

Les documents enregistrés dans un fichier « Mes documents », sont-ils inaccessibles à l'employeur ?

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



Les documents enregistrés dans un fichier « Mes documents », sont-ils inaccessibles à l'employeur ?

Les documents enregistrés dans un fichier « Mes documents », sont-ils inaccessibles à l'employeur ?

« Mes documents » est un terme générique. C'est encore une fois la mention «Personnel» qui permet de protéger un dossier ou un fichier. L'employeur ne peut donc pas en faire état, au risque d'avoir à payer des dommages et intérêts à son salarié. »

Accompagnant depuis 2012 de nombreux établissements, Denis JACOPINI, Expert informatique diplômé en cybercriminalité, certifié en gestion des risques sur les systèmes d'information (ISO 27005) et formé par la CNIL depuis 2011 sur une trentaine de thèmes, est en mesure de vous accompagner dans votre démarche de mise en conformité RGPD.



Besoin d'un expert pour vous mettre en conformité avec le RGPD ?

Contactez-nous

Accompagné de son équipe d'auditeurs et de formateurs, notre Expert, Denis JACOPINI est spécialisé en cybercriminalité et en protection des Données à Caractère Personnel, formateur depuis 1998 et consultant depuis 1996. Avec bientôt une **expérience d'une dizaine d'années** dans la mise en conformité avec la réglementation relative à la Protection des Données à Caractère Personnel, de formation d'abord technique, Correspondant CNIL en 2012 (CIL : Correspondant Informatique et Libertés) puis en 2018 Délégué à la Protection des Données, en tant que praticien de la mise en conformité et formateur, il lui est ainsi aisé d'accompagner les organismes dans leur démarche de **mise en conformité avec le RGPD**.

« Mon objectif, vous assurer une démarche de mise en

conformité validée par la CNIL. ».

Nous vous aidons à vous mettre en conformité avec le RGPD de 2 manières :



Quelques articles sélectionnés par nos Experts :

Comment se mettre en conformité avec le RGPD

Accompagnement à la mise en conformité avec le RGPD de votre établissement

Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

Comment devenir DPO Délégué à la Protection des Données

Des guides gratuits pour vous aider à vous mettre en conformité avec le RGPD et la CNIL

Mise en conformité RGPD : Mode d'emploi

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Réagissez à cet article

Source : *Connaissez-vous vos droits sur les données personnelles au travail (VRAI-FAUX) ? – La Voix du Nord*

RGPD : Concrètement, quelles mesures de sécurité prévoir ?

	RGPD : Concrètement, quelles mesures de sécurité prévoir ?
---	---

La Cnil rappelle les mesures à mettre en œuvre systématiquement sur la sécurité des données

La Commission nationale de l'informatique et des libertés (Cnil) publie un guide rappelant les précautions élémentaires à mettre en œuvre de manière systématique sur la sécurité des données personnelles.

Les 17 mesures de sécurité de base que l'on trouvera dans ce guide sont :

- Sensibiliser les utilisateurs ;
- Authentifier les utilisateurs ;
- Gérer les habilitations ;
- Tracer les accès et gérer les incidents ;
- Sécuriser les postes de travail ;
- Sécuriser l'informatique mobile ;
- Protéger le réseau informatique interne ;
- Sécuriser les serveurs ;
- Sécuriser les sites web ;
- Sauvegarder et prévoir la continuité d'activité ;
- Archiver de manière sécurisée ;
- Encadrer la maintenance et la destruction des données ;
- Gérer la sous-traitance ;
- Sécuriser les échanges avec d'autres organismes ;
- Protéger les locaux ;
- Encadrer les développements informatiques ;
- Chiffrer, garantir l'intégrité ou signer.

Pour information (et rappel pour ceux qui savent), l'article 32 du règlement européen sur la protection des données (RGPD), applicable au 25 mai 2018, prévoit :

1) Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :

- a) la pseudonymisation et le chiffrement des données à caractère personnel;*
- b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;*
- c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;*
- d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.*

2) Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite...

En résumé

Le responsable du traitement et le sous-traitant doivent prendre des mesures afin de garantir que toute personne physique agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne les traite pas, excepté sur instruction du responsable du traitement, à moins d'y être obligée par le droit de l'Union ou le droit d'un État membre.



Besoin d'un **accompagnement pour vous mettre en conformité avec le RGPD** ? ?

Besoin d'une **formation pour apprendre à vous**

mettre en conformité avec le RGPD ?

Contactez-nous

A Lire aussi :

Mise en conformité RGPD : Mode d'emploi

Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles

Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016

Le RGPD, règlement européen de protection des données. Comment devenir DPO ?

Comprendre le Règlement Européen sur les données personnelles en 6 étapes

Notre sélection d'articles sur le RGPD (Règlement Européen sur la Protection des données Personnelles) et les DPO (Délégués à la Protection des Données)

Notre métier : Vous accompagner dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : Formation RGPD : L'essentiel sur le règlement Européen pour la Protection des Données Personnelles



Réagissez à cet article

Source : *La Cnil rappelle les mesures à mettre en œuvre systématiquement sur la sécurité des données* • HOSPIMEDIA

Loi renseignement : une première «boîte noire» activée pour surveiller les communications

<input type="checkbox"/>	Loi renseignement : une première «boîte noire» activée pour surveiller les communications
<input type="checkbox"/>	

Ce dispositif donne aux services de renseignement français un moyen d'analyser automatiquement les métadonnées des communications Internet, notamment pour lutter contre le terrorisme.

De nouvelles oreilles pour le renseignement. Longtemps inactives, les boîtes noires sont désormais en cours de déploiement. Francis Delon, le président de la Commission nationale de contrôle des techniques de renseignement (CNCTR), l'a révélé à l'occasion d'une conférence organisée à Grenoble. Il précise qu'une première boîte noire a été activée «début octobre», à l'issue d'un «travail qui a duré plusieurs mois».

