RGPG Règlement européen sur la protection des données : priorité au chiffrement, à l’authentification et aux contrôles d’accès

	RGPD Règlement européen sur la protection des données : priorité au chiffrement, à l’authentification et aux contrôles d’accès

Philippe Carrère, directeur de la protection des données et de l'identité, Europe du Sud chez Gemalto revient sur le nouveau règlement européen sur la protection des données personnelles et ce qu'il implique pour les entreprises en termes de stratégie de sécurité et de relation client.

L'adoption récente du règlement européen sur la protection des données personnelles constitue un tournant pour les entreprises implantées dans l'Union Européenne. En effet, il exige des gestionnaires d'infrastructures et des fournisseurs de services numériques – tels qu'Amazon ou Google – de faire part d'éventuels vols de données et de mettre en place des mesures de sécurité adéquates. Les chefs d'entreprises devraient y voir là un avertissement et commencer dès à présent à évaluer leurs politiques de sécurité, avant que la proposition de loi ne soit approuvée par le Parlement et le Conseil européen.
Où en sont les entreprises européennes en termes de sécurité des données et quelles mesures doivent-elles prendre afin d'être conformes ? A l'heure actuelle, les pare-feu, les antivirus, le filtrage de contenu et la détection des menaces sont les principaux outils utilisés pour se prémunir des vols de données. Ces mesures sont, cependant, insuffisantes, les hackers pouvant franchir aisément ce premier périmètre de sécurité. Dès lors, l'adresse IP des entreprises ou encore les informations de leurs clients peuvent être compromises, comme ce fut le cas avec Volkswagen et la conception de sa Passat.
D'après le Breach Level Index réalisé pour l'année 2015 par Gemalto, plus de 707,5 millions de dossiers clients ont été volés ou perdus à la suite de 1 673 cyberattaques menées de par le monde. Un chiffre qui devrait faire l'effet d'un véritable électrochoc pour les responsables informatiques, d'autant que, fait encore plus inquiétant, 4 % des infractions ont impliqué des données sécurisées (chiffrées partiellement ou en totalité).
Les clients confient des données confidentielles, et ils doivent donc être assurés et convaincus de leur sécurité. Si le lien de confiance avec le client vient à être brisé, il peut être très difficile pour les entreprises de le renouer.
Une de nos récentes études a révélé que plus de la moitié des individus interrogés (57 %) ne traiterait jamais, ou très peu probablement, avec une société ayant perdu des données personnelles suite à une cyberattaque.

Pourquoi ce règlement apparaît aujourd'hui comme une nécessité ?
La sécurité a toujours été un sujet d'actualité, mais suite aux récentes attaques, comme celle de Talk Talk, et le fait que de plus en plus de données personnelles sont collectées en ligne, assurer leur sécurité et maintenir une relation de confiance avec les clients n'a jamais été aussi primordial. A l'heure actuelle, les entreprises européennes ne sont pas tenues de signaler les brèches de données dont elles peuvent faire l'objet, et, de fait, grand nombre d'entre elles ne le font pas. Une fois la nouvelle réglementation en vigueur, elles seront dans l'obligation de révéler ces violations, sous peine de se voir infliger une amende pouvant aller jusqu'à 4 % de leur chiffre d'affaires. C'est pourquoi elles doivent dès à présent opérer un changement de stratégie.
Cependant, il ne s'agit pas là d'un fait nouveau. Cette pratique est déjà en place depuis plusieurs années aux Etats-Unis. C'est pourquoi nous entendons davantage parler des cyberattaques ayant lieu outre-Atlantique que celles se produisant près de chez nous.

Quels sont les principaux enseignements à en tirer ?
Au lieu de se concentrer uniquement sur la protection du périmètre de sécurité, les entreprises devraient plutôt adopter une approche segmentée, protégeant les données à tous les niveaux et barrant le passage aux hackers qui auraient franchi le 1er palier de défense. Cela signifie également que la priorité doit porter sur les données elles-mêmes et sur le fait qu'elles ne puissent être consultées ou utilisées par des personnes non autorisées. Protéger les données par des solutions de chiffrement de bout en bout, d'authentification et des contrôles d'accès permet d'ajouter un niveau de sécurité supplémentaire. En mettant en place des outils de chiffrement, les données subtilisées n'ont plus aucune valeur pour toute personne non autorisée. L'accès peut être sécurisé en utilisant des clés permettant aux personnes habilitées de consulter les informations. Ainsi, en cas d'attaque, les entreprises sont certaines de garantir la sécurité des données de leurs clients.

