RGPD : Quel est le profil idéal pour devenir DPO

	RGPD : Quel est le profil idéal pour devenir DPO

Aujourd'hui, 47 % des CIL sont issus de l'IT et 19 % possèdent un profil plutôt juridique, selon les chiffres de la Cnil.

Le reste est un panachage assez large, allant du documentaliste au responsable administratif. A priori, le poste de DPO devrait correspondre à ces mêmes profils. « *Il y a cependant aujourd'hui une tendance à penser que le DPO devra surtout disposer d'un profil juridique. Mais c'est une erreur. Il faut préserver la richesse de profils qui a fait la force des CIL, et laisser notamment le poste de DPO ouvert à des informaticiens* », souligne Bruno Rasle (Président de l'AFCDP). Ayant un rôle éminemment transversal, le DPO doit être un « *très bon communicant* », indique-t-on à la Cnil. Outre la technique et le juridique, il doit également bien connaître les enjeux business, afin de ne pas se positionner comme un frein au développement de l'entreprise, mais davantage comme un garant du respect de la « privacy ». Un respect qui peut d'ailleurs être très positif en termes d'image de marque, indique l'AFCDP. Au final, il s'agit donc d'un poste très « politique », plutôt accessible aux collaborateurs expérimentés…[lire la suite]

Besoin d'un formateur RGPD ? Besoin de former votre futur DPO ? Contactez-nous

---

A Lire aussi :
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 : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Data Protection Officer : un gardien pour les données*

personnelles

Quels risques pour ne pas avoir fait faire d’expertise indépendante avant ses élections par voie électronique ?

Notre métier en RGPD et en CYBER : Auditer, Expertiser, Accompagner, Former et Informer					
	Quels risques pour ne pas avoir fait faire d’expertise indépendante avant ses élections par voie électronique ?				

La fiabilité et les modalités de mise en œuvre du vote électronique sont soumises quasiment chaque année à l'examen du juge. Plus d'un a pu se dire surpris de la contradiction apparente entre la jurisprudence du Conseil d'État et celle de la Cour de cassation relativement à l'obligation de réaliser une expertise indépendante préalablement à chaque scrutin recourant au vote électronique.

Le Conseil d'État, dans son arrêt 368748 du 11 mars 2015, a jugé nécessaire la réalisation d'une telle expertise avant chaque scrutin, afin de garantir de manière certaine « la sincérité des opérations électorales ».

La Cour de cassation, dans son arrêt du 21 septembre 2016, indique « qu'il résultait de l'expertise indépendante conduite entre juillet et octobre 2012 que le système de vote électronique utilisé pour le scrutin ne présentait aucune modification substantielle depuis celle qui avait été diligentée en 2005 lors de sa mise en place, le tribunal a exactement décidé qu'il avait été satisfait aux prescriptions des articles R. 2314-12 et R. 2324-8 du code du travail ; » On voit ici le problème qui se pose à l'organisateur d'un scrutin désireux de satisfaire à ses obligations mais aussi désireux de gérer au mieux les coûts occasionnés par l'organisation du vote électronique. Faut-il ou non diligenter une expertise indépendante, alors que la solution de vote a été expertisée auparavant ? Une circonstance est de nature à jeter un trouble encore plus grand lorsque l'on sait que le même système de vote a été utilisé dans les deux cas, objet de ces jurisprudences apparemment contradictoires, mais pour des élections différentes. Le problème n'est qu'apparent et la contradiction peu fondée….[lire la suite]

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

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

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

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

Contactez-nous

Source : *Vote électronique : l'expertise préalable comme principe fondamental du droit électoral – Global Security Mag Online*

La CNIL remet en cause le fonctionnement de la plate-forme APB

	La CNIL remet en cause le fonctionnement de la plate-forme APB

Dans un avis rendu public jeudi 28 septembre, la Commission met en demeure le ministère de l'enseignement supérieur de « cesser de prendre des décisions concernant des personnes sur le seul fondement d'un algorithme ».

