européenne et les États-Unis se sont en effet accordés sur un nouveau cadre pour les transferts transatlantiques de données le mois derniers : le «bouclier vie privée UE-États-Unis» ou « EU-US Privacy Shield ».

To do list avant 2018

Pour conclure, les avocats d'Arendt & Medernach ont dressé une « to do list » générale reprenant les points suivants :

• Recenser les traitements de données réalisés en pratique et leurs finalités;
• Faire un audit pour évaluer le niveau de conformité actuel et identifier les lacunes;
• Réaliser un « mapping » de tous les transferts de données en considérant les catégories de données, les destinataires des transferts, les bases de légitimité etc.;
• Effectuer des études d'impact lorsqu'un traitement à risque est envisagé;
• Nommer un délégué à la protection des données si nécessaire;
• Mettre en place ou adapter la documentation existante (registres, policies, contrats de sous-traitance, etc.)

[1] Proposition de Règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données) (2012/0011 COD)
[2] CJUE, 13 mai 2014, affaire C-131/12
[3] CJUE, 6 octobre 2015, affaire C-362/14
[4] Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
[5] CJUE, 13 mai 2014, affaire C-131/12
[6] http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf
[7] Loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel
… [Lire la suite]

Réagissez à cet article

Source : *Futur Règlement européen sur la protection des données, qui est concerné ?*

L’Europe renforce la pression sur Apple pour ouvrir l’accès aux données personnelles des utilisateurs

	L’Europe renforce la pression sur Apple pour ouvrir l’accès aux données personnelles des utilisateurs

---

Suite aux attaques terroristes de Bruxelles, les autorités européennes envisagent de forcer Apple et d'autres sociétés à ouvrir l'accès aux données personnelles des utilisateurs aux services spéciaux.

Les parlementaires français ont déjà commencé les débats sur le projet de loi à ce sujet. Ils sont convaincus qu'en choisissant entre l'élargissement des pouvoirs des services de sécurité en vue de prévenir des attentats terroristes et le respect de la vie privée, il est raisonnable d'opter pour le premier choix, lit-on dans le New York Times.
Les députés proposent de sanctionner les chefs des sociétés spécialisées dans les technologies de pointe, qui refusent de fournir des informations aux enquêteurs, d'une peine privative de liberté de cinq ans au maximum et d'une amende de 350.000 euros. Selon le New York Times, telle est également la position adoptée par le Royaume Uni.
Les sociétés en question quant à elles essayent de faire de leur mieux pour éviter un tel scénario. Ces derniers temps, le président d'Apple Tim Cook a personnellement rencontré plusieurs politiciens européens, y compris le premier ministre français Manuel Valls et la chef de la diplomatie britannique Theresa Mary May afin de s'assurer leur appui.Auparavant, le tribunal de Californie avait ordonné à Apple de fournir aux enquêteurs du FBI, dans l'affaire de l'attaque terroriste de San Bernardino, des données chiffrées sur l'iPhone du terroriste tué, après que l'entreprise ait refusé de coopérer volontairement avec les autorités.
Le directeur général d'Apple, Tim Cook, avait rétorqué que cette exigence présentait une menace pour la sécurité de ses clients, tandis que ses conséquences « étaient hors du cadre légal ». La société a refusé de se conformer à la décision du tribunal, déclarant avoir l'intention de faire appel… [Lire la suite]

Réagissez à cet article

Source : *Après Bruxelles, l'Europe renforce la pression sur Apple*

Les notaires marocains sensibilisés à la protection des données personnelles

	Les notaires marocains sensibilisés à la protection des données personnelles

L’accent a été mis sur les dispositions de la loi 09-08, mais aussi sur le rôle et les missions de la Commission nationale de contrôle de la protection des données à caractère personnel.

Les notaires ont été invités le 23 mars dernier, à prendre part à un séminaire placé sous le thème «Le notaire, quel rôle en matière de protection des données personnelles ?».

La rencontre organisée par la Commission nationale de contrôle de la protection des données à caractère personnel (CNDP), en partenariat avec le Conseil national de l’ordre des notaires du Maroc (CNONM) avait pour but de mettre la lumière sur les dispositions de la loi 09-08 relative à la protection des personnes physiques à l’égard du traitement des données à caractère personnel, mais aussi sur le rôle et les missions de la CNDP.