Prévu par l'article 851-3 du Code de la sécurité intérieure, le dispositif a été particulièrement critiqué en amont du vote de la loi renseignement de 2015. Il permet aux services de renseignement d'analyser de grandes quantités de métadonnées (relatives au contexte d'un message, comme son origine ou sa date d'envoi) à la volée, afin de détecter une éventuelle menace terroriste. Francis Delon se veut néanmoins rassurant. «Les données récoltées sont des données de connexion anonymisées, recueillies de façon non ciblée pour être mises dans une sorte de grande marmite étanche», a-t-il résumé, par une métaphore de son cru...[lire la suite]

LE NET EXPERT

:

- **FORMATIONS / SENSIBILISATION :**
 - **CYBERCRIMINALITÉ**
 - **PROTECTION DES DONNÉES PERSONNELLES**
 - **AU RGPD**
 - **À LA FONCTION DE DPO**
- **MISE EN CONFORMITÉ RGPD / CNIL**
 - **ÉTAT DES LIEUX RGPD** de vos traitements)
 - **MISE EN CONFORMITÉ RGPD** de vos traitements
 - **SUIVI** de l'évolution de vos traitements
- **RECHERCHE DE PREUVES** (outils Gendarmerie/Police)
 - **ORDINATEURS (Photos / E-mails / Fichiers)**
 - **TÉLÉPHONES** (récupération de **Photos / SMS**)
 - **SYSTÈMES NUMÉRIQUES**
- **EXPERTISES & AUDITS** (certifié ISO 27005)
 - **TECHNIQUES | JUDICIAIRES | ADMINISTRATIVES**
 - **SÉCURITÉ INFORMATIQUE**
 - **SYSTÈMES DE VOTES ÉLECTRONIQUES**

Besoin d'un Expert ? contactez-nous

Notre Expert, Denis JACOPINI, est assermenté, spécialisé en **Cybercriminalité, Recherche de preuves** et en **Protection des données personnelles**. Diplômé en Cybercriminalité (Droit, Sécurité de l'information & Informatique légale), en Droit de l'Expertise Judiciaire et certifié en gestion des risques en Sécurité des Systèmes d'Information (ISO 27005), Denis JACOPINI est aussi formateur inscrit auprès de la DDRTEFP (Numéro formateur n°93 84 03041 84).



Réagissez à cet article

Source : *Loi renseignement : une première «boîte noire» activée pour surveiller les communications*

Quels sont avantages à se mettre en règle avec le RGPD ?

✕	Quels sont les avantages à se mettre en règle avec le RGPD?
---	--

Avec le Règlement Général sur la Protection des Données (RGPD/GDPR), l'UE se dote d'un cadre réglementaire détaillé pour permettre à ses citoyens de reprendre le contrôle sur leurs données numériques. Pour se mettre en conformité, les entreprises ont un travail titanesque devant elles pour ne pas risquer de lourdes amendes prévues par le texte. Quels avantages peuvent tirer les entreprises de prendre le chemin de la mise en conformité ?

Au fil des conférences que nous animons ou des réunions de sensibilisations auxquelles il nous est demandé d'intervenir, nous remarquons que la grande majorité des décideurs voient d'un très mauvais oeil l'arrivée de ce RGPD (Règlement Général sur la Protection des Données).

Le contexte

A cela, Denis JACOPINI, Expert Informatique spécialisé en protection des données personnelles répond plusieurs choses :

1. Ne pensez-vous pas qu'en tant que consommateur, vous êtes en droit d'avoir l'assurance que le professionnel ou le service public à qui vous confiez vos données personnelles (adresse postale, adresse e-mail, date de naissance, n° de tel portable, numéro de carte bancaire, numéro de sécurité sociale, mot de passe pour accéder à notre compte, historique et remboursement de nos actes médicaux, empreintes digitales, vocales, iriennes, adn, photocopie de pièce d'identité ou de justificatif de domicile...) mettra tous les moyens techniques en oeuvre pour protéger votre vie privée ?

A l'heure de la communication de nos données à la vitesse de la lumière peut encore penser que toutes les données nous concernant, absolument toutes, doivent être libres d'accès ?

Ceux qui ne craignent pas les usages malveillants de ces données ?

A mon avis ce sont ceux qui ne connaissent pas les conséquences d'une usurpation d'identité, d'un vol de numéro de carte bancaire ou d'un vol de mot de passe.

2. Denis JACOPINI vous demande maintenant de vous positionner à la place du responsable de l'établissement public ou privé qui a maintenant la lourde responsabilité de conserver et protéger toutes les informations que lu ont confié des milliers voire des millions de personnes.

Maintenant, n'est-il pas normal de faire le ménage dans votre système de traitement de données et de supprimer ou d'anonymiser les données inutiles ?

Ne pensez-vous pas qu'il est important de mettre à l'abris des regards indiscrets les numéros de cartes bancaires que vous avez récupéré dans votre système informatique ou bien plus couramment sur les tickets de votre TPE ?

Ne pensez-vous pas que les SEULES données pour lesquelles pour vous TOUT est permis ce sont VOS DONNÉES (votre nom, votre prénom, votre date de naissance, vos numéros de téléphone, nos numéro de CB, vos mots de passe, les chiffres de votre comptabilité...). vous pouvez faire ce que vous voulez avec VOS données (les accrocher derrière un Sessna et les faire défiler dans le ciel si ça vous chante). Toutes les autres données, celle appartenant à d'autres personnes ne vous appartiennent pas et vous ne pouvez pas faire ce que vous voulez avec.

Toutes les autres données appartiennent à des personnes qui comptent, et cela va de sois, sur votre discrétion et votre professionnalisme pour ne pas diffuser, divulguer ou rendre accessible ces données à des tiers non autorisés ou malveillants.

3. A l'heure des gros titres quasiment quotidiens faisant état d'un usage de données volées, de la diffusion ou de la vente dans le « darknet » (sorte de marché noir de l'Internet) ou pire, dans l'Internet public de données volées à des personnes comme vous et moi, il est, selon l'avis de Denis JACOPINI urgent d'arrêter de donner à manger à ces pirates informatiques qui basent avant tout leur activité lucratives sur les erreurs et failles des utilisateurs et informaticiens négligents insensibles à la sécurité informatique ne se souciant que de la part disponibilité ou intégrité dans leur applications de la sécurité informatiques, mais ni de confidentialité et encore moins d'analyse de risque.

