Le mercredi 25 janvier 2017 l'AFCDP (Association Française des Correspondants à la protection des Données à caractère Personnel www.afcdp.net) organise la 11e Université des CIL, l'événement incontournable des professionnels de la conformité à la loi Informatique et Libertés, à la Maison de la Chimie, à Paris.

Adhérent AFCDP (à jour de leur cotisation, sans condition d'ancienneté, exclusivement sur inscription via AGORA AFCDP) : contribution de 80 € nets.
Non-Adhérent : contribution de 550 € nets. Places en nombre limité.

Cette manifestation bénéficie du soutien des sociétés ISEP Formation Continue, Cabinet Cilex, HSC by Deloitte, Ageris, DPM, CIL Consulting, Devoteam, DPMS, Squire Patton Boggs, BRM Avocats, Actecil. Le programme est susceptible de subir quelques modifications dont seraient informées au préalable les personnes inscrites.

11e UNIVERSITE AFCDP DES CIL – Mercredi 25 janvier 2017

CIL, futurs Délégués à la protection des données/DPO, l'AFCDP vous accompagne !

PROGRAMME - MATINEE – PLENIERE

(Prise de parole 9h00) Ouverture de la conférence par **Paul-Olivier GIBERT**, Président de l'AFCDP

À la merci du Big data ? Comment vivre dans un monde où les objets en savent plus sur nous que nous-mêmes ?

Serge TISSERON, Psychiatre, docteur en psychologie - Université Paris VII Denis Diderot

Il a réalisé sa thèse de médecine sous la forme d'une bande dessinée (1975), puis découvert le secret de la famille de Hergé uniquement à partir de la lecture des albums de Tintin (1983). Il a reçu en 2013, à Washington, un Award du FOSI (Family Online Safety Institute) « For Outstanding Achievement » pour l'ensemble de ses travaux sur la famille, les enfants et Internet. Il est coauteur de l'avis de l'Académie des sciences « L'enfant et les écrans ». Son dernier livre : Le jour où mon robot m'aimera ».

Loi pour une République numérique : quels impacts pour les CIL ?

Interview de M. **Luc BELOT**, Député du Maine-et-Loire (PS), rapporteur pour la commission des lois de l'Assemblée nationale par Me **Martine RICOUART MAILLET**, Vice-présidente de l'AFCDP

La loi pour une République numérique introduit plusieurs nouveautés majeures dans la loi Informatique et Libertés : avenir des données relatives aux personnes décédées, augmentation du quantum de sanction que peut infliger la CNIL, création d'un droit à la portabilité... Comment les intégrer, en pleine phase de préparation au règlement européen ?

Le *Privacy Shield* répond-t-il aux attentes ?

Jan Philipp ALBRECHT, Député au Parlement européen, Vice-président de la Commission des libertés civiles, de la justice et des affaires intérieures (LIBE) – Interview vidéo

Homme politique franco-allemand, membre de l'Alliance 90 / Les Verts, grand spécialiste des questions de liberté civile et de droit dans le monde numérique, Vice-président de la Commission LIBE, Jan Philipp ALBRECHT était le rapporteur, pour la Commission européenne, du projet de Règlement européen.

Règlement – Plus que 485 jours – Comment s'y préparer ?

Table ronde animée par **Albine VINCENT**, Chef du service des Correspondants Informatique et Libertés, CNIL, avec **Michel RIME**, CIL du Groupe Argosyn, **Virginie LANGLET**, CIL du Département des Alpes-Maritimes, **Michel BAZET**, CIL d'AG2R La Mondiale

Même pour un CIL expérimenté, les nouveautés introduites par le règlement européen représentent un changement de paradigme. Nombreux sont les chantiers, avec des points tous plus prioritaires les uns que les autres. Comment s'y prendre ? Par quoi commencer ? Quelle planification ? Peut-on se permettre quelques « impasses » ? Quelles erreurs ne pas commettre ?

Intervention d'Edouard GEFFRAY, Secrétaire général de la CNIL

Un an et quatre mois nous séparent encore de l'application du règlement européen 2016/679. Comment l'autorité de contrôle se prépare—t-elle à cette échéance ? Quel est sa « vision » du Délégué à la protection des données et de l'évolution des CIL vers cette fonction clé ? Qu'attend-t-elle d'eux ? Quels outils prévoit-elle de mettre à leur disposition ? La CNIL continuera-t-elle à dispenser des Ateliers ? Le service des CIL sera-t-il renforcé pour répondre aux nombreuses sollicitations ?