Informer les clients
Une fois ces mesures sécuritaires mises en place, il est important d'en informer les clients et de les rassurer quant à la pertinence des processus instaurés pour protéger leurs données. Si les entreprises peuvent démontrer qu'elles sont prêtes à se dépasser et à mettre toute leur énergie dans cette démarche, elles seront perçues comme innovantes et dignes de confiance.
La sécurité est un effort mutuel. S'il est important d'informer les clients sur le travail qui est fait pour assurer leur sécurité, il est tout aussi primordial qu'ils sachent comment se protéger eux-mêmes. De plus, s'adresser à un utilisateur averti permettra de lui proposer un meilleur service client.
L'adoption du nouveau règlement européen sur la protection des données donne aux entreprises la possibilité de prendre les devants et montrer dès à présent à leurs clients qu'elles prennent ce sujet très au sérieux. Elles ne doivent pas seulement se soucier d'être conformes ou pas, mais comprendre qu'il s'agit là d'une nécessité essentielle à leur réussite. Les utilisateurs sont de plus en plus conscients qu'ils confient des données sensibles aux entreprises, leur demandant, de fait, d'en être responsables. La montée en puissance de cette prise de conscience doit aller de pair avec un niveau d'exigence plus élevé vis-à-vis des structures hébergeant ces informations. Ne pas prendre ce sujet au sérieux pourrait non seulement être préjudiciable en cas d'attaque, mais également nuire à la confiance instaurée avec les clients. Perdre ce lien les incitera à se tourner vers des concurrents jugés plus fiables… [Lire la suite]

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertises techniques (virus, espions, piratages, fraudes, arnaques Internet...) et judiciaires (investigations téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE
Consultant en Cybercriminalité et en Protection des Données Personnelles

Contactez-nous

Réagissez à cet article

Source : *Nouveau règlement européen sur la protection des données : priorité au chiffrement, à l'authentification et aux contrôles d'accès | Solutions Numériques*

Combien vous coûterait le piratage de vos données ?

	**Combien vous coûterait le piratage de vos données ?**

Un consommateur français sur trois reconnaît que sa loyauté envers une marque diminue après qu'une attaque informatique a porté atteinte aux données qu'il lui avait confié.

Souvent préparées de longues dates, les attaques informatiques qui frappent les entreprises laissent des traces longtemps après.
Publiée aujourd'hui, une étude internationale menée par Vanson Bourne, pour l'éditeur de logiciels de cybersécurité FireEye, souligne que les conséquences de tels épisodes entament la performance commerciale de la société victime, au-delà des dégâts informatiques des premiers jours. « *La sécurité des systèmes d'information a un réel impact sur la confiance des consommateurs* », affirme Yogi Chandiramani, directeur des ventes en Europe pour FireEye.
« *En France, l'attaque qui a touché TV5 Monde en avril 2015 et les vols de données chez Orange en 2014 ont particulièrement marqué les esprits* », poursuit-il. 34 % des consommateurs français reconnaissent que leur loyauté en tant que client actuel ou potentiel d'une marque diminue après qu'une entreprise a laissé fuiter des données, pointe le questionnaire en ligne envoyé à 1.000 d'entre eux. Un argument de plus pour ceux qui voient les efforts de cyber-sécurité comme un argument de compétitivité .
L'atteinte à leurs données personnelles refroidit particulièrement les ardeurs à l'achat des consommateurs. Quand le vol de données est connu, plus de trois Français sur quatre déclarent qu'ils stopperaient leurs emplettes de produits ou services fournis par la victime, surtout si la faute vient de l'équipe dirigeante – ils sont plus conciliants s'il s'agit de l'erreur humaine d'un subordonné. La tendance se confirme au fil des années. D'après l'étude, 61 % des Français déclarent avoir pris en considération la sécurité de leurs données lors de leurs achats en 2015. Ils n'étaient que 53% dans cet état d'esprit en 2014…