Ainsi, les notaires ont eu l’occasion de mieux appréhender les enjeux liés à la protection des données personnelles dans l’exercice de leur mission. Le séminaire leur a aussi permis de situer leur rôle dans la consécration des droits des citoyens à la protection de la vie privée et des données personnelles, et de prendre connaissance des obligations légales en vigueur.

Les deux organisateurs soulignent, par ailleurs, que cette initiative «constitue également un premier pas vers une coopération plus étroite entre la CNDP et le Conseil national de l’ordre des notaires»… [Lire la suite]

Réagissez à cet article

Source : *:: Le Matin :: Les notaires sensibilisés à la protection des données personnelles*

Qu’est ce que le principe d’« Accountability » dans le Règlement Européen de Protection des Données Personnelles ?

Qu’est ce que le principe d’« Accountability » dans le Règlement Européen de Protection des Données Personnelles ?

Le principe d'«Accountability » n'est pas nouveau dans le domaine de la protection des données et de la vie privée. Plusieurs textes y ont déjà fait référence et notamment les lignes directrices émises par l'OCDE en 1980, le Standard de la conférence Internationale de Madrid, la norme ISO 29100 ou les règles mises en place au sein de l'APEC. Au sein même de la directive 95/46, le possible recours aux règles internes de groupe pour encadrer les transferts de données en dehors de l'Union Européenne, reflètent cette notion qui vise à responsabiliser le responsable de traitement.

Comment définir le principe d'«Accountability » ?

Ce terme est difficile à traduire en français. Cela revient à montrer comment le principe de responsabilité est mis en œuvre et à le rendre vérifiable. Il est souvent traduit en français par l'« obligation de rendre compte ».
Pour le G29[1] , cela doit s'entendre comme des « mesures qui devraient être prises ou fournies pour assurer la conformité en matière de protection des données ».

Le principe d'«Accountability » dans le Règlement Général de Protection des Données

La traduction française du texte, à savoir « le principe de responsabilité », ne reflète pas toute la signification de ce terme. C'est en lisant le détail des dispositions du règlement, que l'on en saisit la portée.
– Le responsable du traitement est responsable du respect des principes (i.e.de la licéité, de la loyauté, de la transparence des traitements, du respect du principe de finalités, de minimisation des données, de l'exactitude des données, du respect de la durée de conservation et des mesures de sécurité) ;
– Et il est en mesure de démontrer que ces dispositions sont respectées. A cet effet, l'article 22 du Règlement précise que le responsable du traitement met en œuvre des mesures techniques et organisationnelles appropriées. Lorsque cela est proportionné aux activités de traitement de données, les mesures comprennent la mise en œuvre de politiques appropriées.
– Comme dans tout processus d'amélioration continue, ces mesures doivent être réexaminées et actualisées si nécessaire.

Qui est soumis au principe d'« Accountability » ?

Selon les dispositions de l'article 5 du règlement européen, ce principe concerne le responsable de traitement.
Les sous-traitants auront eux aussi des responsabilités portant sur la mise en œuvre de mesures ou sur la documentation des traitements ; mais si le vocabulaire utilisé dans le texte du règlement est souvent similaire, il ne semble pas que l'on puisse en déduire que les sous-traitants seront soumis au respect du principe d'« Accountability ».
Il en va probablement différemment du représentant qui agit pour le compte et au nom du responsable de traitement établi en dehors de l'Union Européenne et qui de ce fait, doit remplir les obligations qui lui incombent.

De quelles mesures technique et organisationnelles s'agit-il ?

Ces mesures doivent être prise en tenant compte de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques pour les droits et libertés des personnes.
Le G29 précise que la mise en pratique du principe d' « Accountability » suppose une analyse au « cas par cas ».
L'article 23 du Règlement relatif à la protection des données dès la conception et par défaut, précise que le responsable de traitement met en œuvre des mesures techniques et organisationnelles appropriées, telles que la pseudonymisation, destinées à donner effet aux principes de protection des données et notamment à la minimisation.
Il est par ailleurs indiqué à l'article 28 du Règlement, que chaque responsable du traitement tient un registre décrivant les traitements et dans la mesure du possible, les mesures de sécurité techniques et organisationnelles mise en place.
Selon l'article 30 du Règlement européen, le responsable de traitement est tenu de prendre des mesures de sécurité et notamment selon les besoins :
– la pseudonymisation et le cryptage des données à caractère personnel ;
– des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement des données ;
– des moyens permettant de rétablir la disponibilité des données et l'accès à celles-ci (…) en cas d'incident ;
– une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures de sécurité.