Cocktail « déjeunatoire »

APRES-MIDI : ATELIERS/FORUMS

(libre parcours) – De 14h10 à 17h45 (fin de la conférence)

Le Délégué à la protection des données responsable pénalement ? – Frédéric CONNES – Directeur juridique, HSC by Deloitte, Jean CHERIN, consultant juridique en sécurité de l'information, HSC by Deloitte

Contrairement au CIL, le Délégué à la protection des données pourrait-il, dans certaines situations, endosser une responsabilité pénale, civile, disciplinaire ? En cas d'analyse de conformité erronée ? En cas de manquement du Responsable de traitement à ses obligations ? Quelles précautions faudrait-il prendre ? Si cette analyse est confirmée, que doit faire un CIL qui ambitionne de se faire confirmer le 25 mai 2018 dans ses nouveaux habits de Délégué à la protection des données ? Et qu'en est-il des Délégués à la protection des données externes ? Pourraient-ils, eux aussi, être inquiétés ?

RSSI et DPO, le duo gagnant – Philippe SALAÜN – CIL de CNP Assurances et Dominique SOULIER, RSSI, membre du Clusif

Si l'AFCDP s'est penchée de longue date sur l'indispensable synergie entre CIL et RSSI (Les deux fonctions sont-elles compatibles ? Quels sont les projets qui se prêtent le mieux à une action commune ? Quels sont les éventuels points de divergence ou les difficultés ?), l'approche du Règlement européen a généré ou renforcé une appétence des experts de la sécurité pour la conformité. Le Clusif a récemment créé un groupe de réflexion à ce sujet, animé par Dominique Soulier. L'AFCDP a donc proposé au Clusif de comparer les deux visions et d'engager le débat.

e-Commerce et publicité en ligne : comment recueillir un consentement valide ? – Maxime JAILLET — Membre de la promotion 2015-2016 du Mastère spécialisé « Informatique et Libertés » de l'ISEP

Le règlement européen renforce les exigences entourant le consentement d'une personne préalablement au traitement de ses données, le responsable de traitement devant notamment être capable de prouver son recueil. Le consentement pouvant être perçu par certains comme une source de contrainte, quels arguments le CIL (et bientôt le Délégué à la Protection des Données) peut-il développer pour le promouvoir en interne ? En particulier, est-ce un moyen d'engager l'utilisateur dans une relation de confiance ? Permet-il de créer de la valeur économique ?

Information des personnes : qu'est-ce qui change avec le règlement ? – Marine AHUAT WOODGE– Juriste, Française des jeux

Le règlement renforce les exigences en termes d'information des personnes, et pas seulement dans le cadre des mentions d'information. Ainsi, suite à une demande de droit d'accès, le responsable de traitement pourrait être amené à communiquer les grandes lignes de l'accord passé entre lui et une autre entité, au titre de la co-responsabilité. Quelles sont les nouvelles règles ? Que faudra-t-il modifier par rapport aux mentions actuelles, quand et comment ? Comment assurer, simultanément, la clarté et la validité juridique ? Que faire dans le cas d'une application mobile ?

Quelles évolutions de la politique répressive de la CNIL ? – Karin KIEFER, Responsable du service des sanctions et du contentieux, CNIL

Le règlement européen et la loi pour une République numérique dote la CNIL de nouveaux pouvoirs en termes de sanctions. Quelles nouvelles opportunités pour les plaignants ? Quels risques pour les responsables de traitement ? Comment les autorités utiliseront-elles leurs nouveaux pouvoirs répressifs ? Quid d'un renforcement des opérations conjointes entre autorités de contrôle au niveau européen ?

Quelles nouvelles règles pour les sous-traitants ? – Patrice THILLIEZ, CIL et RSSI interne de GFI Informatique

Plusieurs des nouveautés apportées par le Règlement concernent les sous-traitants : quasi-obligation de désigner un Délégué à la protection des données, création de la notion de « co-responsabilité » qui va permettre à la CNIL de "répartir" ses sanctions entre le client et son sous-traitant (si elle estime que ce dernier porte une part de responsabilité)... Quelles actions peut/doit entreprendre dès aujourd'hui un sous-traitant pour être prêt aux nouvelles règles ? Quelles interactions entre les DPO du sous-traitant et du client ? Les sous-traitants ne devraient-ils d'ores et déjà désigner un CIL ?