C'est un nouveau coup porté à la plate-forme Admission post-bac (APB), qui permet de faire ses vœux d'orientation dans l'enseignement supérieur. Dans une décision du 30 août rendue publique jeudi 28 septembre, la Commission nationale de l'informatique et des libertés (CNIL) met en demeure le ministère de l'enseignement supérieur de « cesser de prendre des décisions concernant des personnes sur le seul fondement d'un algorithme et de faire preuve de plus de transparence » dans l'utilisation de la plate-forme.
Cette décision, qui « n'est pas une sanction », précise la CNIL, oblige cependant le ministère à se mettre en conformité avec la loi « dans un délai de trois mois ». Elle intervient suite aux polémiques qui ont émaillé la session 2017 d'APB. Notamment autour des milliers de candidats n'ayant pas reçu de proposition lors des trois phases de la procédure. Mais surtout en raison de l'utilisation du tirage au sort pour départager les candidats trop nombreux à l'entrée des filières universitaires en tension. Tirage au sort régulièrement remis en cause devant les tribunaux administratifs, qui estiment qu'il ne repose sur aucune base légale…[lire la suite]

A Lire aussi :
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)

Réagissez à cet article

Source : *La CNIL remet en cause le fonctionnement de la plate-forme APB*

Comment devenir DPO ? (Data Protection Officer)

	Comment devenir DPO ? (Data Protection Officer)

Quelles seront les missions du DPO ? La principale sera de veiller à l'intégrité et la protection des données personnelles de son organisation, tant sur le plan juridique que technique. Il sera également l'intermédiaire entre son organisation et l'autorité de contrôle, en France la Commission nationale de l'informatique et des libertés (Cnil).

Ce poste est donc assez proche de celui de Correspondant informatique et libertés (CIL), déployé depuis 2005 dans des entreprises et les entités publiques françaises. « *Les fonctions sont très similaires, mais le contexte est différent* », résume Albine Vincent, chef du service des CIL à la Cnil. Même son de cloches à l'AFCDP (*), association française représentant les CIL. « *Les fonctions d'un DPO sont à peu près les mêmes que celles d'un CIL, mais avec le niveau de sanctions prévues par le nouveau règlement, elles prennent une tout autre dimension* », estime son délégué général Bruno Rasle. D'ailleurs, sur les 4 800 CIL actuellement en poste, une grande majorité d'entre eux devraient devenir DPO d'ici à mai 2018. Cette évolution ne sera pas automatique, mais ce choix sera souvent le plus logique. « *Si le CIL a donné satisfaction dans sa mission, il sera bien placé pour devenir DPO. Il devra bien entendu se former pour connaître parfaitement la nouvelle réglementation* », poursuit Albine Vincent. Elle rappelle que la Cnil propose des ateliers d'information sur le sujet. Des formations longues existent aussi pour se former au poste de DPO, comme le Master CEID de Nanterre ou le mastère spécialisé de l'Institut supérieur d'électronique de Paris (Isep). « *Ce sera de la responsabilité de l'entreprise ou de l'entité publique de choisir la personne qui sera en mesure d'occuper ce poste* », poursuit Albine Vincent. « *Dans le cadre de ses missions de contrôles, la Cnil pourra vérifier que le DPO est bien en mesure de réaliser sa mission et notamment qu'il n'y a pas de conflits d'intérêts avec d'autres fonctions éventuelles qu'il occupe.* » Concrètement, la nomination du DPO devra être déclarée auprès de la Cnil, via un formulaire en ligne…[lire la suite]

A Lire aussi :
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)

Réagissez à cet article

Source : *Data Protection Officer : un gardien pour les données personnelles*

Les Français de plus en plus soucieux de la Protection de leurs données personnelles

Les Français de plus en plus soucieux de la Protection de leurs données personnelles

UN FRANÇAIS SUR TROIS A DEJA ESSAYE D'EFFACER DES INFORMATIONS PERSONNELLES SUR LA TOILE, 6 SUR 10 CHEZ LES MILLENIALS

33% des Français ont déjà essayé d'effacer des informations les concernant sur internet, dont 17% « plusieurs fois ». Un chiffre qui grimpe à 61% chez les 18-24 ans, dont 33% « plusieurs fois ».

