

Demande d'annulation du Privacy Shield par UFC-Que Choisir



Alors que la protection des données personnelles est une préoccupation majeure des consommateurs, l'UFC-Que Choisir, compte tenu des risques que fait peser l'accord transatlantique sur la protection des données personnelles (Privacy Shield), intervient en soutien de deux recours en annulation contre cet accord.

Après l'invalidation en 2015 par la Cour de justice de l'Union européenne de l'accord encadrant le transfert de données entre les Etats-Unis et l'Europe, le « Safe Harbour », compte tenu du niveau de protection insuffisant des consommateurs européens, l'Union européenne a négocié un nouvel accord avec les Etats-Unis, le Privacy Shield. Cet accord a été adopté le 8 juillet 2016, malgré les inquiétudes formulées par le Parlement européen, plusieurs gouvernements, les CNIL et les associations de consommateurs européennes.

Loin de renforcer significativement le cadre juridique du transfert des données personnelles aux Etats-Unis et d'offrir un niveau de protection « adéquate », comme exigé par les textes communautaires, le nouvel accord n'offre qu'une protection lacunaire aux ressortissants européens : L'admission d'une collecte massive et indifférenciée des données personnelles par les services de renseignements américains

Les lois américaines autorisent encore aujourd'hui, malgré les critiques formulées dans le cadre de l'invalidation du Safe Harbour, la collecte massive d'information par la NSA et les services de renseignement américains auprès des entreprises détentrices de données personnelles, incluant des données de consommateurs français qui ont été transférées aux Etats-Unis.

Bien que le gouvernement américain se soit moralement engagé à réduire cette collecte autant que possible, aucune mesure concrète n'a encore été mise en place pour limiter ces traitements de données personnelles.

Cette situation est d'autant plus inquiétante que les autorités américaines sont aussi autorisées, sur la seule base de vos données personnelles, à rendre des décisions susceptibles de produire des effets juridiques préjudiciables à votre égard. Ainsi, suite à l'envoi d'un message privé sur Facebook, exprimant une opinion politique ou critiquant la collecte à tous crins des données par les multinationales américaines, vous pourriez vous voir interdire l'entrée aux Etats-Unis par les autorités américaines !

Un ersatz de droit au recours pour les consommateurs européens

Alors que le droit européen exige un droit au recours effectif et un accès à un tribunal impartial, le dispositif de réclamation prévu par le Privacy Shield est stratifié et complexe... Le principal recours en cas de décision préjudiciable rendue par les autorités américaines à l'encontre d'un ressortissant européen, est un médiateur... nommé par le Secrétaire d'état américain.

Enfin, le droit de s'opposer à un traitement est prévu uniquement en cas de « modification substantielle de la finalité du traitement », alors même que le droit européen offre le droit de s'opposer à un traitement de ses données personnelles à tout moment, aussi bien lors de la collecte, qu'en cours de traitement de données personnelles.

Dans le contexte de mondialisation des échanges et de transfert des données vers des Etats avec des niveaux moindres de protection que le niveau européen, ces risques sont loin d'être théoriques comme l'a souligné récemment l'association s'agissant de la collecte de données via des jouets connectés ou des applications mobiles et leur transfert vers les Etats-Unis.

Au vu de ces éléments inquiétants, deux recours en annulation ont été déposés en septembre 2016 devant le Tribunal de l'Union européenne : l'un par le 'Digital Right Ireland', groupe lobbyiste Irlandais de défense de la vie privée sur Internet, l'autre par les 'Exégètes amateurs', groupe de travail regroupant trois associations françaises...[lire la suite]

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 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>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DIRETIF n°93 84 03041 84)
- Formation de C.I.L (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.