Les mesures indiquées dans le Règlement Européen font écho à celles citées en exemple par le G29 à l'occasion de son avis[2] émis sur l'« Accountability »:
– Des politiques et procédures internes permettant de garantir le respect des principes de protection des données (notamment lors de la création ou la modification d'un traitement),
– L'inventaire des traitements,
– La répartition des rôles et responsabilités,
– La sensibilisation et formation du personnel,
– La désignation d'un délégué à la protection des données,
– La vérification de l'efficacité des mesures (contrôles, audits).

Lors de la 31ème Conférence des Commissaires à la Protection des Données et à la Vie Privée de Madrid, le principe d'«Accountability » avait été illustré de la manière suivante:
– Implémentation de procédures destinées à prévenir et détecter les failles,
– La désignation d'un ou de plusieurs délégués à la protection des données,
– Des sessions de sensibilisation et de formation régulières,
– La conduite régulière d'audits indépendants,
– La prise en compte de la réglementation au travers de spécificités techniques,
– La mise en place d'études d'impacts sur la vie privée,
– L'adoption de codes de conduite.
Le G29 a également indiqué que la transparence sur les politiques de confidentialité et sur la gestion interne des plaintes contribuait à un meilleur niveau d'« Accountability ».

Le rôle de la certification

Le Règlement européen précise que l'application d'un code de conduite approuvé ou d'un mécanisme de certification approuvé peut servir à attester du respect des obligations incombant au responsable du traitement au titre de l' « Accountability ».
De manière générale, les actes délégués de la Commission devraient fournir de plus amples informations sur le sujet.

Le principe d'« Accountability » : une évolution plus qu'une révolution

L'« Accountability » n'est pas une révolution dans la mesure où les organisations ont déjà l'obligation de se conformer aux principes de protection des données et notamment à la loi Informatique et Libertés en France. Ce principe est d'ailleurs déjà connu des acteurs du secteur financier.
L'obligation de documentation à des fins de démonstration est en revanche plus novatrice et ce d'autant plus que les entreprises connaissent mal l'étendue de cette réglementation.
Ainsi en cas de violation des principes de protection des données, les autorités de protection des données devraient prendre en considération l'implémentation (ou pas) de mesures et l'existence de procédures de contrôle.
De plus, si les informations relatives aux procédures et politiques ne peuvent être fournies, les autorités de protection des données pourront sanctionner une organisation sur la base de ce seul manquement, indépendamment du fait qu'il y ait eu une violation des données.
Comme l'a indiqué le groupe de travail des autorités européennes de protection des données (G29), les personnes ayant des connaissances techniques et juridiques pointues en matière de protection des données, capables de communiquer, de former le personnel, de mettre en place des politiques et de les auditer seront indispensables à la protection des données.
[1] Opinion 3/2010 on the principle of accountability
[2] http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp173_en.pdf
… [Lire la suite]

Réagissez à cet article

Source : *Règlement Européen de Protection des Données Personnelles : Le principe d'« Accountability » ou comment passer de la théorie à la pratique – CIL Consulting*

Évolution du « Safe Harbor » vers le l' »UE-US Privacy Shield »

Évolution du « Safe Harbor » vers le l' »UE-US Privacy Shield »

La Commission européenne et les États-Unis ont convenu d'un nouveau cadre pour les transferts transatlantiques de données, l' « UE Privacy Shield », en lieu et place du « Safe Harbor ».

Le cadre était attendu depuis l'annulation du Safe Harbor par la Cour de justice de l'UE (CJUE) dans son arrêt du 6 octobre 2015, qui avait créé un vide juridique important en matière de transfert des données (voir notre article).
La Commission européenne et le groupe des CNIL européennes (G29) avaient, d'ailleurs, apporté une première réponse aux inquiétudes des entreprises confirmant que les clauses contractuelles types et les Binding Corporate Rules (BCR) restaient les solutions à privilégier pour assurer la conformité des transferts en cours, durant cette période de transition (voir notre brève).
Ce « bouclier de la confidentialité », présenté le 29 février dernier, aurait donc vocation à protéger les droits fondamentaux des Européens en cas de transfert des données aux États-Unis et à fournir des garanties aux entreprises qui font des affaires transatlantiques.