Big data : quels impacts pour les personnes concernées ? — Florence BONNET, CIL Consulting

Les traitements qui mettent en œuvre un projet Big data seront-ils systématiquement soumis à une EIVP ? Comment mener une analyse des risques et une étude d'impact dans ces situations ? Est-ce que les Big Data sont compatibles avec les exigences du règlement européen (le consentement sera-t-il toujours nécessaire ? Comment assurer la sécurité des données dans une architecture Big Data ? Comment gérer la purge des données à l'expiration de leur durée de conservation ? Comment faire droit aux demandes d'exercice de droit d'accès des personnes quand les données sont conservées dans un Data Lake ou dé-dupliquées dans de multiples systèmes ? Comment gérer les accès et la traçabilité dans une infrastructure Big Data ? Le Data Protection by Design peut être La solution ? Sur quelles normes peut-on s'appuyer pour avoir une démarche de Privacy By Design ?

Une Charte de déontologie pour les Délégués à la protection des données ? – Christophe CHAMPOUSSIN, Consultant Informatique et Libertés, Laurent CARON, Avocat à la Cour

La déontologie (du grec deon, -ontos, ce qu'il faut faire, et logos, discours) est la science morale qui traite des devoirs à remplir. Une Charte de déontologie régit un mode d'exercice d'une profession en vue du respect d'une éthique, la conduite de ceux qui l'exercent, les rapports entre ceux-ci et les parties-prenantes (employeurs, publics, clients, etc.). L'entrée en vigueur prochaine du Règlement européen sur la protection des données à amené l'AFCDP à relancer les travaux de sa Commission Métier à ce sujet, afin de formaliser une Charte de déontologie du Délégué à la protection des données. De nombreuses questions se posent : Une charte unique peut-elle être envisagée, applicables aux DPO internes et externes ? Ce cadre serait-il contraignant ? Les professionnels « autres » (non désignés auprès d'une autorité de contrôle) pourraient-ils adhérer à une telle charte ? Les co-animateurs de ses travaux présentent les enjeux et les composantes de ce projet.

Label de protection des données personnelles : de la contrainte règlementaire à l'avantage concurrentiel ?

Arnaud BELLEIL, Directeur général adjoint, Cecurity

Articles 42 et 43 du règlement européen sur les données personnelles consacré à la certification, délivrance par la CNIL du premier label technologique : l'année 2016 marque-t-elle un nouveau départ pour les labels, certification et marque de protection de la vie privée ? Meilleur information du public, démarche qualité au sein des organismes candidats : le label semble disposer des meilleurs atouts pour devenir un dispositif essentiel des nouvelles approches de la conformité. Pour un responsable de traitement vertueux, il permet notamment de faire passer la protection des données du domaine de la contrainte réglementaire à celui de l'avantage concurrentiel. Pourtant, force est de constater que depuis l'apparition des premiers privacy seals à la fin des années 90 aux Etats-Unis, le bilan demeure bien en deçà des espérances. L'atelier sera l'occasion de faire un point d'étape sur les labels de protection de la vie privée en France et en Europe à un moment charnière et disposer ainsi des informations clés pour se préparer au mieux et investir efficacement.

Comment, très concrètement, fait un CIL pour obtenir un budget et des moyens ? — Marie EYMOND, CIL de Randstad France, Alexandre ELOY, CIL de GMF Assurances
Si les premiers CIL ont pu exercer sans budget propre et avec des moyens réduits, les exigences du règlement européen militent pour que soient affectés au Délégué à la protection des données les leviers qui lui permettront de mener à bien ses missions et d'être efficace. Mais comment s'y prendre, auprès de qui et quand ? Quels arguments utiliser ? Comment évaluer et justifier ses demandes ? Quels sont les composantes principales du budget d'un DPO ? Comment « donner du sens » aux dépenses ?

Analyse de risques : comment réconcilier CIL et RSSI ? — Nicolas SAMARCQ, DPM, Frédéric HAY, Straton IT
L'évaluation objective du risque imposée par le règlement européen nécessite de réconcilier les démarches « Top Down » du CIL et « Bottom Up » du RSSI. Les intervenants proposeront une méthodologie basée sur le retour d'expérience de leur solution, qui réconcilie et consolide automatiquement la cartographie des traitements effectuée par le CIL avec les informations d'infrastructure et d'usages scannées par la « box » de Straton IT.