Contactez-nous

Réagissez à cet article

Original de l'article mis en page : Protection des données personnelles : demande d'annulation du Privacy Shield – UFC-Que Choisir

Devenir délégué à la protection des données | CNIL



Comment devenir délégué à la protection des données (BPD ou DPO)

Le délégué à la protection des données (D.P.D.) ou Data Protection Officer (D.P.O.) est au cœur du nouveau règlement européen. Les lignes directrices adoptées le 13 décembre 2016 par le G29, groupe des « CNIL » européennes, clarifient et illustrent d'exemples concrets le nouveau cadre juridique applicable en mai 2018 dans toute l'Europe.



Le règlement européen sur la protection des données pose les règles applicables à la désignation, à la fonction et aux missions du délégué, sous peine de sanctions.

Les lignes directrices du G29 ont pour objectif d'accompagner les responsables de traitement et les sous-traitants dans la mise en place de la fonction de délégué ainsi que d'assister ces délégués dans l'exercice de leurs missions. Elles contiennent des recommandations et des bonnes pratiques permettant aux professionnels de se préparer et de mettre en œuvre leurs obligations avec flexibilité et pragmatisme.

A retenir

Le délégué est chargé de mettre en œuvre la conformité au règlement européen sur la protection des données au sein de l'organisme qui l'a désigné. Sa désignation est obligatoire dans certains cas. Un délégué, interne ou externe, peut être désigné pour plusieurs organismes sous conditions.

Pour garantir l'effectivité de ses missions, le délégué :

- doit disposer de qualités professionnelles et de connaissances spécifiques,
- doit bénéficier de moyens matériels et organisationnels, des ressources et du positionnement lui permettant d'exercer ses missions.

La mise en place de la fonction de délégué nécessite d'être anticipée et organisée dès aujourd'hui, afin d'être prêt en mai 2018.

Dans quels cas un organisme doit-il obligatoirement désigner un délégué à la protection des données ?

La désignation d'un délégué est obligatoire pour :

1. Les autorités ou les organismes publics,
2. Les organismes dont les activités de base les amènent à réaliser un suivi régulier et systématique des personnes à grande échelle,
3. Les organismes dont les activités de base les amènent à traiter à grande échelle des données dites « sensibles » ou relatives à des condamnations.

En dehors des cas de désignation obligatoire, la désignation d'un délégué à la protection des données est encouragée par les membres du G29. Elle permet en effet de confier à un expert l'identification et la coordination des actions à mener en matière de protection des données personnelles.

Les organismes peuvent désigner un délégué interne ou externe à leur structure. Le délégué à la protection des données peut par ailleurs être mutualisé c'est-à-dire désigné pour plusieurs organismes sous certaines conditions. Par exemple, lorsqu'un délégué est désigné pour un groupe d'entreprises, il doit être facilement joignable à partir de chaque lieu d'établissement. Il doit en effet être en mesure de communiquer efficacement avec les personnes concernées et de coopérer avec l'autorité de contrôle.

Les lignes directrices du G29 clarifient les critères posés par le règlement, notamment les notions d'autorité ou d'organisme public, d'activités de base, de grande échelle et de suivi régulier et systématique.

Qui peut être délégué à la protection des données ?

Le délégué est désigné sur la base de ses qualités professionnelles et de sa capacité à accomplir ses missions.

Le délégué doit posséder des connaissances spécialisées de la législation et des pratiques en matière de protection des données. Une connaissance du secteur d'activité et de l'organisme pour lequel il est désigné est également recommandée. Il doit enfin disposer de qualités personnelles, et d'un positionnement lui donnant la capacité d'exercer ses missions en toute indépendance.

Les lignes directrices du G29 précisent le niveau d'expertise, les qualités professionnelles et les capacités du délégué.

Les personnes désignées en tant que correspondant Informatique et Libertés (CIL) ont vocation à devenir délégués à la protection des données en 2018. Toutefois, la qualité de CIL n'ouvrira pas automatiquement droit à celle de délégué à la protection des données. Les organismes ayant désigné un CIL indiqueront à la CNIL en 2018 si leur CIL deviendra délégué à la protection des données, selon des modalités précisées ultérieurement.