De nouvelles obligations pour les entreprises américaines
« La collaboration des deux partenaires de part et d'autre de l'Atlantique vise à ce que les données individuelles soient parfaitement protégées, sans renoncer pour autant aux possibilités qu'offre l'ère numérique », a déclaré Andrus Ansip, vice-président de la Commission européenne lors de la présentation publique du Privacy Shield. Et cette protection des données personnelles passerait d'abord par un encadrement des politiques des entreprises américaines en la matière. C'est en tout cas le souhait de la Commission. Le projet de « bouclier » prévoit que les entreprises américaines souhaitant importer des données personnelles provenant d'Europe devront s'engager, dans un code de bonne conduite, à respecter des conditions strictes quant à leurs traitements.
Le dispositif actuel du Privacy Shield prévoit aussi des mécanismes de surveillance afin de garantir le respect de ces obligations par les entreprises. Ces dernières seraient ainsi obligés de rendre public leurs engagements en la matière, qui restent pour le moment à définir, sous peine d'être sanctionnées par la Federal trade commission.
En cas de non-respect de ces engagements les citoyens européens pourraient déposer plainte contre les agissements des entreprises. Elles auront alors 45 jours maximum pour y répondre. Cependant, aucune sanction n'est prévue à ce jour si les délais sont dépassés. Pour que leurs plaintes soient traitées, les citoyens européens pourraient également s'adresser à leur CNIL nationale qui collaborera avec la Federal trade commission. L'instance américaine devra apporter une réponse dans les 90 jours. Enfin pour les cas non résolus, l'accord américano-européen prévoit le recours, en dernier ressort, à un tribunal d'arbitrage devant lequel les entreprises pourront être convoquées. La Commission précise que ce mécanisme de règlement extrajudiciaire des litiges sera accessible sans frais.
La surveillance des services de renseignements plus encadrée
Outre ces mécanismes de surveillance concernant les entreprises, l'exécutif européen a affirmé avoir obtenu de la part des américains un strict encadrement de l'accès des autorités publiques aux données personnelles. « Pour la première fois, le gouvernement américain, par l'intermédiaire des services du directeur du renseignement national, a donné par écrit à l'UE l'assurance que tout accès des pouvoirs publics aux données à des fin de sécurité nationale sera subordonné à des limitations, des conditions et des mécanismes de supervision bien définis, empêchant un accès généralisé aux données personnelles », s'est félicité Bruxelles dans un communiqué. Selon cet engagement pris par les américains, les citoyens européens disposeront d'un recours dans le domaine du renseignement national grâce à un mécanisme de médiation indépendant des services de sécurité nationaux. A ce jour, aucune précision n'a été donné sur les conditions de nomination de ce médiateur ni aucune garantie concrète concernant son indépendance, ce que regrettent les détracteurs de ce texte.
Pour que les limitations de l'accès des pouvoirs publics soient respectés, le Privacy Shield prévoit un mécanisme de réexamen commun aux deux continents. En effet, la Commission européenne et la Federal trade commission, associés à des experts nationaux, pourraient contrôler chaque année le respect des engagements en s'appuyant sur toutes sources d'informations disponibles comme les rapports annuels de transparence des entreprises et ceux d'ONG spécialistes du respect de la vie privée. Côté européen, la Commission adressera un rapport public au Parlement européen et au Conseil, à la suite de ce réexamen.
Ce nouveau cadre international de protection des données doit encore être adopté par le collège des commissaires européens, après l'avis des autorités européennes chargées de la protection des données. En parallèle, les États-Unis vont devoir mettre en place ce nouvel instrument ainsi que les mécanismes de contrôle et de médiation. De nombreuses modifications ont encore le temps d'être apportées, surtout dans le contexte international des élections présidentielles américaines… [Lire la suite]

Réagissez à cet article

Source : *[Direction juridique] L'actualité actuEL DJ : Du « Safe Harbor » à l' »UE-US Privacy Shield »*

Une incroyable bourde de Numericable dénoncée par la CNIL !

Une incroyable bourde de Numericable dénoncée par la CNIL !