Soucieux de leur e-réputation, près de 75% des 18-24 ans déclarent par ailleurs rechercher régulièrement sur le net des informations associées à leurs nom et prénom (vs 57% sur l'ensemble des Français).

LA PROTECTION DES DONNEES PERSONNELLES, UNE PREOCCUPATION EN HAUSSE, PARTICULIEREMENT CHEZ LES JEUNES

En 2017, **85% des Français se disent préoccupés par la protection de leurs données personnelles en général, soit une augmentation de 4 points par rapport à 2014**.

Une question qui suscite encore plus d'inquiétude dès lors qu'il s'agit de la protection des données sur Internet : **90% se disent préoccupés pour leurs données mises en lignes (+5 pts depuis 2014).**

Les 18-24 ans apparaissent particulièrement sensibles à cette question puisqu'ils sont 93% à se dire préoccupés par la protection de leurs données en ligne, **dont 48% « très préoccupés » (vs 39% pour l'ensemble des Français).**

ALORS QUE LES USAGES EN LIGNE ONT FORTEMENT PROGRESSE EN 3 ANS

51% des Français déclarent réaliser « souvent » des paiements en ligne (+12 points depuis 2014), 39% stockent des documents personnels (mails, photos, vidéos, fichiers divers) sur des serveurs, contre 31% il y a 3 ans ; enfin plus d'1 Français sur 2 publie régulièrement des propos ou des photos personnels sur les réseaux sociaux (52%), ils sont 72% chez les 18-24 ans.

SI LES USAGES A RISQUES RECULENT ET QUE LES PRATIQUES VERTUEUSES PROGRESSENT…

23% des Français déclarent saisir leurs coordonnées personnelles sur les forums, soit une baisse de 5 points par rapport à 2014, et seuls 17% des Français partagent par mail des messages types chaînes de lettre (-10 pts).

En parallèle, la protection de l'accès aux « device » a augmenté, l'utilisation d'un mot de passe s'est systématisée pour tous les équipements : 86% des Français utilisent un mot de passe pour leur ordinateur professionnel (+8 pts vs 2014), 76% pour leur ordinateur personnel (+7 pts), 73% pour leur téléphone mobile (+ 9 pts), 61% pour leur tablette tactile (+10 pts). Comme en 2014, plus de 93% des Français ont le souci de mettre à jour leur anti-virus.

… LES FRANCAIS N'ONT PAS ENCORE ADOPTE TOUS LES BONS REFLEXES

La grande majorité des Français (74%) utilise un seul et même mot de passe pour ses comptes et espaces en ligne, **une pratique en augmentation (+5 pts vs 2014),** sans doute à relier à la démultiplication du nombre de comptes par internaute et à la difficulté à gérer de nombreux mots de passe différents.

PIRATAGE BANCAIRE ET NON-RESPECT DE LA CONFIDENTIALITE DE LEURS DONNEES : PRINCIPALES CRAINTES DES FRANCAIS

80% des Français jugent le risque de piratage de leurs données bancaires important dont 47% « très » important. Parallèlement, les craintes des Français sont également vives concernant le respect de la confidentialité de leurs données (42%, +3 pts) et la protection des enfants dans leur usage d'Internet (49%, + 4 pts).

A QUI LES FRANÇAIS FONT-ILS CONFIANCE POUR PROTEGER LEURS DONNEES ?

Dans ce contexte, le lien de confiance entre les Français et les acteurs qui utilisent leurs données reste à renforcer, et pour certains acteurs, ce lien reste même à construire :

Les banques sont les seuls acteurs à obtenir la confiance de plus de la moitié des Français en matière de protection des données (53%, en augmentation de 3 pts). Comparativement, les opérateurs télécom, les moteurs de recherche ou les acteurs des réseaux sociaux ne recueillent qu'un faible niveau de confiance (respectivement 23%, 20%, et 10%).

Parallèlement, la confiance des Français envers l'Etat (47%,+7 pts) s'améliore sur cette question, et reste très élevée à l'égard de la CNIL, une instance très positivement perçue (77% + 3 pts)…[lire la suite]

Réagissez à cet article

Source : *CSA – Protection des données personnelles*

Privacy Shield : Le transfert de données Europe-USA suffisamment sécurisé ?