Quelles sont les missions du délégué à la protection des données ?

« Chef d'orchestre » de la conformité en matière de protection des données au sein de son organisme, le délégué à la protection des données est principalement chargé :

- d'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que leurs employés ;
- de contrôler le respect du règlement et du droit national en matière de protection des données ;
- de conseiller l'organisme sur la réalisation d'une analyse d'impact relative à la protection des données et d'en vérifier l'exécution ;
- de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

Les lignes directrices détaillent le rôle du délégué en matière de contrôle, d'analyse d'impact et de tenue du registre des activités de traitement.

Elles indiquent que le délégué n'est pas personnellement responsable en cas de non-conformité de son organisme avec le règlement.

Quels sont les moyens d'action du délégué à la protection des données ?

Le délégué doit bénéficier du soutien de l'organisme qui le désigne. L'organisme devra en particulier :

- s'assurer de son implication dans toutes les questions relatives à la protection des données (exemple : communication interne et externe sur sa désignation)
- lui fournir les ressources nécessaires à la réalisation de ses tâches (exemples : formation, temps nécessaire, ressources financières, équipe)
- lui permettre d'agir de manière indépendante (exemples : positionnement hiérarchique adéquat, absence de sanction pour l'exercice de ses missions)
- lui faciliter l'accès aux données et aux opérations de traitement (exemple : accès facilité aux autres services de l'organisme)
- veiller à l'absence de conflit d'intérêts.

Les lignes directrices fournissent des exemples concrets et opérationnels des ressources nécessaires à adapter selon la taille, la structure et l'activité de l'organisme. S'agissant du conflit d'intérêts, le délégué ne peut occuper des fonctions, au sein de l'organisme, qui le conduise à déterminer les finalités et les moyens d'un traitement (ne pas être juge et partie). L'existence d'un conflit d'intérêt est appréciée au cas par cas. Les lignes directrices indiquent les fonctions qui, en règle générale, sont susceptibles de conduire à une situation de conflit d'intérêts.

Comment organiser la fonction de délégué à la protection des données ?

En vue de la préparation à la fonction de délégué, il est recommandé de :

- s'approprier les nouvelles obligations imposées par le règlement européen, en s'appuyant notamment sur les lignes directrices du G29.
- confier au CIL ou au futur délégué les missions suivantes :
 - réaliser l'inventaire des traitements de données personnelles mis en œuvre ;
 - évaluer ses pratiques et mettre en place des procédures (audits, privacy by design, notification des violations de données, gestion des réclamations et des plaintes, etc.) ;
 - identifier les risques associés aux opérations de traitement ;
 - établir une politique de protection des données personnelles ;
 - sensibiliser les opérationnels et la direction sur les nouvelles obligations.

Lignes directrices du G29

> Guidelines on Data Protection Officers ('DPOs')

> WP243 ANNEX – Frequently asked questions

La version française de ces documents sera disponible début 2017.

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 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>



Denis JACOPINI est Expert Judiciaire en Informatique

spécialisé en « Sécurité », « Cybercriminalité » et en

protection des « Données à Caractère Personnel ».

▪ Audit Sécurité (ISO 27005) ;

▪ Expertise technique et judiciaire (Avis

techniques, recherche de preuves téléphones,

disques durs, emails, conteneurs, débroulements

de clientèle...);

▪ Expertise de systèmes de vote électronique ;

▪ Formations et conférences en cybercriminalité ;

(Autorisation de la DCTRI n°93 84 03041 84)

▪ Formation de C.I.L. (Correspondants Informatique

et Libertés) ;

▪ Accompagnement à la mise en conformité CNIL de

votre établissement.

Publication de contenus à caractère privé sur internet : La Cdp condamne et agite des sanctions



La Commission de protection des données personnelles (Cdp) condamne fermement, à travers un communiqué, la publication de vidéos, de photos et d'enregistrements audio notée ces derniers temps sur les réseaux sociaux et les sites d'information en ligne...[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** sur la mise en conformité CNIL, des formations sur la protection des données Personnelles et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les

décideurs et les utilisateurs aux **obligations et moyens de se mettre en conformité avec le RGPD**, futur règlement européen relatif à la Protection des Données Personnelles (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Plus d'informations sur notre page formations.