Un abonné à Numericable a été suspecté à tort de pédopornographie, subi de multiples perquisitions et harcelé à tort par la Hadopi, parce que l'opérateur renvoyait par erreur son identité aux services de police et de gendarmerie qui l'interrogeaient.
Les faits sont assez graves pour que la CNIL décide de les rendre publics. Le gendarme de la vie privée a révélé mardi que l'opérateur Numericable était directement responsable du harcèlement administratif et judiciaire subi par un abonné, qui a été « *identifié 1 531 fois pour délit de contrefaçon, inculpé 7 fois* », et qui a « *fait l'objet de nombreuses perquisitions à son domicile et de plusieurs saisies de ses équipements informatiques* ».
L'homme n'avait pourtant rien à se reprocher. Mais lorsque Numericable recevait de l'Hadopi, de la police ou de la gendarmerie une demande d'identification d'un abonné à partir de son adresse IP avec date et d'heure d'utilisation, l'opérateur utilisait un logiciel maison, buggé.
« *Lorsque l'application ne parvenait pas à associer une adresse IP à une personne, elle ne générait pas de message d'erreur et renvoyait par défaut à un même abonné* », constate la CNIL. Plus concrètement, le logiciel associait l'adresse IP de la réquisition à l'adresse MAC de son client, unique pour chaque box Numericable. Mais lorsqu'il n'arrivait pas à trouver les informations, le logiciel utilisait alors l'adresse MAC *00:00:00:00:00:00*, attribuée fictivement à plusieurs abonnés. Dont la victime du harcèlement.
Très énervée contre Numericable (mais sans doute moins que le malheureux client), elle note que « *ce problème n'a été identifié qu'avec l'insistance d'un service de police chargé d'une procédure pénale ouverte à l'encontre de l'abonné* ».

1531 DÉNONCIATIONS EN QUATRE MOIS

C'est alertée par l'ancienne présidente de la Hadopi, Marie-Françoise Marais, que la CNIL a décidé d'une mission de contrôle auprès de Numericable, et découvert le pot aux roses. « *Au vu des éléments du dossier, la formation restreinte de la CNIL a considéré que la société NC NUMERICABLE n'avait pas respecté son obligation légale de transmettre des données exactes aux autorités de poursuite, en vertu de l'article 6-4° de la loi Informatique et Libertés* », rapporte l'autorité administrative.

Selon le texte de la délibération (.pdf), le nom de l'abonné persécuté a été communiqué à 1531 reprises entre le 26 janvier et le 15 avril 2013, c'est-à-dire en l'espace de moins de quatre mois. Y compris, ce qui est plus que fâcheux, dans des affaires de pédophilie. C'est lorsque l'Hadopi a tranmis le dossier de l'abonné ultra-multi-récidiviste à la justice que le parquet a constaté qu'il y avait visiblement un petit problème.
Le contrôle de la CNIL n'est toutefois intervenu que deux ans plus tard, le 15 avril 2015. Des contrôles complémentaires sur pièces ont été réalisés jusqu'à fin septembre 2015.
Le problème aurait été corrigé par Numericable en 2014, à la suite d'une demande d'information adressée par un service de police le 26 septembre 2014. L'opérateur a reconnu les faits, et échappé à une sanction financière en raison de sa promptitude à modifier le logiciel lorsqu'elle a eu connaissance de l'origine du problème. La CNIL a toutefois décidé d'adresser un avertissement public, en guise de peine infamante, devant appeler tous les opérateurs à la vigilance.
L'histoire ne dit pas si l'abonné en cause a porté plainte pour réparation du préjudice subi… [Lire la suite]

Réagissez à cet article

Source : *Une incroyable bourde de Numericable dénoncée par la CNIL ! – Politique – Numerama*

Un dispositif de vote électronique doit-il être

déclaré à la CNIL ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer

Un dispositif de vote électronique, notamment pour l'organisation d'élections primaires, doit être déclaré à la CNIL et répondre aux recommandations n° 2010-371 formulées par la Commission.

[block id="24761" title="Pied de page HAUT"]

A Lire aussi :

Nouveautés dans l'organisation des votes électroniques pour les élections professionnelles

3 points à retenir pour vos élections par Vote électronique

Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique

Modalités de recours au vote électronique pour les Entreprises

L'Expert Informatique obligatoire pour valider les systèmes de vote électronique

Dispositif de vote électronique : que faire ?

La CNIL sanctionne un employeur pour défaut de sécurité du vote électronique pendant une élection professionnelle

Notre sélection d'articles sur le vote électronique

Vous souhaitez organiser des élections par voie électronique ? Cliquez ici pour une demande de chiffrage d'Expertise

Vos expertises seront réalisées par **Denis JACOPINI** :

• Expert en Informatique **assermenté et indépendant** ;

• **spécialisé dans la sécurité** (diplômé en cybercriminalité et certifié en Analyse de risques sur les Systèmes d'Information « ISO 27005 Risk Manager ») ;

• ayant suivi la **formation délivrée par la CNIL sur le vote électronique** ;

• qui n'a **aucun accord ni intérêt financier** avec les sociétés qui créent des solution de vote électronique ;

• et possède une expérience dans l'analyse de nombreux systèmes de vote de prestataires différents.