Les opportunités pour les établissements concernés

En entamant une démarche de mise en conformité avec la Loi Informatique et liberté I ou II, avec la Loi pour une République Numérique ou avec le RGPD (Règlement Général sur la Protection des Données), Denis JACOPINI ajoute que vous allez être amenés à corriger plusieurs failles dans les traitements de données personnelles dont votre activité administrative ou professionnelles dépend :

- En vous intéressant à la durée de conservation de vos documents, vous allez épurer vos archives contenant la plupart du temps « au cas où » la totalité de la mémoire de l'entreprise de la plus petite notre manuscrite jusqu'au dossier complet sur une entreprise ou une personne en particulier. En mettant à plat l'ensemble de vos traitements de données personnelles, vous constaterez très certainement que vous conservez des données sans y être obligé. Les détruire vous permettra non seulement de gagner de la place (**Gain de place = Gain d'argent**), mais également de réduire vos responsabilité en sécurisant l'accès à ces données confidentielles pour la plupart (**Moins de responsabilités = moins de risque**) ;

- Concernant la confidentialité, vous allez ensuite vous rendre compte qu'à la question QUI à accès à QUOI ? il est peut être temps de faire du ménage. Entre les utilisateurs qui n'existent plus et les dossiers contenant des informations sensibles partagés sans restriction particulière, il sera probablement nécessaire de revoir sa PSSI (Politique de Sécurité des Systèmes d'Information) ; L'entreprise y tirera un avantage en matière de tranquillité et surtout cela diminuera ses responsabilités en cas de vol de données (**Moins de risques = Plus de tranquillité**) ;

- Difficile de mettre en place une telle démarche sans avoir une personne dédiée à ces fonctions. Jusqu'au 25 mai 2018 il s'appelle CIL (Correspondant Informatique et Libertés) et DPD (Data Protection Officer) ensuite. Ce soldat dédié à la protection des données n'est pas là que pour dire à son employeur ce qu'il faut faire pour rester dans les clous de la réglementation sur les données personnelles ou signaler ce qu'il ne faut pas faire.

Cette personne dédiée à temps partiel ou à temps complet à ces fonctions a pour but, par son existence et sa déclaration auprès de l'autorité compétente (la CNIL en France), de rassurer celui qui vous a confié, qui vous confie et qui vous confiera encore des données personnelles. Sachant que bientôt la quasi totalité des citoyens et consommateurs déposeront des informations auprès d'organismes ou sur des site Internet essentiellement parce qu'ils ont confiance envers le service utilisé, l'existence de cet intermédiaire entre l'autorité compétente et votre établissement sera à minima essentielle pour ne pas faire fuir les usagers de vos services (**Plus de confiance = Plus d'activité**).

Autres avantages collatéraux

En entamant une démarche de mise en conformité avec les lois relatives à la protection des données personnelles, vous contribuez à la diminution de la cybercriminalité dans le monde. En effet, données plus protégées = données difficile à voler par les pirates du Web = moins de pirates = moins de temps perdu à traiter les prélèvements frauduleux, les usurpations d'identité et pannes informatiques.

Les démarches à accomplir recommandées par Denis JACOPINI

1. Faire un état des lieux des données personnelles soumises à la réglementation ;
2. Rechercher la présence ou non de dérogation ou d'exception relatives à votre activité ou aux données personnelles traitées ;
3. Réaliser une analyse de risque relative aux données personnelles (Denis JACOPINI a spécialement passé la certification ISO 27005 qui concerne les analyses de risques relatives aux données) ;
4. Mettre en conformité les traitements des données personnelles afin qu'ils répondent aux réglementations (Loi Informatique et Libertés / Loi pour une République Numérique / Règlement Général sur la Protection des Données RGPD) ;
5. Mettre en place un registre et porter les annotations nécessaires à l'amélioration des traitements ;
6. Suivre l'évolution de l'établissement, des traitements, des risques et mettre à jour le registre.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Qui a le droit d'accéder à nos données numériques après notre mort ?

<input type="checkbox"/>	Qui a le droit d'accéder à nos données numériques après notre mort ?
--------------------------	---

Faisant partir de la Loi du 7 octobre 2016 pour une République numérique

le 10 10 2016 (dite aussi Loi Lemaire), en complément d'un chapitre traitant de mesures sur l'ouverture des données publiques, d'un autre sur le principe de neutralité des réseaux et de portabilité des données, un chapitre traite de notre mort numérique ou en d'autres termes, après notre mort, qui pourra avoir accès aux données numériques qui nous appartenaient ?

La loi n° 78-17 du 6 janvier 1978 a été impactée par cette Loi pour une République numérique.

L'article 40 est ainsi complété par un article 40-1 ainsi rédigé :

Art. 40-1 article I. : « Les droits ouverts à la présente section s'éteignent au décès de leur titulaire. Toutefois, ils peuvent être provisoirement maintenus conformément aux II et III suivants.

Art. 40-1 article II. : « Toute personne peut définir des directives relatives à la conservation, à l'effacement et à la communication de ses données à caractère personnel après son décès. Ces directives sont générales ou particulières.

« Les directives générales concernent l'ensemble des données à caractère personnel se rapportant à la personne concernée et peuvent être enregistrées auprès d'un tiers de confiance numérique certifié par la Commission nationale de l'informatique et des libertés.

« Les références des directives générales et le tiers de confiance auprès duquel elles sont enregistrées sont inscrites dans un registre unique dont les modalités et l'accès sont fixés par décret en Conseil d'Etat, pris après avis motivé et publié de la Commission nationale de l'informatique et des libertés.

« Les directives particulières concernent les traitements de données à caractère personnel mentionnés par ces directives. Elles sont enregistrées auprès des responsables de traitement concernés. Elles font l'objet du consentement spécifique de la personne concernée et ne peuvent résulter de la seule approbation par celle-ci des conditions générales d'utilisation.

« Les directives générales et particulières définissent la manière dont la personne entend que soient exercés, après son décès, les droits mentionnés à la présente section. Le respect de ces directives est sans préjudice des dispositions applicables aux archives publiques comportant des données à caractère personnel.

« Lorsque les directives prévoient la communication de données qui comportent également des données à caractère personnel relatives à des tiers, cette communication s'effectue dans le respect de la présente loi.

« La personne peut modifier ou révoquer ses directives à tout moment.

« Les directives mentionnées au premier alinéa du présent II peuvent désigner une personne chargée de leur exécution. Celle-ci a alors qualité, lorsque la personne est décédée, pour prendre connaissance des directives et demander leur mise en œuvre aux responsables de traitement concernés. A défaut de désignation ou, sauf directive contraire, en cas de décès de la personne désignée, ses héritiers ont qualité pour prendre connaissance des directives au décès de leur auteur et demander leur mise en œuvre aux responsables de traitement concernés.