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

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



[Contactez-nous](#)

Réagissez à cet article

La CNIL qui est censée protéger nos données informatiques fait elle assez

de contrôles ?



...[Lire la suite]

Denis JACOPINI anime des **conférences, des formations** sur la mise en conformité CNIL, des formations sur la protection des données Personnelles et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **obligations et moyens de se mettre en conformité avec le RGPD, futur règlement européen relatif à la Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Plus d'informations sur notre page formations.



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

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



[Contactez-nous](#)

Réagissez à cet article

La Cnil s'énerve contre Brandvalley mais la sanction est faible

The screenshot shows the BrandAlley website interface. At the top, there's a search bar with 'Je cherche un article, une marque' and an 'OK' button. To the right, there are links for 'Aide', 'Mon compte', and 'Mon Panier (0)'. A red box highlights '1 ami partenaire | 10€ OFFERTS'. Below the header, a navigation menu includes 'SOLDES', 'MARCUES', 'FEMME', 'HOMME', 'ENFANT', 'LINGERIE', 'BEAUTÉ', 'MAISON', and 'LE LAB'. A breadcrumb path 'Accueil > Femme > Prêt-à-porter: Vests/Tailleur' is shown. On the left, a sidebar for 'FEMME' lists categories like 'Toutes les collections', 'Printemps-Eté 2016', 'Automne-Hiver 2016', and 'Outlet (jusqu'à -70%)'. It also shows a list of product types such as Chaussures, Accessoires, Casques moto, Ecriture / Agendas, Parapluies, Cadres, Insolites, Accessoires Chaussures, Sport, Prêt-à-porter, Robes, Blousons/Manteaux, Vests/Tailleur, Vests, Vests paletots, Trenches/Bouées, Chemises, T-shirts, Jeans, Shorts/Bermudas, Jupes. A large banner on the left says '3ème démarque SOLDES Jusqu'à -80%' with a green leaf icon. The main content area displays a grid of women's jackets with labels '3ÈME démarque' and price tags like '14.40€', '87.26€', and '40.05€'. A large orange text overlay on the right reads: 'La Cnil énerve contre Brandvalley mais la sanction est faible'.

La Cnil a dressé un constat sévère de l'irrespect de la loi Informatique et Libertés par le site de ventes privées BrandValley, spécialisé dans les grandes marques. Mais le site qui génère environ 300 millions d'euros de chiffre d'affaires n'a été condamné qu'à 30 000 euros d'amende....[Lire la suite]

Denis JACOPINI anime des **conférences**, des **formations** sur la mise en conformité CNIL, des formations sur la protection des données Personnelles et est régulièrement invité à des **tables rondes en France et à l'étranger** pour sensibiliser les décideurs et les utilisateurs aux **obligations et moyens de se mettre en conformité avec le RGPD, futur règlement européen relatif à la Protection des Données Personnelles** (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84).

Plus d'informations sur notre page formations.



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

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



[Contactez-nous](#)

Réagissez à cet article

L'essentiel Online – La surveillance au travail pourrait être modifiée – Luxembourg



La
surveillance
au travail
pourrait
etre
modifiée

Les députés se sont penchés lundi sur le nouveau cadre concernant la protection des données au Grand-Duché.

Un patron pourrait bientôt ne plus avoir besoin de demander une autorisation préalable à la Commission nationale pour la protection des données (CNPD) avant de placer ses employés sous vidéosurveillance au travail. Cette mesure fait partie d'un projet de loi concernant la protection des données privées que les députés ont commencé à étudier lundi et qui s'inscrit dans le nouveau règlement européen qui entrera en vigueur le 25 mai 2018.