Le CIL et la sécurité des données à caractère personnel : une vision synthétique des dispositifs techniques et organisationnels à mettre en œuvre — Denis VIROLE — AGERIS, Directeur de la formation
Conformément à l'article 34 de la Loi du 6 janvier 1978, à l'article 17 de la Directive européenne du 24 octobre 95 et à l'article 32 du Règlement européen du 14 avril 2016, le Responsable et le sous-traitant doivent mettre en œuvre les mesures organisationnelles et techniques appropriées (consécutives aux EIVP) afin de garantir un niveau de sécurité adapté aux risques. Le CIL (DPO) doit accompagner et conseiller le Responsable du Traitement et son sous-traitant sur les mesures à mettre en place. Cette fonction doit s'exercer en collaboration avec la fonction SSI. Cependant, un grand nombre de CIL à culture non technique se sent en difficulté face à ce devoir de conseil et de contrôle. L'objectif de cet atelier est donc de donner les éléments nécessaires aux CIL afin d'améliorer le dialogue avec les acteurs à profil technique, internes ou sous-traitants. Afin de mieux appréhender la mise en œuvre du principe de sécurité ou de son contrôle, l'animateur vulgarisera et synthétisera dans une approche structurée et adaptée à des CIL non techniques, l'ensemble des mesures organisationnelles, techniques et architecturales concernant la protection des données à caractère personnel sur la sécurité des accès, des échanges, des serveurs et des « postes de travail ».

Télétravail : un catalyseur ou un inhibiteur de la porosité entre vie perso/vie pro ? — Bernard FORAY — Partenaire stratégique RH (triple compétence Sécurité informatique/Ressources Humaines/CIL)
Les TIC ont rendu perméable la frontière entre la vie personnelle et la vie professionnelle. La performance des outils de communication, la demande pressante d'être disponible en tout lieu et à tout heure, pour l'entreprise, pour ses proches et pour ses activités personnelles nous obligent à repenser la frontière entre les sphères pro et perso. Le télétravail, sans être un nouveau mode d'organisation du travail est-il un levier, pour nous aider à gérer nos différents temps de vie ? A l'heure de la loi El Khomri et de son droit à la déconnexion, ne devrions-nous pas considérer ce droit comme un devoir ? Le télétravail à domicile est-il intrusif ou est-ce notre vie personnelle qui fait irruption dans notre activité de télétravail ? Quel point d'équilibre trouver ? Comment éviter la confusion des lieux et distinguer les temps de vie ? Comment garantir la protection de la vie personnelle tout en augmentant la performance de l'entreprise ?

Profilage : quelles sont les nouvelles règles ? – Florence GAULLIER, Lorette DUBOIS, Avocates, Cabinet Gilles Vercken
Le règlement 2016/679 comporte plusieurs considérants et articles encadrant le profilage. De nombreuses questions se posent : qu'est-ce-que recouvre la notion de profilage ? Celui-ci est-il par principe permis ou interdit par le règlement ? Peut-on parler d' « opt-in » ou d' « opt-out » ? Peut-on poursuivre des intérêts légitimes en profilant des individus ? Faut-il systématiquement recourir à une analyse d'impact en présence d'un profilage ? Quelles obligations/vérifications complémentaires en cas de profilage ? Le futur Comité européen de la protection des données devra se saisir de ce sujet pour apporter aux praticiens, entreprises et institutions des éclaircissements et des éléments de réponse à certaines de ces questions. Dans l'attente de ces clarifications, les intervenantes proposent de sonder le règlement à la recherche des dispositions sur le profilage afin de formuler quelques conseils et pistes d'interprétation.

Une nouvelle réponse au problème de l'inventaire des traitements et du contrôle de conformité — Thierry BAHOUGNE, CIL de la Caisse des Dépôts et Consignations, Virginie BAREILLE, Chargée de mission auprès du CIL
La gestion de processus (ou Process management, management par les processus) décompose en différents stades de réalisation d'une opération complexe. Cette approche permet à chacun de se situer dans la masse gigantesque de tâches que l'entreprise réalise chaque jour, à chacun de connaître sa valeur ajoutée dans la réalisation d'une tâche, de responsabiliser l'ensemble des acteurs impliqués et de connaître les dysfonctionnements. Quelles sont les apports de cette démarche au regard de la conformité ? Comment définir les « verbes » (c'est-à-dire les traitements) et les données ? Comment modéliser le processus Informatique et Libertés, formaliser les logigrammes, affecter des symboles aux différents acteurs ?

Former et informer jusqu'au grand public : tel est le choix du CIL du CNRS — Nicolas CASTOLDI, CIL du CNRS
L'ampleur et la variété des activités du Centre national de la recherche scientifique ont impliqué la création de nombreux traitements de données personnelles, comme la gestion des utilisateurs d'une chimiothèque, une étude sur la formation des aversions alimentaires chez l'enfant ou une recherche sociologique sur les profils de carrière d'élus. Très tôt, le CIL désigné a mis à disposition du plus grand nombre, sur Internet, une base documentaire très riche dédiée à la thématique « Informatique et Libertés », allant jusqu'à publier des exemples caractéristiques des traitements de son registre ainsi que ses coordonnées et celles des membres de son équipe. M. Castoldi, également délégué général à la valorisation, conseiller juridique du président du CNRS, revient sur les raisons de cette démarche et ses apports, et décrit la structure « Informatique et Libertés » dont s'est doté l'organisme.