Après une cyber-attaque, la transparence prime

A cette perte de chiffre d'affaires potentiel s'ajoute le risque de poursuite en justice. La moitié des Français déclarent qu'ils engageraient des poursuites contre l'entreprise cyber-attaquée qui n'a pas su protéger leurs données personnelles, volées ou utilisées à des fins criminelles. Aux Etats-Unis, Target et Sony Picture s ont été attaqués en Justice par des procédures de class action, le premier par ses clients, le second par ses salariés.
Dès lors, la tentation peut être grande pour une entreprise de garder secret le fait que son système d'information ait été vulnérable à des cyber-criminels. Ce serait pourtant aggraver le mal qui surviendra au moment où, inévitablement à l'heure d'Internet, l'information ressortira.
« *Les consommateurs pointent les négligences des entreprises mais attendent surtout d'elles de la transparence, 93 % d'entre eux souhaitent être prévenus dans les 24h quand leurs données sont exposées* », prévient Yogi Chandiramani.

Des changements dans quelques mois ?

Le règlement européen sur la protection des données, qui devrait s'appliquer en France d'ici 2018, prévoit d'imposer aux sociétés de notifier les autorités, voir leurs clients, de toutes atteintes sur les données personnelles des citoyens européens dans les 72h après la découverte du problème.
A noter :
L'attaque particulièrement destructrice qui a touché TV5Monde en 2015 devrait coûter près de 10 millions d'euros sur trois ans, uniquement en réparation informatique… [Lire la suite]

Réagissez à cet article

Source : *Cyber-attaque : les coûts d'après, Cybersécurité – Les Echos Business*

Fuite, perte, piratage de données ? Entreprise, il va falloir communiquer ! – Data Security BreachData Security Breach

CNIL. Commission Nationale de l'Informatique et des Libertés	Fuite, perte, piratage de données ? Entreprise, il va falloir communiquer !

La directive européenne de protection des données personnelles est morte ! Vive le règlement général sur la protection des données (GDPR). Fuite, perte, piratage de données ? Entreprise, il va falloir communiquer !

En 1995, l'Europe s'équipait de la directive européenne de protection des données personnelles. Mission, protéger les informations des utilisateurs d'informatique. 21 ans plus tard, voici venir le règlement général sur la protection des données (GDPR). La Commission européenne avait proposé en 2012 un nouveau règlement portant sur un ensemble de règles unique pour toutes les données collectées en ligne afin de garantir qu'elles soient conservées de manière sûre et de fournir aux entreprises un cadre clair sur la façon dont les traiter.

Mercredi 13 avril 2016, le paquet législatif a été formellement approuvé par le Parlement dans son ensemble. Le GDPR impose aux entreprises (petites ou grandes) détenant des données à caractère personnel d'alerter les personnes touchées par une fuite, une perte, un piratage de la dire informations privée.

Grand groupe, PME, TPE doivent informer les autorités de contrôle nationales (CNIL) en cas de violation importante de ces données.
Comme je pouvais déjà vous en parler en 2014, il faut alerter les autorités dans les 72 heures après avoir découvert le problème. Les entreprises risquent une grosse amende en cas de non respect : jusqu'à 4% de son chiffre d'affaire. Les informations que nous fournissons doivent être protégées par défaut (Art. 19). A noter que cette régle est déjà applicable en France, il suffit de lire le règlement de la CNIL à ce sujet. Faut-il maintenant que tout cela soit véritablement appliqué.