	Privacy Shield : Le transfert de données Europe-USA suffisamment sécurisé ?

Pour le Conseil national du numérique, le Privacy Shield doit être « renégocié » car l'accord n'offre pas de garanties suffisantes à la protection des données.

A l'occasion du premier bilan annuel du Privacy Shield et de ses garanties, le **Conseil national du numérique** (CNNum) exprime sa divergence.
L'accord de transfert d'une partie des données entre l'Union européenne et les Etats-Unis, qui a succédé au dispositif Safe Harbor à partir du 1er août 2016, « doit être renégocié », selon le comité consultatif d'experts en charge d'éclairer les pouvoirs publics sur le numérique.
Celui-ci dit partager les inquiétudes d'autres organisations comme les CNIL européennes (fédérées à travers le G29), la commission des libertés civiles du Parlement européen et des associations de défense des droits.
« Le Privacy Shield présente un trop grand nombre de zones d'ombre et ne donne pas suffisamment de garanties à la protection des données personnelles des Européens », souligne par voie de communiqué le CNNum.
L'accord en l'état est *« faible, susceptible d'annulation sur les mêmes fondements que son prédécesseur ».*
Le Safe Harbor avait été invalidé fin 2015 par la Cour de justice de l'Union européenne (CJUE).
La collecte massive et indifférenciée de données pratiquée par les services de renseignement américain, une pratique mise à jour par les révélations d'Edward Snowden relative au cyberespionnage américain, était au coeur de ce dossier.
Le Privacy Shield n'offrirait toujours pas de garanties satisfaisantes dans ce domaine.

Bouclier percé ?

Lors de négociations qui ont précédé l'adoption du Privacy Shield en juillet 2016, la Commission européenne avait obtenu des autorités américaines une avancée présumée : la collecte de masse de données devait être écartée au profit d'une collecte ciblée.
Mais cette avancée n'est qu'une *« simple directive présidentielle »* prise par l'ancien locataire de la Maison Blanche, Barack Obama, souligne le CNNum dans son communiqué. Sur le fond, *« le droit américain reste largement inchangé »* en la matière.
« Les évolutions législatives et jurisprudentielles récentes, combinés à la position affichée par la nouvelle administration [Trump] » sont *« un signal politique particulièrement préoccupant. »*
Le CNNum fait notamment référence aux évolutions à venir de la législation américaine en matière de données, dont le titre VII du FISA Amendments Act (FAA).Il est censé expirer à la fin de l'année mais pourrait être reconduit.
Ces dispositions incluent la controversée « section 702 », qui autorise la surveillance large de tout ressortissant d'un pays étranger.
Une section qui a notamment servi de fondement aux programmes de surveillance Prism et Upstream de la National Security Agency (NSA) que Snowden avait dévoilés à partir de mi-2013.
Le Conseil national du numérique s'inquiète également de *« la vacance de postes clés en charge de la supervision du dispositif côté américain »* et de *« l'effectivité des mécanismes de recours. »*
Des problématiques de souveraineté sont également soulevées par l'organisation.
Les données constituent un actif essentiel de l'économie numérique. Or les flux de données d'Europe sont *« massivement captés par les États-Unis »*, souligne l'organisation.
Cette asymétrie des transferts de data avait déjà été constaté dans le cadre du Safe Harbor…[lire la suite]

A Lire aussi :
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)

Réagissez à cet article

Source : *Transfert de données Europe-USA: le CNNum rejette le Privacy Shield | Silicon*

Télétravail et protection des données personnelles

Le télétravail pose certaines questions concernant d'abord le droit du salarié à la déconnexion mais aussi sur la protection des données. La barrière de plus en plus floue entre outils personnels et outils professionnels avec la collecte d'informations impose de revoir le régime juridique de la protection des données. Explications par François Alambret, Counsel chez Bryan Cave Paris.

L'essor du télétravail a accru la nécessaire protection des données personnelles. Si ces deux sujets se complètent, ils ne doivent éclipser les autres aspects de la digitalisation des relations de travail.