Denis JACOPINI ainsi **respecte l'ensemble des conditions recommandées** dans la Délibération de la CNIL n° 2019-053 du 25 avril 2019 portant adoption d'une recommandation relative à la sécurité des systèmes de vote par correspondance électronique, notamment via Internet.

Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses rapport d'expertises, d'une rigueur dans ses audits et d'une impartialité et neutralité dans ses positions vis à vis des solutions de votes électroniques.

Correspondant Informatique et Libertés jusqu'en mai 2018 et depuis Délégué à La Protection des Données, nous pouvons également vous accompagner dans vos démarches de mise en conformité avec le RGPD (Règlement Général sur la Protection des Données).

Contactez-nous

Source : *CNIL Besoin d'aide ? – Vote électronique : le dispositif doit-il être déclaré à la CNIL ?*

Moyens pour les entreprises de (re)gagner la confiance des clients

Moyens pour les entreprises de (re)gagner la confiance des clients

Chaque citoyen a un rôle à jouer au niveau de la sécurité. La connaissance des fonctionnalités de sécurité, la sauvegarde de nos données et le maintien à jour des logiciels de sécurité, des systèmes d'exploitation, applications et navigateurs Internet, ne sont que quelques-unes des précautions que chacun devrait prendre sur tous ses appareils.

Lorsque ces bases ne sont pas respectées, ou si nous téléchargeons et communiquons des informations personnelles via la dernière application incontournable sans être sûrs de sa source, nous prenons simplement un énorme risque avec nos propres informations. Bien que de plus en plus de particuliers prennent conscience de ce qu'ils doivent faire pour sécuriser leurs données, comment pouvons-nous être sûrs que ces dernières sont traitées correctement lorsqu'elles sont communiquées à des entreprises? Afin de regagner la confiance de leurs clients et de l'opinion publique, les entreprises doivent travailler sur plusieurs points.

• Assurer la transparence et la confidentialité des données constamment ;
• Contrôler et chiffrer les données où qu'elles soient, stockées ou en transit;
• #GDPR : Investir pour respecter la conformité**GDPR :** (GDPR #General Data Protection Regulation / #Projet de règlement européen sur la protection des données personnelles)

Réagissez à cet article

Source : *Données personnelles: 3 moyens pour les entreprises de (re)gagner la confiance des clients | FrenchWeb.fr*

Projet de règlement européen relatif à la protection des données personnelles (en anglais GDPR General Data Protection Regulation)

Projet de règlement européen relatif à la protection des données personnelles (en anglais #GDPR #General Data Protection Regulation)

1/ Qu'est-ce que le GDPR ?
Il s'agit de l'acronyme anglais d'un nouveau règlement européen modifiant le cadre juridique relatif à la protection des données personnelles au sein de l'union européenne, effectif début 2015. Il impactera toutes les entreprises collectant, gérant, ou stockant des données et aura pour but principal de simplifier et harmoniser la protection des données dans les 28 pays de l'union européenne. En cas de non respect du règlement par les entreprises, des amendes allant jusqu'à 20 millions d'euros ou 4% du chiffre d'affaire mondial seront applicables.
L'objectif du GDPR est de faire face aux nouvelles réalités du marché, notamment en matière de protection des données liée aux réseaux sociaux ou encore au cloud computing, Les notions de transferts de fichiers sécurisés et de droit à l'oubli font également parti du GDPR.
Le développement des clouds privés, publics, ou encore de solutions hybrides a compliqué le stockage et le traitement des données au cours de ces dernières années. Le GDPR clarifiera les responsabilités de chaque entreprise en contact avec les données, facilitant ainsi la mise en conformité.

2/ Actuellement, comment les organisations gèrent-elles les impératifs de protection des données ? Existe-t-il des différences en fonction des pays ?
Chaque pays détient sa propre autorité de protection des données pour le moment. Puisque le GDPR est un règlement et non une directive, il s'appliquera directement à tous les pays de l'UE sans avoir besoin de changer les législations nationales.
Le GDPR aura un impact significatif sur les compagnies non-européennes opérant sur le sol européen, puisqu'il s'appliquera aussi bien aux compagnies européennes qu'aux non-européennes commerçant dans l'UE, reflétant ainsi la réalité actuelle : le business est sans frontière.