Fuite, perte, piratage de données
Parmi les autres articles, le « 7 » indique que les entreprises ont l'obligation de demander l'accord « *clair et explicite* » avant tout traitement de données personnelles. Adieu la case par défaut imposée, en bas de page. De l'opt-in (consentement préalable clair et précis) uniquement. Plus compliqué à mettre en place, l'article 8. Je le vois dans les ateliers que je mets en place pour les écoles primaires et collèges. Les parents devront donner leur autorisation pour toutes inscriptions et collectes de données. Comme indiqué plus haut, les informations que nous allons fournir devront être protégées par défaut (Art. 19). Intéressant à suivre aussi, l'article 20. Comme pour sa ligne téléphonique, le numéro peut dorénavant vous suivre si vous changez d'opérateur, cet article annonce un droit à la portabilité des données. Bilan, si vous changez de Fournisseur d'Accès à Internet par exemple, mails et contacts doivent pouvoir vous suivre. L'histoire ne dit pas si on va pouvoir, du coup, garder son adresse mail. 92829@orange.fr fonctionnera-t-il si je passe chez Free ?
La limitation du profilage par algorithmes n'a pas été oublié. En gros, votre box TV Canal +, Orange ou Netflix (pour ne citer que le plus simple) utilisent des algorithmes pour vous fournir ce qu'ils considèrent comme les films, séries, émissions qui vous conviennent le mieux. L'article 21 annonce que l'algorithme seul ne sera plus toléré, surtout si l'utilisateur n'a pas donné son accord.
Enfin, notre vie numérique est prise en compte. Les articles 33 et 34 s'annoncent comme les défenseurs de notre identité numérique, mais aussi notre réputation numérique. L'affaire Ashley Madisson est un des exemples. Votre identité numérique est volée. L'entreprise ne le dit pas. Votre identité numérique est diffusée sur Internet. Vous ne la maîtrisez plus.
Bref, 33 et 34 annonce clairement que les internautes ont le droit d'être informé en cas de piratage des données. La CNIL sera le récipiendaire des alertes communiquées par les entreprises piratées. Bref, fuite, perte, piratage de données ? Entreprise, il va falloir communiquer !
Les entreprises ont jusqu'au 1er janvier 2018 pour se mettre en conformité. Les 28 pays membres doivent maintenant harmoniser leurs lois sur le sujet. Je me tiens à la disposition des entreprises, associations, particuliers qui souhaiteraient réfléchir à leur hygiène informatique.

Police : nouvelles règles sur les transferts de données
Le paquet sur la protection des données inclut par ailleurs une directive relative aux transferts de données à des fins policières et judiciaires. La directive s'appliquera aux transferts de données à travers les frontières de l'UE et fixera, pour la première fois, des normes minimales pour le traitement des données à des fins policières au sein de chaque État membre.
Les nouvelles règles ont pour but de protéger les individus, qu'il s'agisse de la victime, du criminel ou du témoin, en prévoyant des droits et limites clairs en matière de transferts de données à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales – incluant des garanties et des mesures de prévention contre les menaces à la sécurité publique, tout en facilitant une coopération plus aisée et plus efficace entre les autorités répressives.

« ***Le principal problème concernant les attentats terroristes et d'autres crimes transnationaux est que les autorités répressives des États membres sont réticentes à échanger des informations précieuses*** », a affirmé Marju Lauristin (S&D, ET), députée responsable du dossier au Parlement.
« ***En fixant des normes européennes sur l'échange d'informations entre les autorités répressives, la directive sur la protection des données deviendra un instrument puissant et utile pour aider les autorités à transférer facilement et efficacement des données à caractère personnel tout en respectant le droit fondamental à la vie privée*** « , a-t-elle conclu… [Lire la suite]

Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles.

- Expertise techniques et judiciaire en litige commercial, piratages, arnaques Internet;
- Expertise de systèmes de vote électronique;
- Formation en cybercriminalité;
- Formation de C.I.L. (Correspondants Informatique et Libertés);
- Accompagnement à la mise en conformité CNIL de votre établissement.

Contactez-nous

Suivez nous sur

Réagissez à cet article

Source : *Fuite, perte, piratage de données ? Entreprise, il va falloir communiquer ! – Data Security BreachData Security Breach*

Avant le règlement européen sur les données personnelles, la Loi pour la République Numérique

Avant le règlement européen sur les données personnelles, la Loi pour la République Numérique

Le nouveau règlement européen relatif à la protection des données personnelles (GDPR) fait grand bruit en Europe. Il donne, en effet, plus de droits aux consommateurs sur la façon dont leurs données sont traitées et requiert des contrôles complémentaires (et des informations) sur quiconque dispose de données personnelles dans l'Union européenne.

Comme toutes les lois, celle-ci a été largement discutée, avec des points de vue contradictoires, mais une chose a été acceptée par tous : les entreprises auront deux ans, à compter de la date de publication de la loi (en juin 2016), avant que celle-ci entre en vigueur. Deux années indispensables aux entreprises pour leur permettre de mettre en place les politiques, les processus et les technologies nécessaires pour être en conformité avec le règlement.
En avance sur ses voisins européens, la France a d'ores et déjà adopté un projet de loi en phase avec les principes fondamentaux du règlement européen relatif à la protection des données personnelles. Ainsi, le projet de loi pour une République numérique, validé par l'Assemblée nationale le 26 janvier dernier (actuellement examiné par le Sénat), devrait être approuvé pour entrer en vigueur cette année.