« Toute clause contractuelle des conditions générales d'utilisation d'un traitement portant sur des données à caractère personnel limitant les prérogatives reconnues à la personne en vertu du présent article est réputée non écrite.

Art. 40-1 article III.-En l'absence de directives ou de mention contraire dans lesdites directives, les héritiers de la personne concernée peuvent exercer après son décès les droits mentionnés à la présente section dans la mesure nécessaire :

- «-à l'organisation et au règlement de la succession du défunt. A ce titre, les héritiers peuvent accéder aux traitements de données à caractère personnel qui le concernent afin d'identifier et d'obtenir communication des informations utiles à la liquidation et au partage de la succession. Ils peuvent aussi recevoir communication des biens numériques ou des données s'apparentant à des souvenirs de famille, transmissibles aux héritiers ;

- «-à la prise en compte, par les responsables de traitement, de son décès. A ce titre, les héritiers peuvent faire procéder à la clôture des comptes utilisateurs du défunt, s'opposer à la poursuite des traitements de données à caractère personnel le concernant ou faire procéder à leur mise à jour.

« Lorsque les héritiers en font la demande, le responsable du traitement doit justifier, sans frais pour le demandeur, qu'il a procédé aux opérations exigées en application du troisième alinéa du présent III.

« Les désaccords entre héritiers sur l'exercice des droits prévus au présent III sont portés devant le tribunal de grande instance compétent.

« IV.-Tout prestataire d'un service de communication au public en ligne informe l'utilisateur du sort des données qui le concernent à son décès et lui permet de choisir de communiquer ou non ses données à un tiers qu'il désigne. » ;

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Source : *LOI n° 2016-1321 du 7 octobre 2016 pour une République numérique* | *Legifrance*

Secret des correspondances : Ce que change la Loi Lemaire à partir de 2017

✕	Secret des correspondances : Ce que change la Loi Lemaire à partir de 2017
---	--

Le 30 mars 2017 a été publié au Journal Officiel un décret d'application de la loi pour une République numérique relatif au secret des correspondances (article 68 de la loi). A cette occasion, la CNIL en profite pour faire le point sur cette notion et sur ce qui change pour les utilisateurs de services de messagerie électronique.

Le 30 mars 2017 a été publié au Journal Officiel un décret d'application de la loi pour une République numérique relatif au secret des correspondances (article 68 de la loi). A cette occasion, la CNIL en profite pour faire le point sur cette notion et sur ce qui change pour les utilisateurs de services de messagerie électronique.

La correspondance privée se définit comme tout message exclusivement destiné à une ou plusieurs personnes physiques ou morales, déterminées et individualisées. L'exemple le plus concret est le courrier échangé entre deux ou plusieurs correspondants, depuis un service de messagerie.

Ainsi, toute correspondance entre deux personnes doit être protégée au titre du secret, par les opérateurs dont l'activité consiste à acheminer, transmettre ou transférer le contenu de ces correspondances. Tout comme un facteur n'a pas le droit d'ouvrir un courrier postal, le fournisseur de messagerie électronique ou le fournisseur d'accès à internet sont tenus de respecter le secret des courriers électroniques.

Ce principe de confidentialité était d'ailleurs déjà garanti par l'article L32-3 du Code des postes et des communications électroniques qui prévoyait, dans sa version antérieure à la publication de la loi pour une République numérique que « les opérateurs, ainsi que les membres de leur personnel, sont tenus de respecter le secret des correspondances ».

La directive européenne 2002/58 modifiée relative à la vie privée dans les communications électroniques (l'article 5.1) interdit « à toute autre personne que les utilisateurs d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance, sans le consentement des utilisateurs ».

Le contenu des communications, c'est-à-dire des correspondances entre deux individus, est par principe confidentiel et l'obligation de garantir le secret repose sur les opérateurs de télécommunication.

Il est en revanche possible de lever le secret des correspondances, en demandant aux personnes concernées leur consentement.

Qu'est-ce qui change avec la loi pour une République numérique et son décret d'application relatif à la confidentialité des correspondances ?

L'article 68 de la loi pour une République numérique précise ce que couvre le secret des correspondances. Le secret s'applique ainsi à l'identité des correspondants, au contenu, à l'intitulé et aux pièces jointes des correspondances.

Quels sont les professionnels concernés ?

Sont désormais soumis au respect du secret des correspondances, à la fois les « opérateurs », c'est-à-dire les opérateurs de télécommunications essentiellement, et les « fournisseurs de services de communication au public en ligne », en d'autres termes, tout acteur permettant à deux personnes de correspondre en ligne. Seront notamment concernés les fournisseurs de services de messagerie électronique, de réseaux sociaux, de communication synchrone (VoIP), etc.

A quelles conditions peuvent-ils exploiter la correspondance privée ?

La loi leur permet toutefois d'exploiter la correspondance privée, sous réserve d'obtenir le consentement des utilisateurs et pour les seules finalités suivantes :

- l'amélioration du service de communication au public en ligne,
- la réalisation de statistiques,
- l'utilisation des données à des fins publicitaires.

Quels sont les effets en pratique pour les opérateurs de communication électronique ou fournisseurs de service ?

La CNIL rappelle que, pour être valable, ce consentement doit être libre, spécifique et informé. Il doit en outre résulter d'un acte positif et être préalable à la collecte des données, c'est-à-dire à la réalisation du traitement.

Un consentement informé

Les opérateurs souhaitant utiliser la correspondance de leurs utilisateurs à des fins statistiques, publicitaires ou encore pour améliorer leur service devront recueillir leur consentement spécifique après les avoir informés de ce qu'ils souhaitent faire (en rappelant les mentions requises par l'article 32 de la loi Informatique et Libertés).

Un consentement spécifique

La CNIL rappelle que le consentement doit être spécifique et qu'à ce titre, un consentement global pour plusieurs finalités différentes, de même que l'acceptation globale des Conditions générales d'utilisation (ou CGU) du service, ne peuvent être considérés comme un consentement valable.

Un consentement libre

Le consentement ne doit pas être contraint, c'est-à-dire que le refus de consentir ne doit pas empêcher la personne d'accéder au service de messagerie. Le consentement doit prendre la forme d'un acte positif des utilisateurs et ne peut donc être déduit du silence ou de l'inaction des utilisateurs. Le consentement devant être recueilli avec une périodicité d'un an, la CNIL recommande que les responsables de traitement alerte les personnes dans un délai raisonnable avant l'échéance de ce délai, pour que le renouvellement ne soit pas automatique.