Du registre à une vision globale, avec pour objectif le « Label Gouvernance » — Jean-François VARIN, Directeur général, DPMS
Comment, à partir de la liste des traitements dans sa version actuelle, mettre en œuvre une démarche pour obtenir le label « Gouvernance Informatique et Libertés » et être en phase avec la mise en œuvre du règlement européen en se prévalant de l'Accountability ? L'intervenant proposera un plan de transition, en fera ressortir les avantages et identifiera les écueils à éviter et les clés du succès.

Quel avenir pour le *Privacy Shield* et les Clauses contractuelles ?— Stéphanie FABER, Avocat à la cour, Squire Patton Boggs
Le bouclier de protection des données UE-Etats-Unis, adopté en juillet 2016, va-t-il être remis en cause ? Cette modalité de protection des transferts vers les USA présente-t-elle une opportunité, ou au contraire un risque ? L'intervenante décrira les avancées du Privacy Shield par rapport au Safe Harbour, mais aussi les points de préoccupation qui demeurent et les prochaines étapes importantes, et fera un point sur la validité des clauses types... et toute surprise de dernière minute. Cet Atelier s'impose pour tout organisme concerné par les flux transfrontières.

CIL/DPO externe, CIL/DPO interne, même combat ? Regards croisés — Pierre-David VIGNOLLE, Martine RICOUART-MAILLET, BRM Avocats
Le règlement faisant disparaitre la limite des « 50 personnes », le nombre de Délégués à la protection des données externes va sans doute exploser. Si de multiples questions se posent aux DPO internes, les mêmes s'imposent aux DPO externes, souvent avec encore plus d'acuité. Mais d'autres questions, spécifiques aux intervenants externes, apparaissent : que devra faire un DPO externe, désigné à la fois pour un responsable de traitement et son sous-traitant ? Quelle devrait-être la durée du contrat ? Comment prévoir la fin de mission ? Comment gérer la transition de CIL externe à DPO externe ? Les intervenants – l'un CIL interne durant dix ans au sein de la SANEF, l'autre CIL externe au sein du cabinet BRM Avocats, partagent leurs expériences et décriront l'organisation à mettre en œuvre, côté Responsable de traitement, pour permettre au DPO externe de remplir efficacement ses missions.

Comment établir son registre ? Retour d'expérience - Yannis MURGUET, CIL de Smatis
L'établissement d'une cartographie des traitements de données personnelles est l'une des obligations faite au CIL, dans le cadre du décret n°2005-1309 du 20 octobre 2005. La liste des traitements, cet outil de conduite de changement, restera le pivot de la documentation qui devra être tenue sous l'empire du RGPD. Mais comment l'établir, en combien de temps et avec l'aide de quels acteurs ? Quel plan d'actions mettre en oeuvre et quels pièges éviter ? Quelle documentation y associer ? Combien de « fiches » un registre doit-il comporter, en moyenne ? Jusqu'à quel niveau de détails faut-il aller ? Qui peut y avoir accès ? Le CIL de Smatis France, basé à Angoulême, fait part de son expérience sur ces questions auxquelles tous les Correspondants Informatique et Libertés ont été confrontés.

Fin des Ateliers vers 17h45. Le programme est susceptible de subir quelques modifications dont seraient informées au préalable les personnes inscrites. Les participants sont informés qu'ils sont susceptibles de figurer sur des photographies (plan général de la salle) qui seraient prises à l'occasion de cette manifestation pour en illustrer le compte-rendu (publié sur le site de l'AFCDP ou par voie de Presse) et en acceptent le principe. Les supports de présentation utilisés lors de la conférence seront publiés au sein d'AGORA AFCDP quelques jours après la manifestation. Les opinions exprimées par les intervenants lors de la conférence ne sont pas celles de l'AFCDP.

Lieu : Maison de la Chimie, 28 Rue Saint Dominique, 75007 Paris

Cette manifestation bénéficie du soutien des sociétés ISEP Formation Continue, Cabinet Cilex, HSC by Deloitte, Ageris, DPM, CIL Consulting, Devoteam, DPMS, Squire Patton Boggs, BRM Avocats, Actecil.

Vous n'est pas encore membre AFCDP ? Téléchargez sans attendre votre demande d'adhésion disponible sur le site www.afcdp.net à la rubrique « Comment adhérer ? ».