Quelles sont les grandes lignes de la loi pour la République numérique ?

Droit à la portabilité des données : le consommateur peut demander à ce que ses données soient conservées par le responsable du traitement des données et dispose en toutes circonstances d'un droit de récupération de ses données.
• Conservation des données : le responsable du traitement des données doit informer le consommateur de la durée pendant laquelle les données sont conservées.
• Droit de rectification : les consommateurs peuvent demander à ce que leurs données soient éditées pour les modifier.
• Droit à la suppression : les personnes concernées peuvent demander à ce que leurs données soient supprimées ou interdire l'usage de leurs données.
• Recours collectifs : les consommateurs peuvent déposer une plainte collective pour demander réparation lors de la perte ou de l'utilisation abusive de leurs données.
• Amende maximale : celle-ci peut aller de 150.000 à 20.000.000 euros ou 4 % du chiffre d'affaires global, pour l'amende la plus élevée.
D'autres pays vont-ils prendre exemple sur la France pour faire avancer leurs propres législations sur la protection des données avant la mise en œuvre du règlement européen ? Il y a fort à parier que oui. Et les entreprises ont également anticipé cette nouvelle réglementation puisque l'utilisation de services cloud basés dans la zone européenne a presque doublé en six mois (de 14,3 % au premier trimestre 2015 à 27 % pour 2016)… [Lire la suite]

Réagissez à cet article

Source : *Nouveau règlement européen sur les données personnelles : la France en avance sur ses voisins européens – Global Security Mag Online*

Le Paquet « Protection des données à caractère personnel » adopté

Le Paquet « Protection des données à caractère personnel » adopté

Le règlement général sur la protection des données ainsi que la directive relative à la protection des données à caractère personnel à des fins répressives ont été adopté le 14 avril…

Ce Paquet vise à réformer la législation communautaire d'une part et à remplacer la directive générale sur la protection des données qui datait de 1995 d'autre part.

1. Les nouveaux principes à mettre en oeuvre par le règlement

Le règlement européen sur la sur la protection des données (2) consacre de nouveaux concepts et impose aux entreprises de « disrupter » leurs pratiques et de revoir leur politique de conformité Informatique et libertés.
Si les formalités administratives sont simplifiées pour mettre en œuvre un traitement, les obligations sont en revanche renforcées pour assurer une meilleure protection des données personnelles :

• la démarche de « Privacy by design » (respect de la protection des données dès la conception) (Règlement, art. 25 §1) ;
• la démarche de « Security by default » (sécurité par défaut) (Règlement, art. 25 §2) ;
• les règles d'accountability (obligation de documentation) (Règlement, art. 24) ;
• l'étude d'impact avant la mise en œuvre de certains traitements (Règlement, art. 35) ;
• la désignation obligatoire d'un Data Protection Officer (DPO) (Règlement, art. 37) ;
• les nouveaux droits fondamentaux des personnes (droit à l'oubli, droit à la portabilité des données, etc.) sur lesquels nous reviendrons dans un prochain article.

1.1 Le respect de la protection des données dès la conception ou « Privacy by design »

Le règlement européen sur la protection des données consacre le principe de « Privacy by design » qui impose aux entreprises publiques comme privées de prendre en compte des exigences relatives à la protection des données dès la conception des produits, services et systèmes exploitant des données à caractère personnel.
Cette obligation requiert que la protection des données soit intégrée par la Direction des systèmes d'information dès la conception d'un projet informatique, selon une démarche « Privacy by design ». Elle rend également nécessaire la coopération entre les services juridiques et informatiques au sein des entreprises
.

1.2 La sécurité par défaut ou « Security by default »

Le règlement européen sur la protection des données pose une nouvelle règle, la « sécurité par défaut ». Cette règle impose à tout organisme de disposer d'un système d'information ayant les fonctionnalités minimales requises en matière de sécurité à toutes les étapes (enregistrement, exploitation, administration, intégrité et mise à jour).
La sécurité du système d'information doit être assurée dans tous ses éléments, physiques ou logiques (contrôle d'accès, prévention contre les failles de sécurité, etc.).
Par ailleurs, cette règle implique que l'état de la sécurité du système d'information puisse être connu à tout moment, par rapport aux spécifications du fabricant, aux aspects vulnérables du système et aux mises à jour.