Un consentement renouvelé tous les ans

La loi pour une République numérique prévoit que le consentement doit être renouvelé périodiquement, c'est-à-dire recueilli tous les ans par les opérateurs exploitant les correspondances.

Par ailleurs, la CNIL rappelle que les traitements réalisés sur les correspondances doivent se limiter aux données collectées de manière loyale et licite. En conséquence, les traitements ne doivent produire des effets qu'à l'égard des personnes qui ont valablement consenti à la collecte de leurs données à caractère personnel issues du contenu de leurs correspondances. A titre d'exemple, les traitements opérés à des fins publicitaires et basés sur le contenu des correspondances ne doivent pas permettre à l'opérateur de cibler d'éventuelles personnes tierces dont les données personnelles apparaîtraient dans la correspondance.

Enfin, la CNIL rappelle qu'une fois le règlement européen relatif à la protection des données, adopté, les responsables de traitement devront être en mesure de prouver que les personnes ont effectivement consenti au traitement et seront tenus de les informer de la possibilité de retirer leur consentement.

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement. (Autorisation de la Direction du Travail de l'Emploi et de la Formation Professionnelle n°93 84 93941 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>

Régissez à cet article

Source : *Secret des correspondances : un consentement renforcé des utilisateurs de services de communication électronique | CNIL*

La CNIL face au compte à rebours de la nouvelle loi européenne

 **La CNIL face au compte à rebours de la nouvelle loi européenne**

La Commission nationale de l'informatique et des libertés doit préparer l'application, en mai 2018, du nouveau règlement européen sur les données personnelles. Le temps presse.

De l'aveu de sa présidente, Isabelle Falque-Pierrotin, l'année 2016 a été « *intense* » pour la Commission nationale de l'informatique et des libertés (CNIL). La présidente de l'instance chargée de la protection des données personnelles en a donné la mesure, lundi 27 mars lors de la présentation de son rapport annuel, en égrenant les principaux dossiers qui ont concerné l'institution lors de l'année passée : adoption du nouveau règlement européen sur les données personnelles ; actions lancées contre plusieurs géants du Net ; débat sur le chiffrement ; loi pour la république numérique ; polémique autour du fichier biométrique TES ; début des processus électoraux...

Ce surcroît d'activité ne s'est cependant pas traduit dans le nombre de procédures traitées par la Commission. En 2016, elle a reçu plus de 7 703 plaintes, un peu moins que l'année précédente (7 908), procédé à 430 contrôles (501 en 2015), prononcé 82 mises en demeure (93 en 2015) et infligé 13 sanctions dont 4 financières (10 en 2015). C'est plutôt du point de vue législatif que l'année 2016 a été chargée, marquée par l'adoption de « *trois textes qui bouleversent la protection des données personnelles* » dans le sens d'« *une plus grande maîtrise de leurs données par les individus* », a expliqué Mme Falque-Pierrotin.

Le défi du règlement européen

La loi pour une république numérique a été publiée au *Journal officiel* le 7 octobre, et l'accord Privacy Shield est entré en vigueur, après de longues négociations, le 1^{er} août. Mais c'est surtout l'adoption définitive, en mai, du nouveau règlement européen sur les données personnelles qui a constitué, selon Mme Falque-Pierrotin, « *une étape majeure pour la protection des données personnelles en Europe* ». Ce règlement institue notamment des sanctions plus importantes pour les entreprises, de nouveaux droits pour les citoyens et une meilleure coordination des autorités de protection des données. Il nécessite à la fois des adaptations de la part des entreprises, mais aussi un travail législatif au niveau français pour toilettier la loi informatique et libertés de 1978. Le temps presse : le règlement s'appliquera dès le 25 mai 2018. « *2017, c'est la cote d'alerte* », a ainsi prévenu M^{me} Falque-Pierrotin.

Les entreprises « *doivent se mettre en marche* » pour se conformer au règlement, a-t-elle expliqué, insistant sur le rôle d'accompagnement de la Commission. Consciente de l'effort requis, elle a tenté de rassurer : « *Nous sommes convaincus qu'il n'y a pas d'innovation sans protection des données personnelles* » : « *Il est possible d'innover et que, loin de la contraindre, la protection des données permet de développer l'innovation.* »

Autre obstacle de taille, législatif cette fois : pour être appliqué dès le mois de mai 2018, la nouvelle loi informatique et liberté « *devra être déposée en conseil des ministres avant l'été* ».

« *Pour le moins délicat* », a euphémisé M^{me} Falque-Pierrotin...[lire la suite]

Téléchargez le rapport annuel 2016

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur
: <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Source : *En 2017, la CNIL face au compte à rebours de la nouvelle loi européenne*

Le Règlement Général sur la Protection des Données (RGPD) en détail

<input type="checkbox"/>	Le Règlement Général sur la Protection des Données (RGPD) en détail
--------------------------	--

Après quatre années d'âpres négociations, les États Membres de l'Union Européenne sont enfin convenus d'un texte venant moderniser la directive 1995/46/CE du 24 octobre 1995, laquelle datait des débuts d'Internet. Mais, contrairement à une directive, le Règlement adopté le 8 avril 2016 par le Conseil de l'Europe puis, le 16 avril, par le Parlement européen, est d'application directe et s'imposera aux États Membres à compter du 25 mai 2018, sans qu'il soit besoin de le transposer dans les législations nationales.

Le processus d'élaboration du texte, long et émaillé de près de 4000 amendements, a mis au monde un texte très long – plus de 200 pages – comportant 99 articles introduits par 173 considérants. Intitulé « Règlement n°2016/679 du Parlement Européen et du Conseil du 27 avril 2016 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 », le texte résultant, complexe et technique, est particulièrement difficile à aborder par les entreprises et les administrations, lesquelles sont pourtant les principaux acteurs visés par le texte. Ainsi, dans un article du 18 octobre 2016, le journal La Tribune écrivait que « 90% des entreprises des trois principales économies européennes (France, Allemagne, Royaume-Uni) ne comprennent pas encore clairement le Règlement général de protection des données (RGPD) ». Selon une étude publiée ce mardi par la société de sécurité informatique Symantec, 92% des dirigeants et décideurs français s'inquiètent de ne pas être en conformité au moment de l'entrée en vigueur de la RGPD » !