Le texte supprime la liste de traitement des données qui est aujourd'hui soumis à autorisation préalable de la CNPD, dont les traitements effectués à fin de surveillance. La CNPD fera, selon le projet de loi, des contrôles a posteriori, dans un but de simplification administrative. Un changement qui a suscité l'inquiétude de plusieurs députés, soucieux de protéger les citoyens d'une surveillance illégale par leurs employeurs.

La Chambre des salariés avait émis un avis défavorable en novembre, «dénonçant d'emblée la suppression de l'autorisation préalable (...). Elle s'oppose plus particulièrement, et de manière formelle, à cette exemption en faveur des traitements à des fins de surveillance sur le lieu de travail», expliquant que la loi actuelle, de 2002, «traduisait justement la volonté expresse du législateur luxembourgeois de protéger les personnes physiques de certains traitements « susceptibles de présenter des risques particuliers au regard des droits et libertés des personnes concernées »». À noter que le projet de loi introduit également des sanctions financières.

(JW/JV/L'essentiel)

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 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>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Ce que les entreprises doivent savoir pour se mettre en conformité avec Règlement européen de protection des données en vigueur dans 18 mois



Ce que les entreprises doivent savoir pour se mettre en conformité avec Règlement européen de protection des données en vigueur dans 18 mois

Entré en vigueur en mai 2016, le RGPD (Règlement général sur la protection des données) modifie les règles de gestion des données à caractère personnel dans les entreprises. Fin mai 2018, toutes les organisations devront être en conformité. Il vous reste donc moins de 18 mois pour mener ce chantier.

Qui est concerné?

Le RGPD s'applique « au traitement de données à caractère personnel, automatisé en tout ou en partie, ainsi qu'au traitement non automatisé de données à caractère personnel contenues ou appelées à figurer dans un fichier. » Ce règlement s'applique à toute structure (responsable de traitement des données ou sous-traitant) ayant un établissement dans l'Union européenne ou bien proposant une offre de biens ou de services visant les personnes qui se trouvent sur le territoire de l'Union européenne. Les actions de profilage visant cette cible sont également concernées. Ainsi, alors que la loi Informatique et libertés se basait sur des critères d'établissement et de moyens de traitement, le règlement européen 16-679 introduit la notion de ciblage: le critère principal d'application est désormais le traitement des données d'une personne se trouvant au sein de l'UE.

Qu'est-ce qu'une donnée à caractère personnel?

L'une des difficultés posées par le RGPD va consister à définir les données personnelles concernées. Le règlement stipule qu'il s'agit de « toute information concernant une personne physique identifiée ou identifiable », directement ou indirectement. Des données indirectement identifiantes, telles qu'un numéro de téléphone, ou un identifiant, sont donc concernées. De même, les données comportementales collectées sur Internet (notamment recueillies dans le cadre d'actions marketing de profilage), si elles sont corrélées à une identité, deviennent des données à caractère personnel. Selon le traitement appliqué aux données, des informations non identifiantes peuvent ainsi devenir identifiantes, par croisement des informations collectées. À noter, le RGPD prévoit des exceptions selon les traitements concernés, notamment au niveau des traitements de données RH (recrutement, contrat de travail...), pour lesquels les États membres peuvent prévoir « des règles plus spécifiques pour assurer la protection des droits et libertés » (article 88).

Quelles obligations pour les entreprises?

La loi Informatique et libertés se basait sur du déclaratif initial et des contrôles ponctuels. Le nouveau règlement européen remplace cette obligation de déclaration par une obligation de prouver à chaque moment que l'entreprise protège les données. Dès lors, la structuration même des outils permettant la collecte des données (CRM, DMP, solutions de tracking ou de géolocalisation...), mais aussi les contrats passés avec les sous-traitants et clients sont impactés. « Le règlement couple des notions techniques et juridiques », souligne Thomas Beaugrand, avocat au sein du cabinet Staub & Associés. Il introduit des nouveaux principes et concepts qui renvoient désormais vers plus de précautions techniques. Par ailleurs, les entreprises ont, entre autres, l'obligation de donner la finalité précise de la collecte des données (il s'agit du principe de minimisation, un des grands principes de la dataprotection, qui impose que seules les données nécessaires à la finalité poursuivie pourront être collectées).