Le développement du télétravail

Le télétravail n'a pas attendu l'émergence d'internet pour exister mais il s'est incontestablement développé par la conjonction de différents facteurs : les progrès des outils technologiques individuels, l'individualisation des relations du travail et l'accroissement des centres urbains et leur congestion concomitante.

Poussé d'abord par les revendications des salariés, le télétravail a été organisé par les entreprises par le biais d'accords collectifs ou de chartes (informatiques ou sur la qualité de vie au travail), puis reconnues par les organisations syndicales au niveau européen et national (accord cadre européen sur le télétravail du 16 juillet 2002 et accord national interprofessionnel du 19 juillet 2005). Enfin, encadré par le législateur par le biais des lois du 22 mars 2012, du 8 août 2016 (Loi travail dite loi « El-Khomri ») et les ordonnances Macron en cours de promulgation.

Cette dernière étape législative vise encore à simplifier le recours au télétravail, notamment par le biais d'un accord ou d'une charte d'entreprise en dispensant ensuite les parties d'un avenant au contrat de travail (voir article 24 de l'ordonnance n°3 du 31 aout 2017 modifiant les articles L.1222-9 et suivants du code du travail).

L'employeur n'est plus tenu, non plus, de supporter le coût de ce télétravail, ce qui autorise le salarié « de facto » à utiliser son propre matériel informatique (avec les conséquences afférentes en termes de confidentialité et de sécurité).

La protection des données personnelles

Dès son apparition, le télétravail s'est heurté aux problématiques de la protection des données informatiques. Cette contrainte a d'ailleurs été rappelée expressément par les partenaires sociaux dans leur premier accord européen (point 5 de l'accord cadre du 16 juillet 2002) et national (article 5 de l'accord national interprofessionnel du 19 juillet 2005).

Et de fait, le télétravail accroît les risques sur la protection des données de façon à la fois structurelle et technique. Structurellement, par le mode même d'organisation du travail (qui augmente les communications digitales au détriment de communications directes et orales dans l'entreprise) et techniquement car le salarié demeure à distance des services informatiques de l'entreprise et peut dorénavant utiliser ses propres matériels informatiques avec les risques qui en découlent.

Le règlement communautaire sur la protection des données en date du 27 avril 2016 (souvent dénommé GDPR « Global Data Protection Regulations ») prend acte de la digitalisation croissante de la société et de ses nouvelles formes de travail. Il renforce les mesures de protection à l'égard des personnes et donc vis-à- vis des salariés et des télétravailleurs.

L'imbrication des deux notions/ le rôle de l'entreprise

Ces deux sujets (télétravail et protection des données) s'accompagnent et s'encouragent mutuellement. Le renforcement de la protection des données offre des garanties nécessaires au développement du télétravail.

Toutefois, ce cadre législatif et réglementaire posé, c'est aux acteurs de l'entreprise de s'en saisir et de le façonner.

A eux de négocier et de rédiger un accord collectif ou une charte permettant une mise en œuvre fluide mais aussi sécurisée du télétravail, dans le respect du nouveau règlement communautaire du 27 avril 2016.

Mais traiter ces deux thèmes isolément méconnaît l'ampleur des bouleversements de la digitalisation de la société et des relations du travail…[lire la suite]

A Lire aussi :

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)

Réagissez à cet article

Source : *Télétravail et protection des données personnelles – LE MONDE DU DROIT : le magazine des professions juridiques*

Qu’est-ce que GDPR ou RGPD ? Quelques principes

	Qu’est-ce que GDPR ou RGPD ? Quelques principes

GDPR, également appelée RGPD en France, le texte européen de référence sur la protection des données à caractère personnel, sera applicable dans tous les Etats membres de l'Union le 25 mai 2018, accompagné d'un volet répressif qui n'incite pas à passer outre…

Quelques principes de GDPR – RGPD

• **Le principe du consentement** : les entreprises doivent l'obtenir du citoyen/client. Et cela dès la conception des données. Et même avant avec la nouvelle règle de la sécurité par défaut qui impose aux entreprises de disposer d'un système d'information sécurisé.