1.3 L'étude d'impact

Le règlement européen sur la protection des données consacre l'obligation par les organismes de réaliser des analyses d'impact relatives à la protection des données.
Cette obligation impose à tous les responsables de traitements et aux sous-traitants d'effectuer une analyse d'impact relative à la protection des données personnelles préalablement à la mise en œuvre des traitements présentant des risques particuliers d'atteintes aux droits et libertés individuelles.
Dans un tel cas, le responsable du traitement ou le sous-traitant, doit examiner notamment les dispositions, garanties et mécanismes envisagés pour assurer la protection des données à caractère personnel et apporter la preuve que le règlement sur la protection des données est bien respecté.

1.4 L'obligation de documentation ou « accountability »

Le règlement européen sur la protection des données met à la charge du responsable de traitement des règles d'accountability qui constituent la pierre angulaire de la conformité « ab initio » avec la règlementation en matière de données personnelles.
Il s'agit pour le responsable du traitement de garantir la conformité au règlement en adoptant des règles internes et en mettant en œuvre les mesures appropriées pour garantir, et être à même de démontrer, que le traitement des données à caractère personnel est effectué dans le respect du règlement.
Les mesures prévues en matière de données personnelles et d'accountability vont de la tenue de la documentation, à la mise en œuvre des obligations en matière de sécurité en passant par la réalisation d'une analyse d'impact.
Cette démarche anglo-saxonne connue sous le terme d'accountability est une obligation pour le responsable du traitement de rendre compte et d'expliquer, avec une idée de transparence et de traçabilité permettant d'identifier et de documenter les mesures mises en œuvre pour se conformer aux exigences issues du règlement.
Il devra démontrer qu'il a rempli ses obligations en matière de protection des données. C'est une charge de la preuve qui l'oblige à documenter l'ensemble des actions de sa politique de protection des données de manière à pouvoir démontrer aux autorités de contrôle ou aux personnes concernées comment il s'y tient.

2. La protection des données à caractère personnel traitées à des fins répressives

Les pratiques en matière pénale sont très différentes d'un Etat à l'autre. Jusqu'à présent il n'y avait pas de cadre commun aux services répressifs des Etats membres.
La directive relative à la protection des données à caractère personnel à des fins répressives (3) prévoit que chaque Etat membre doit suivre un cadre commun tout en développant sa propre législation qui devra reprendre toutes les règles de base en matière de protection des données notamment en matière de sécurité.
Ce n'est pas une chose aisée dans la situation actuelle avec les menaces terroristes qui pèsent en Europe.
Parmi les nouveaux éléments importants de cette directive, figure la nécessiter de se préoccuper en permanence de la protection des données et de la vie privée. A ce titre, toutes les institutions liées aux services répressifs devront se doter d'un « Data protection officer ».
Il ne devrait plus y avoir de collecte de données personnelles sans objectif clair, sans durée limitée et les justiciables auront des droits clairs, comme celui de savoir quelles sont les données collectées, à quelle fin, et combien de temps elles seront conservées.
La directive permet de prendre en compte les spécificités liées aux services répressifs tout en préservant les droits universels des citoyens justiciables. Ces deux textes font partis d'un même paquet « protection des données ».
La tâche n'a pas été simple de réformer la directive de 1995 et d'en faire un règlement unifié directement applicable par les Etats membres. C'est probablement une grande première que d'avoir réalisé un tel texte qui s'applique directement à toute l'Union européenne dans un domaine qui règlemente un droit aussi fondamental que la protection des données.
Le règlement entrera en vigueur 20 jours après sa publication au Journal officiel de l'Union européenne. Ses dispositions seront directement applicables dans tous les Etats membres deux ans après cette date, soit en avril 2018.
En ce qui concerne la directive relative à la protection des données à caractère personnel à des fins répressives, les Etats membres auront deux ans pour transposer les dispositions qu'elle contient dans leur droit national.
Il s'agit là d'une grande avancée pour l'Union européenne tant pour les citoyens consommateurs que pour les entreprises.
Notes :
(1) Résolution législative du Parlement européen du 14 avril 2016 sur la position du Conseil en première lecture en vue de l'adoption du règlement général sur la protection des données.
(2) Règlement général sur la protection des données révisé le 8 avril tel qu'adopté par le Parlement européen le 14 avril 2016.
(3) Résolution législative du Parlement européen du 14 avril 2016 sur la position du Conseil en première lecture en vue de l'adoption de la directive relative à la protection des données à caractère personnel à des fins répressives… [Lire la suite]