Le GRPD impose également le principe de conservation limitée des données, ainsi que celui de coresponsabilité des sous-traitants et des entreprises en matière de protection de la data, qui permet de distribuer les responsabilités en fonction de la mainmise de chacun sur les données.

Enfin, parmi les changements majeurs, la nomination d'un DPO, ou délégué à la protection des données, qui sera obligatoire dans tout le secteur public, ainsi que dans les structures privées qui font des traitements de données exigeant un suivi régulier et systématique des personnes à grande échelle (dans le secteur du marketing, notamment). Il sera le garant de la conformité au règlement (voir encadré en page suivante)...[lire la suite]

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 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>



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité », « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRIER n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Original de l'article mis en page : Règlement européen de protection des données: les nouvelles règles de gestion des données

Piratage de ses comptes de réseaux sociaux. Comment réagir ?

 <p>Denis JACOPINI vous informe LCI</p>	<p>Piratage de ses comptes de réseaux sociaux. Comment réagir ?</p>
---	---

Décret relatif au vote par voie électronique pour l'élection des délégués du personnel et des représentants du personnel au comité d'entreprise.

Le décret n° 2016-1676 du 5 décembre 2016 relatif au vote par voie électronique pour l'élection des délégués du personnel et des représentants du personnel au comité d'entreprise est publié au Journal Officiel du 6 décembre 2016. Il modifie le code du travail.

A retenir (DILA) : « le décret précise les modalités du vote électronique pour les élections des délégués du personnel et du comité d'entreprise prévues en l'absence d'accord. »

Consulter le décret n° 2016-1676 sur Legifrance :

<https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033538273&dateTexte=&categorieLien=id>
[block id="24761" title="Pied de page HAUT"]

A Lire aussi :

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

3 points à retenir pour vos élections par Vote électronique

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

Modalités de recours au vote électronique pour les Entreprises

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

Dispositif de vote électronique : que faire ?

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

Notre sélection d'articles sur le vote électronique

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



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

• Expert en Informatique assermenté et indépendant ;

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

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

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

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

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

Son expérience dans l'expertise de systèmes de votes électroniques, son indépendance et sa qualification en sécurité Informatique (ISO 27005 et cybercriminalité) vous apporte l'assurance d'une qualité dans ses 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

Alerte Que Choisir sur les jouets connectés et nos

données personnelles



A l'approche de Noël et face à la multiplication des offres de jouets connectés pour enfants dans les rayons de magasins ou sur Internet, l'UFC-Que Choisir dénonce aujourd'hui, sur la base d'une analyse technique, des lacunes quant à la sécurité et la protection des données personnelles des enfants utilisateurs de la poupée connectée 'Mon amie Cayla' et du robot connecté 'i-Que' disponibles chez de nombreux vendeurs en France.

Sur la base de ces inquiétants constats, l'association saisit la CNIL et la DGCCRF.



L'étude technique commanditée par notre homologue norvégien, Forbrukerradet, souligne que Cayla et i-Que, en apparence inoffensifs, ne garantissent pas le respect de la vie privée et de la sécurité des données personnelles de vos enfants.