Les acteurs du traitement de données vont donc devoir investir considérablement pour se mettre à niveau de la nouvelle réglementation, d'autant que toutes les entreprises du monde traitant des données personnelles de citoyens européens sont concernées par le Règlement.

Nous nous proposons, à travers cet article, d'exposer les principales nouveautés du texte sous une forme compréhensible pour le non-initié. Nous dresserons au préalable un tableau général des intentions du texte (I) avant d'insister sur ses innovations principales (II).

I- Présentation générale du RGPD

Le but déclaré du texte est de renforcer le contrôle des citoyens européens sur l'utilisation de leurs données personnelles, tout en simplifiant, en l'unifiant, la réglementation pour les entreprises.

Les citoyens pourront désormais réclamer contre l'utilisation abusive de leurs données auprès d'une autorité unique, chargée de la protection des données, plutôt que de devoir le faire auprès de l'entreprise détentrice de leurs données. Les particuliers pourront également se joindre à des recours collectifs via des organisations représentatives qui, si la loi nationale les y autorise, pourront agir de leur propre initiative.

Le RGPD développe ainsi considérablement les droits reconnus à la personne dont les données sont collectées. Ainsi, des trois droits reconnus à la personne par la loi Informatique et Liberté (opposition au traitement sous réserve de motif légitime, droit d'accès/communication aux données, droit de rectification/suppression), l'on passe à 11 droits (droit à une information complète en langage clair, droit à l'oubli, droit à la limitation du traitement, droit à la portabilité des données, droit d'opposition (notamment au profilage), etc.). D'une manière générale, la personne concernée dispose d'un droit étendu et facilité à accéder aux données à caractère personnel qui la concernent et le texte réaffirme les principes essentiels de la protection de la vie privée :

- Restriction d'utilisation ;
- Minimisation des données ;
- Précision ;
- Limitation du stockage ;
- Intégrité ;
- Confidentialité.

Les entreprises sont incitées à privilégier l'utilisation de pseudonymes avant et pendant le traitement des données pour en garantir la protection (concept de la prise en compte du respect de la vie privée dès la conception). La « pseudonymisation » consiste à s'assurer que les données sont conservées sous une forme ne permettant pas l'identification directe d'un individu sans l'aide d'informations supplémentaires.

II- Principales mesures du RGPD

1. Réalisation d'une analyse d'impact avant la mise en place d'un traitement de données

Avant la mise en place d'un traitement de données pouvant présenter des risques pour la protection des données personnelles, l'entreprise devra réaliser une analyse d'impact : « Lorsqu'un type de traitement, en particulier par le recours à de nouvelles technologies, et compte tenu de la nature, de la portée, du contexte et des finalités du traitement, est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le responsable du traitement effectue, avant le traitement, une analyse de l'impact des opérations de traitement envisagées sur la protection des données à caractère personnel. » (Article 35 du Règlement)

Le RGPD introduit ainsi le concept de prise en compte du respect de la vie privée dès la conception du traitement ; les différentes obligations pesant sur la collecte des données doivent être prises en compte dès la conception du traitement de données (« privacy by design and by default »).

2. Consentement clair et explicite à la collecte des données

La directive 1995/46/CE donnait une définition du consentement à la collecte des données, laquelle a été transposée de manière très hétérogène dans les législations nationales, certaines exigeant un consentement explicite, d'autres décidant qu'un consentement implicite était suffisant. Notre loi Informatique et Liberté se contente ainsi de définir des cas dans lesquels le consentement devrait être explicite. Le Règlement vient unifier une fois pour toute cette définition au onzième point de son article 4 consacré aux définitions, en définissant le consentement comme « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ».

Ce consentement doit donc être expressif. Il doit résulter d'un acte positif. La personne doit réellement avoir été mise devant la nécessité de donner son accord au traitement. Ainsi, dans son considérant n°32, le Règlement précise qu'« il ne saurait dès lors y avoir de consentement en cas de silence, de case cochée par défaut ou d'inactivité. » Plus encore, la charge de la preuve du consentement pèse sur le responsable du traitement (article 7, 1°). En outre, la personne dont les données sont collectées peut retirer son consentement à tout moment (article 7, 3°).

Malgré cela, le Règlement prévoit un certain nombre de cas pour lesquels le traitement demeure licite même sans consentement (article 6, b) à f) :

- Lorsque ce traitement est nécessaire à l'exécution d'un contrat accepté par la personne ;
- Lorsque le traitement découle d'une obligation légale ;
- Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne ;
- Le traitement est nécessaire à l'exécution d'une mission d'intérêt public ;
- Tout autre intérêt légitime du responsable du traitement, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne, en particulier s'il s'agit d'un enfant.

3. Accès facilité de la personne à ses données

Les personnes dont les données sont collectées disposent de droits à la rectification, à l'effacement des données et à l'oubli : « la personne concernée a le droit d'obtenir du responsable du traitement l'effacement, dans les meilleurs délais, de données la concernant et le responsable du traitement a l'obligation d'effacer ces données dans les meilleurs délais » (Article 17), et ce pour six motifs : les données ne sont plus nécessaires, la personne concernée retire son consentement, la personne concernée s'oppose au traitement à des fins de prospection, les données ont fait l'objet d'un traitement illicite, les données doivent être effacées pour respecter une obligation légale, ou encore les données ont été collectées dans le cadre d'une offre de service à destinations de mineurs.

4. Notification des violations de données personnelles (« Data Breach Notification »)

À l'heure actuelle, les différentes directives européennes font peser sur les entreprises du secteur de la télécommunication l'obligation d'informer les autorités en cas d'accès non autorisé à des données personnelles. En clair, lors d'un piratage, le Règlement, quant à lui, généralise cette obligation de signalement à l'ensemble des responsables de traitement, et ce au plus tard 72 heures après la découverte du problème (Article 33). Bien entendu, il faut que le problème atteigne une certaine gravité pour qu'il soit nécessaire de le rapporter, et tout va donc dépendre de la détermination du seuil à partir duquel le signalement devient obligatoire. L'article 34 du Règlement indique que ce signalement devra intervenir « lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique. » L'emploi du mot « élevé » laisse donc place à appréciation et donnera donc probablement lieu au développement d'une jurisprudence abondante.