Réagissez à cet article

Source : *Adoption du Paquet « Protection des données à caractère personnel »*

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 ?*

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*

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*

Fic 2016 : Etude d’impacts sur la vie privée : suivez la méthode de la CNIL

Fic 2016 : Etude d’impacts sur la vie privée : Suivre la méthode de la CNIL

La CNIL publie sa méthode pour mener des PIA (Privacy Impact Assessment) pour aider les responsables de traitements dans leur démarche de mise en conformité et les fournisseurs dans la prise en compte de la vie privée dès la conception de leurs produits.

De l'application de bonnes pratiques de sécurité à une véritable mise en conformité

La Loi informatique et libertés (article 34), impose aux responsables de traitement de « prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données ».
Chaque responsable doit donc identifier les risques engendrés par son traitement avant de déterminer les moyens adéquats pour les réduire.
Pour aider les TPE et PME dans cette étude, la CNIL a publié en 2010 un premier guide sécurité. Celui-ci présente sous forme de fiches thématiques les précautions élémentaires à mettre en place pour améliorer la sécurité d'un traitement des données personnelles.
En juin 2012, la CNIL publiait un autre guide de gestion des risques sur la vie privée pour les traitements complexes ou aux risques élevés. Il aidait les responsables de traitements à avoir une vision objective des risques engendrés par leurs traitements, de manière à choisir les mesures de sécurité nécessaires et suffisantes.

Une méthode plus rapide, plus facile à appliquer et plus outillée

Ce guide a été révisé afin d'être plus en phase avec le projet de règlement européen sur la protection des données et les réflexions du G29 sur l'approche par les risques. Il tient aussi compte des retours d'expérience et des améliorations proposées par différents acteurs.
La CNIL propose ainsi une méthode encore plus efficace, qui se compose de deux guides : la démarche méthodologique et l'outillage (modèles et exemples). Ils sont complétés par le guide des bonnes pratiques pour traiter les risques, déjà publié sur le site web de la CNIL.

Un PIA (Privacy Impact Assessment) ou étude d'impacts sur la vie privée (EIVP) repose sur deux piliers :

les principes et droits fondamentaux, « non négociables », qui sont fixés par la loi et doivent être respectés. Ils ne peuvent faire l'objet d'aucune modulation, quels que soient la nature, la gravité et la vraisemblance des risques encourus ;
la gestion des risques sur la vie privée des personnes concernées, qui permet de déterminer les mesures techniques et d'organisation appropriées pour protéger les données personnelles.
Pour mettre en œuvre ces deux piliers, la démarche comprend 4 étapes :
• Étude du contexte : délimiter et décrire les traitements considérés, leur contexte et leurs enjeux ;
• Étude des mesures : identifier les mesures existantes ou prévues (d'une part pour respecter les exigences légales, d'autre part pour traiter les risques sur la vie privée) ;
• Étude des risques : apprécier les risques liés à la sécurité des données et qui pourraient avoir des impacts sur la vie privée des personnes concernées, afin de vérifier qu'ils sont traités de manière proportionnée ;
• Validation : décider de valider la manière dont il est prévu de respecter les exigences légales et de traiter les risques, ou bien refaire une itération des étapes précédentes.
L'application de cette méthode par les entreprises devrait ainsi leur permettre d'assurer une prise en compte optimale de la protection des données personnelles dans le cadre de leurs activités.

Denis JACOPINI EST FORMATEUR EN ETUDE D'IMPACT SUR LA VIE PRIVÉE

Réagissez à cet article

Source : *Etude d’impacts sur la vie privée : suivez la méthode de la CNIL – CNIL – Commission nationale de l’informatique et des libertés*