Faile de sécurité du Bluetooth intégré

Ces jouets disposent d'un microphone intégré qui se connecte par Bluetooth à une application mobile, préalablement téléchargée par l'utilisateur sur son smartphone ou sa tablette. Le jouet peut alors comprendre ce que lui dit l'enfant et y répondre. Mais, les sociétés fabricantes, ont fait le choix d'implanter dans Cayla et i-Que, une technologie Bluetooth sujette à des risques de failles de sécurité élevées. En effet, si les sociétés ont fait le choix d'une connexion simple et rapide, aucun code d'accès ou procédure d'association entre ces jouets et les téléphones/tablettes n'est exigé avant la connexion au jouet, ce qui garantirait pourtant que seul le propriétaire puisse s'y connecter. Résultat : un tiers situé à 20 mètres du jouet peut s'y connecter par Bluetooth et entendre ce que dit votre enfant à sa poupée ou à son robot, sans même que vous en soyez averti. La connexion peut même se faire à travers une fenêtre ou un mur en béton et le nom du Bluetooth, « Cayla » et « i-Que », permet très simplement d'identifier les poupées. Plus grave encore... Un tiers peut prendre le contrôle des jouets, et, en plus d'entendre votre enfant, communiquer avec lui à travers la voix du jouet.

Conditions contractuelles et utilisation des données personnelles

La protection des données personnelles des utilisateurs français est prévue par la loi Informatique et Libertés mais semble avoir été oubliée par les sociétés fabricantes.

Les conditions contractuelles les autorisent, sans consentement express, à collecter les données vocales enregistrées par Cayla et i-Que, et ce, pour des raisons étrangères au strict fonctionnement du service. Ces données peuvent ensuite être transmises, notamment à des fins commerciales, à des tiers non identifiés. Les données sont aussi transférées hors de l'Union européenne, sans le consentement des parents: « aux Etats-Unis, ou vers les autres territoires concernés où les lois sur la protection de la vie privée ne sont peut-être pas aussi complètes que celles du pays où vous résidez et/ou dont vous êtes ressortissant»!

Matraquage publicitaire ciblé

Les sociétés fabricantes n'hésitent pas à faire de la publicité ciblée à destination de vos enfants. Les conditions contractuelles supposent que le simple fait de visualiser une publicité ciblée, constitue de votre part, un accord express à recevoir de telles publicités ciblées. L'étude a ainsi révélé que Cayla et i-Que prononcent régulièrement des phrases préprogrammées, faisant la promotion de certains produits – notamment des produits Disney ou des références aux dessins animés de Nickelodeon.

Loin d'être des cas isolés, Cayla et i-Que reflètent un problème général de sécurité et de données personnelles des jouets connectés. En effet, l'étude commanditée par nos homologues norvégiens souligne que la poupée Hello Barbie (*pas encore commercialisée en France*) est sujette aux mêmes griefs.

Au vu de ces éléments inquiétants, l'UFC-Que Choisir:

- appelle les parents à réfléchir à deux fois avant d'acheter la poupée Cayla et le robot i-Que ; rappelle qu'en cas de vente à distance, ils bénéficient d'un délai de rétractation de 14 jours. Pour ceux déjà équipés et qui souhaitent le conserver, l'association les invite à n'utiliser le jouet connecté qu'en leur présence, ou à défaut de l'éteindre.
- saisit d'une part la CNIL pour qu'elle diligente sans délai un contrôle du respect de la protection des données personnelles des utilisateurs de la poupée Cayla et du robot i-Que, et d'autre part, la DGCCRF afin que ses services enquêtent sur le niveau de sécurité des jouets connectés et sanctionnent tout manquement aux dispositions légales et réglementaires.

Notre métier : Nous réalisons des audits sécurité, nous vous apprenons par des formations ou des conférences, comment vous protéger des pirates informatiques. Nous vous accompagnons également dans votre mise en conformité avec le Règlement Européen sur la Protection des Données Personnelles. Audits sécurité, animations de formations en cybercriminalité et accompagnement à la mise en conformité avec le règlement sur la protection des données personnelles. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84) Denis JACOPINI réalise des audits et anime dans toute le France et à l'étranger des formations, des conférences et des tables rondes pour sensibiliser les décideurs et les utilisateurs aux risques liés à la Cybercriminalité et à la protection de leurs données personnelles. Enfin, nous vous accompagnons dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.

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



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

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

Original de l'article mis en page : Jouets connectés et données personnelles – UFC-Que Choisir