Les personnes concernées par la violation des données doivent également être notifiées dans les meilleurs délais, sauf si des mesures de protection ont été mises en œuvre ou seront prises ultérieurement.

5. La création et la maintenance d'un registre des traitements devient obligatoire

Aux termes de l'article 30 du RGPD, un registre détaillé des traitements doit désormais être obligatoirement conservé non seulement par le responsable du traitement mais également par ses éventuels sous-traitants. Ce registre doit pouvoir être mis à tout moment à disposition des autorités de contrôle.

Le texte insiste ainsi sur la responsabilité du contrôleur des données, lequel est responsable de la conformité du traitement avec le Règlement et doit être, à tout moment, en mesure de le démontrer.

Lorsque le traitement de données est délégué par le responsable du traitement à un sous-traitant, ou « data processor », même situé hors de l'Union Européenne, celui-ci a désormais les mêmes obligations que le responsable du traitement, y compris la désignation d'un délégué à la protection des données, et ce même dans le cas d'un traitement de données gratuits.

6. Création de délégués à la protection des données (Data Protection Officer)

Si notre loi Informatique et Liberté, et ses mises à jour, ont créé le Correspondant Informatique et Liberté (le « CIL »), le Règlement, quant à lui, rend obligatoire dans certains cas la nomination d'un délégué à la protection des données (DPO ou, en anglais, DPO : Data Protection Officer) pour les organismes privés ou publics dont « les activités de base (-) exigent un suivi régulier et systématique à grande échelle des personnes concernées » ou lorsque « le traitement est effectué par une autorité publique ou un organisme public » (article 37), à l'exception des juridictions. Ce délégué n'est obligatoire que dans certains cas, mais il est fortement recommandé de le nommer systématiquement puisque toute entreprise ou administration doit être capable à tout moment de rendre comptes à l'autorité de contrôle de l'état de ses traitements de données.

Le rôle du délégué à la protection des données sera de garantir la conformité des traitements de données avec les principes de protection de la sphère privée, tels que fixés par le RGPD, ainsi que de gérer les relations entre les personnes concernées (employés, clients) et les autorités de surveillance.

7. Le transfert des données est soumis à vérification et peut être demandé par la personne elle-même

Les transferts de données personnelles vers des pays étrangers sont désormais soumis à la vérification des garanties offertes par les lois de ce pays pour préserver un niveau de sécurité équivalent pour les données. L'article 45 du Règlement prévoit que, dans l'idéal, le pays destinataire devra être listé par la Commission européenne. A défaut, des clauses de garantie spéciales devront être prévues dans les contrats, outre la possibilité de recourir à des codes de conduite, des certifications et autres labels. Auquel cas, il ne sera pas nécessaire d'obtenir une autorisation auprès de l'autorité nationale du pays d'origine des données.

En outre, l'article 49 du Règlement prévoit que, si le traitement nécessitait de recueillir le consentement de la personne, alors celle-ci devra être informée du transfert de ses données et des risques que présente l'opération. Ceci, bien entendu, afin de permettre à la personne de revenir éventuellement sur son consentement.

Enfin, les personnes dont les données sont collectées disposent elles-mêmes d'un droit à demander le transfert des données les concernant (ou « droit à la portabilité des données ») vers un autre fournisseur de services : « Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle » (Article 20).

8. Restriction du profilage automatisé servant de base à une décision

L'article 21 du Règlement dispose que « La personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques la concernant ou l'affectant de manière significative de façon similaire », sauf si ce traitement est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement, ou bien que la décision est autorisée par le droit de l'Union européenne, ou bien encore que le consentement explicite de la personne concernée a été recueilli en amont.

9. Recours et aggravation considérable des sanctions

La directive 1995/46/CE prévoyait jusqu'ici simplement la possibilité, pour la personne dont les droits ont été violés, de recourir aux tribunaux et d'obtenir du responsable du traitement réparation de son préjudice.

Le Règlement prévoit quant à lui un « droit à un recours effectif » (articles 78 et 79) et un « droit à réparation » (article 82). Il définit des règles de compétences des juridictions se substituant aux règles de droit international privé des États Membres et détermine les amendes qui devront être délivrées par les autorités nationales de contrôle (article 83). Or, les amendes mises en place par le Règlement sont considérables, puisqu'elles peuvent aller jusqu'à 20 millions d'euros ou 4% du chiffre d'affaire mondial ! Le risque qui pèse sur les entreprises imprudentes est donc très sérieux...[lire la suite]

Notre métier :

Nous proposons des services d'accompagnement sur plusieurs niveaux :

1/ Au niveau des utilisateurs qui, face à la résistance au changement, doivent comprendre l'intérêt des démarches de mise en conformité des traitements des données personnelles, pour favoriser leur implication et faciliter la mission du Correspondant aux Données Personnelles.

1'/ Au niveau des utilisateurs encore peu sensibilisés les utilisateurs aux différentes formes d'attaques et d'arnaques informatiques (cybercriminalité) dont les établissements sont très largement victimes.

Les services chargés de gérer les fournisseurs sont fortement incités à suivre notamment un module sur les arnaques aux FOVI et à voir leurs procédures auditées et probablement améliorées.

2/ Au niveau de l'établissement complet afin de faire un état des lieux des traitements concernés et un audit des mesures de sécurité en place et à faire évoluer pour les rendre acceptables vis à vis de la Réglementation relative aux Données Personnelles.

3/ Au niveau du futur CIL ou du futur DPO afin de lui faire découvrir ses missions, l'accompagner dans sa prise de fonction et l'accompagner au fil des changements.

Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Régissez-vous à cet article

Original de l'article mis en page : RGPD : le Règlement Général sur la Protection des Données qui bouleverse la loi Informatique et Liberté. Par Bernard Rineau, Avocat, et Julien Marcel, Juriste.

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

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
<input type="checkbox"/>	Le décret du 6 décembre 2016 qui modifie les modalités de vote électronique				
<input type="checkbox"/>					


Le décret n°2016-1676 du 5 décembre 2016 publié au JO du 6 décembre précise les modalités de vote par voie électronique pour certaines élections professionnelles. Ce texte vient appliquer une mesure de l'article 58 de la loi Travail*.