• **Le droit à l'oubli** : le droit à l'effacement impose à l'entreprise l'obligation d'effacer les données à caractère personnel sous plusieurs motifs, et cela dans les délais les plus brefs. Le citoyen européen peut également s'opposer au profilage via des traitements automatisés.

• **Le droit à la portabilité des données personnelles** : les personnes pourront obtenir communication, dans un format lisible et structuré, des données personnelles les concernant. Au-delà de la communication des données, il autorise leur transfert vers d'autres acteurs, sous réserve que cela soit techniquement possible.

• **La nomination d'un DPO** : le DPO (*Data Protection Officer*) ou Délégué à la protection des données est une personne qui se voit confier la mission d'être associé aux questions relatives à la protection des données personnelles dans les entreprises privées comme les organisations publiques.

[lire la suite]

Besoin d'un formateur RGPD ? Besoin de former votre futur DPO ? Contactez-nous

---

A Lire aussi :
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
: https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *Qu’est-ce que GDPR ou RGPD ? Définition de GDPR et RGPD – IT Social | Média des Enjeux IT & Business, Innovation et Leadership*

ACCReD, le mégafichier de données personnelles qui suscite la polémique

ACCReD, le mégafichier de données personnelles qui suscite la polémique

---

Un décret paru dans le Journal officiel en pleine torpeur du mois d'août. La création d'ACCReD, mégafichier ciblant des milliers d'individus, a été discrète, voire escamotée.

Pourtant, comme l'a repéré Europe 1, ce nouveau traitement de données personnelles est loin d'être anecdotique.

Menace terroriste oblige, il doit améliorer le recoupement de fichiers déjà existants – celui des personnes recherchées, des antécédents judiciaires, des objets et véhicules signalés etc. – et en permettre une « consultation automatique et simultanée ». Au nom de la sécurité du territoire.

Mais un mois seulement après son apparition, la CNIL met déjà le holà. L'objectif d'ACCReD est certes « légitime », mais les moyens d'y parvenir suscitent quelques inquiétudes. Voici pourquoi.

Qui est fiché dans ACCReD ?

Tous les individus occupant un poste considéré comme « sensible » en France. Cette qualification est désormais élargie aux postes dans les aéroports, dans les centrales nucléaires mais aussi dans les événements festifs que ce soit des concerts, des festivals, des événements sportifs, etc…[lire la suite]

Que signifie ACCReD ?

Denis JACOPINI : (Automatisation de la Consultation Centralisée de Renseignements de Données)

Réagissez à cet article

Source : *Créé pendant l'été, un mégafichier de données personnelles suscite la polémique*

RGPD : Ce que les entreprises doivent savoir

	RGPD : Ce que les entreprises doivent savoir

Une étude réalisée par Trend Micro révèle que les cadres dirigeants n'ont pas encore pris en considération la mise en conformité avec le RGPD (Réglement Général sur la Protection des Données) qui entrera en vigueur le 25 mai 2018. Cela ne fait en tout cas pas partie de leur priorité.

L'étude Trend Micro indique, en effet, que 95 % des dirigeants savent qu'ils doivent se conformer à ce règlement et que 85 % d'entre eux ont déjà examiné ses dispositions légales. Sauf que 79 % d'entre eux sont persuadées que leurs données ne peuvent pas être mieux protégées qu'elles ne le sont aujourd'hui.
Si la prise de conscience est réelle, une certaine confusion demeure toujours concernant la nature exacte des données personnelles à protéger. En effet, 64 % des sondés ignorent que la date de naissance d'un client est considérée comme une donnée personnelle. De même pour les bases de données marketing contenant des emails (42 %), des adresses postales (32 %) et les adresses électroniques (21 %). Ces résultats montrent bien que les entreprises ne sont pas aussi préparées ou protégées qu'elles le prétendent…[lire la suite]

Besoin d'un formateur RGPD ? Besoin de former votre futur DPO ? Contactez-nous

---

A Lire aussi :
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
: https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article

Source : *RGPD : les entreprises n'ont pas encore pris toute la mesure de ce règlement*