3/ Quel sera l'impact sur les entreprises ?
Les entreprises devront repenser la manière dont elles collectent, traitent et stockent les données.Il sera obligatoire de tenir à disposition des internautes dont les données sont stockées un texte clair expliquant la politique de sécurisation des données. Les entreprises devront également pouvoir leur fournir toutes leurs données personnelles dans un format simple et transférable via internet. Bien sur le droit à l'oubli devra également rendre possible la suppression rapide de toutes les données. Cette partie du règlement influence déjà certaines sociétés, comme Facebook et Google qui se préparent peu à peu au GDPR.

4/ Les entreprises sont elles prêtes pour la mise en place de ce règlement ?
Il semble que peu d'entreprises soient prêtes. Selon un sondage Ipswitch réalisé fin 2014 sur 316 entreprises européennes, 52% des sondés ont répondu ne pas être prêts. Plus grave encore 56% ne savaient pas exactement à quoi correspond le sigle GDPR.
Par ailleurs, 64 % des personnes interrogées ont reconnu n'avoir aucune idée de la date d'entrée en vigueur supposée de ce règlement. Seules 14 % des personnes interrogées ont pu indiquer clairement que le GDPR est censé entrer en vigueur début 2015.Autre point préoccupant : 79% des sondés font appel à un fournisseur cloud, mais seulement 6% ont pensé à demander à leur prestataire s'il était en règle avec le règlement européen.

5/ Que peuvent faire les entreprises pour s'assurer qu'elles sont en conformité avec le GDPR ?
Plusieurs mesures peuvent être prises pour s'assurer de la conformité de sa structure informatique. Les contrats avec tous les prestataires informatiques, notamment les fournisseurs de services cloud, doivent être passer en revue. Il faut s'assurer que, pour chaque information collectée, une demande de consentement soit effectuée et enfin il est nécessaire de savoir précisément où les données sont stockées.Une fois les processus en règle, l'entreprise pourra demander un certificat européen, valable 5 ans, attestant sa conformité au GDPR.* Enquête en ligne réalisée en octobre 2014 par Ipswitch, à laquelle ont répondu 316 professionnels de l'informatique (104 du Royaume-Uni, 101 de France et 111 d'Allemagne).

Réagissez à cet article

Source : *Projet de règlement européen (en anglais GDPR General Data Protection Regulation) – Fil d'actualité du Service Informatique et libertés du CNRS*

La CNIL lance un ultimatum à Facebook au sujet des cookies et des transferts de données

La CNIL lance un ultimatum à Facebook au sujet des cookies et des transferts de données

La Commission Nationale de l'Informatique et des Libertés a publiquement mis en demeure Facebook de ne plus placer de cookies indésirables sur les postes des utilisateurs et d'arrêter le transfert des données personnelles de ses membres vers les Etats-Unis.

Le géant des réseaux sociaux a 3 mois pour se conformer à cette décision sous peine de sanction. La Commission Nationale de l'Informatique et des Libertés (CNIL) a ordonné à Facebook de stopper le transfert de certaines données personnelles de ses utilisateurs vers les Etats-Unis et de changer la façon dont elle récolte leurs données lorsqu'ils visitent son site web.
Dans sa mise en demeure, rendue publique lundi en fin de journée, la CNIL reproche ainsi à Facebook de transférer les données de ses membres aux Etats-Unis sur la base du Safe Harbor « ce qui n'est plus possible depuis la décision de la Cour de Justice de l'Union Européenne du 6 octobre 2015 », rappelle la commission.
La liste des griefs ne s'arrête pas là : « Le site dépose sur l'ordinateur des internautes des cookies à finalité publicitaire, sans les en avoir au préalable correctement informés ni avoir recueilli leur consentement », indique la CNIL.
Autre constat et non des moindres : « La CNIL a constaté que le site Facebook est en mesure de suivre la navigation des internautes, à leur insu, sur des sites tiers alors même qu'ils ne disposent pas de compte Facebook. En effet, le site dépose un cookie sur le terminal de chaque internaute qui visite une page Facebook publique, sans l'en informer. »… [Lire la suite]

Réagissez à cet article

Source : *La CNIL lance un ultimatum à Facebook au sujet des*

cookies et des transferts de données – Le Monde Informatique