Un vote électronique simplifié pour les DP et CE

Avant la loi Travail, le recours au vote électronique pour les élections professionnelles nécessitait un accord d'entreprise ou de groupe. Aujourd'hui, il est prévu qu'en l'absence d'accord, l'employeur pourra recourir au vote électronique unilatéralement dans le cadre des élections des délégués du personnel (DP) et du comité d'entreprise (CE). Le décret définit les modalités pratiques de cette mesure.

Ces dispositions sont entrées en vigueur le 7 décembre 2016.

* Loi n° 2016-1088 du 8 août 2016 relative au travail, à la modernisation du dialogue social et à la sécurisation des parcours professionnels

 Décret n° 2016-1676 du 5 décembre 2016 relatif au vote par voie électronique

Réagissez à cet article

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 solutions 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 rapports 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

Les lanceurs d'alertes dans la Loi pour une République numérique

✕	Les lanceurs d'alertes dans la Loi pour une République numérique
---	--

Les lanceurs d'alertes ou « white hats » interpellent de plus en plus les médias depuis quelques années. Ces hackers éthiques interviennent dans l'informatique et le numérique, ils veillent à avertir les responsables de la sécurité des SI des vulnérabilités de leurs systèmes d'information ou de leurs sites web.

De plus, avec le développement de plates-formes de bug bounty comme YesWeHack, il était important de légaliser une pratique exposée à des sanctions pénales (ex : art. 323-1 du code pénal, 2 ans de prison et 60.000 euros d'amende). La loi n° 2016-1321 du 7 octobre 2016 pour une République numérique vient préciser le cadre légal de leurs actions.

L'AFFAIRE DE L'ANSES ET LE VOL DE DONNÉES

Un journaliste-blogueur surnommé « Bluetouff » avait extrait, puis publié de nombreux fichiers confidentiels en pénétrant sur le site extranet de l'Agence nationale de sécurité sanitaire de l'alimentation, de l'environnement et du travail (ANSES). Il a été condamné par la Cour d'appel de Paris le 5 février 2014, puis par la Cour de cassation le 20 mai 2015 pour maintien frauduleux dans le SI et vol de données. Le législateur, « alerté » de cette situation, a commencé par modifier l'article 323-3 du code pénal en y ajoutant les actions d'extraire, de détenir, de reproduire, de transmettre frauduleusement des données (Loi n°2015-912 du 24 juillet 2015).

LA PREMIÈRE MOUTURE VISÉE À L'ARTICLE 20 SEPTIÈME DE LA LOI

C'est un amendement du 15 janvier 2016, dit « Bluetouff » qui a relancé les débats sur le sujet ayant abouti à la proposition d'ajouter un nouvel alinéa à l'article 323-1 du code pénal, ainsi rédigé :

« Toute personne qui a tenté de commettre ou commis le délit prévu au présent article est exempte de peine si elle a immédiatement averti l'autorité administrative ou judiciaire ou le responsable du système de traitement automatisé de données en cause d'un risque d'atteinte aux données ou au fonctionnement du système. »

Il était censé protéger les lanceurs d'alerte lorsqu'ils veillent « à avertir les responsables de traitement des failles dans leurs systèmes. » Or, cette rédaction laissait dubitatifs les juristes et posait plus de questions qu'elle n'en résolvait, notamment : quelle autorité saisir et par quel canal (appel téléphonique à la police, courrier postal ou électronique à une cour d'appel ou à la CNIL, etc.) ? Que se passe-t-il après l'avertissement et surtout, si entre temps le responsable du SI a porté plainte, ou encore si le lanceur d'alertes diffuse les informations sur l'internet pour se faire de la publicité ? De plus, exemption de peine ne signifie pas non inscription au casier judiciaire de la condamnation. Pourtant, une décision du 9 septembre 2009 a jugé que tout accès non autorisé à un SI constitue un trouble manifestement illicite alors même que cela peut permettre d'éviter des atteintes ultérieures aux données ou au fonctionnement du système.

LA PROTECTION NOUVELLE DES LANCEURS D'ALERTE

L'article 47 de la nouvelle loi prévoit que le code de la défense soit complété par un article L. 2321-4 ainsi rédigé : « Art. L. 2321-4.-Pour les besoins de la sécurité des systèmes d'information, l'obligation prévue à l'article 40 du code de procédure pénale n'est pas applicable à l'égard d'une personne de bonne foi qui transmet à la seule autorité nationale de sécurité des systèmes d'information une information sur l'existence d'une vulnérabilité concernant la sécurité d'un système de traitement automatisé de données. »

« L'autorité préserve la confidentialité de l'identité de la personne à l'origine de la transmission ainsi que des conditions dans lesquelles celle-ci a été effectuée. »

« L'autorité peut procéder aux opérations techniques strictement nécessaires à la caractérisation du risque ou de la menace mentionnés au premier alinéa du présent article aux fins d'avertir l'hébergeur, l'opérateur ou le responsable du système d'information. »

L'information vise les vulnérabilités de sécurité des SI (art. 323-1) mais sans doute pas les autres délits informatiques prévus aux articles 323-2 (entraver et fausser le fonctionnement d'un SI), 323-3 (introduction de données, extraction, transmission, reproduction, suppression, modification des données) et 323-3-1 (programmes malveillants), ainsi que les infractions commises en groupe ou en bande organisée. Ces dernières infractions peuvent, en effet, causer des dommages importants au responsable du SI. L'un des points essentiels sera de déterminer les conditions de la *bonne foi* de la personne ayant détecté la vulnérabilité, étant observé que si la personne agit dans le cadre d'un programme de Bug bounty, on peut supposer que la bonne foi est présumée dans la mesure où le programme est déterminé par l'utilisateur, c'est à dire l'entreprise (idem pour la société qui réalise un Pentest). Il en va de même, si l'informateur a pénétré dans le site et qu'il s'en retire dès le moment où il s'aperçoit qu'il accède à une partie du site ou des données protégées...[lire la suite]

Notre métier : Sensibiliser les décideurs et les utilisateurs. Vous apprendre à vous protéger des pirates informatiques, vous accompagner dans votre mise en conformité avec la CNIL et le règlement Européen sur la Protection des Données Personnelles (RGPD). (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Denis JACOPINI anime dans toute la France et à l'étranger des conférences, des tables rondes et des formations pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles (Mise en Place d'un Correspondant Informatique et Libertés (CIL) dans votre établissement.

Plus d'informations sur : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>



Réagissez à cet article

Original de l'article mis en page : Les lanceurs d'alertes dans la Loi pour une République numérique