Le mercredi 24 janvier 2018, l'AFCDP (Association Française des Correspondants à la protection des Données à caractère Personnel www.afcdp.net) organise la 12e Université des DPO, 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 CNP Assurances, Ageris Priv@cy, Squire Patton Boggs, Actecil, Digitemis, Devoteam, Mathias Avocats, Oxalia Data Protection, ISEP Formation Continue, Formind, DPO Consulting, DPM, Conscio Technologies, Œil pour Œil, BRM Avocats, Deloitte

12e UNIVERSITE AFCDP DES DPO – Mercredi 24 janvier 2018

Conférence placée sous le haut patronage de Monsieur Mounir MAHJOUBI, Secrétaire d'État chargé du Numérique

PROGRAMME - MATINEE – PLENIERE

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

Quel projet numérique pour la France ? Mounir MAHJOUBI, Secrétaire d'Etat au Numérique (sous réserve)

Entrepreneur engagé et ancien président du Conseil national du numérique, Mounir Mahjoubi est rattaché au premier ministre pour marquer le fait que le numérique est un sujet de transformation de la société, de l'économie et de l'administration. De nombreux chantiers sont devant lui : transition numérique des TPE/PME, investissements à réaliser dans l'intelligence artificielle, inclusion numérique, soutien aux start-ups du numérique… mais aussi passage au RGPD et renégociation du Privacy Shield. Rappelons qu'en mai 2017, le Président de la République déclarait « Nous devons d'abord savoir mener de vraies batailles face aux grands groupes de l'Internet et aux grands groupes américains. Les GAFA ne sont pas nos ennemis, mais nous ne devons pas être plus longtemps complaisants. (…) Si nous voulons défendre nos intérêts, protéger nos intérêts, la valorisation de nos données sur le plan européen, défendre nos concitoyens et le respect, par exemple, du secret des libertés individuelles, nous devons faire valoir nos préférences collectives européennes. On peut le faire en grand respect, en étant tout à fait amicaux mais en étant exigeants ».

Comment nos voisins allemands se préparent-ils au RGPD ? Tabea RIEDEL, Agent de la *Bayerisches Landesamt für Datenschutzaufsicht*

Madame Tabea Riedel est l'une des collaboratrices de M. Thomas Kranig, Président de l´autorité de surveillance de la protection des données bavaroise. Ayant fait une partie de ses études en Bretagne, c'est en français qu'elle nous expliquera comment la préparation au GDPR s'effectue très concrètement en Bavière.

La nouvelle jeunesse de la Loi Informatique et Libertés Interview de M. **Thomas ANDRIEU**, Directeur des affaires civiles et du sceau, Ministère de la Justice, par Me **Martine RICOUART MAILLET**, Vice-présidente de l'AFCDP

Si les dispositions du RGPD s'imposent sans transposition dès le 25 mai 2018, il était indispensable de revoir le contenu de la loi Informatique et Libertés pour y intégrer des points sur lesquels les Etats membres disposaient d'une marge de manœuvre, des précisions sur les missions de la CNIL ainsi que des spécificités nationales, issues principalement de la loi pour une République numérique. M. Andrieu nous dévoilera les coulisses des travaux préparatoires qui ont conduit au projet de loi.

L'heure tourne pour le règlement e-Privacy Rosa BARCELO, *Deputy Head of Unit (Cybersecurity and Digital Privacy)*, Commission européenne

La directive « Vie privée et communications électroniques » traite de nombreuses problématiques comme la confidentialité des informations, le traitement des données relatives au trafic, les spams et les cookies. Dans l'idéal, sa révision devait être finalisée pour entrer en application en même temps que le RGPD, car la cohérence et la sécurité sont essentielles pour les consommateurs et les entreprises. C'est pour cette raison que la Commission a opté pour un règlement, qui, une fois adopté par les institutions de l'UE, sera d'applicabilité directe dans l'ensemble des Etats membres.

Intervention d'Isabelle Falque-Pierrotin, Présidente du G29 et de la CNIL

À quelques semaines de l'application du RGPD, qu'attend l'autorité de contrôle des DPO ? Quels nouveaux outils prévoit-elle de mettre à leur disposition ? La CNIL continuera-t-elle à dispenser des Ateliers ? Le service des CIL… pardon, des Délégués à la protection des données, 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)

Comment la CNIL se prépare-t-elle au RGPD ? – Norbert FORT, CIL, CNIL, et Benjamin VIALLE, RSSI, CNIL
La CNIL met en œuvre, pour accomplir ses missions, des traitements de données à caractère personnel qui seront soumis au RGPD. Découvrez comment son CIL, également responsable « qualité-performance-risques », et son RSSI préparent ensemble la Commission à être en conformité le 25 mai 2018.

Analyse d'impact : comment adapter la démarche au degré de maturité de mon entreprise ? – Denis VIROLE – Directeur des services d'Ageris Group, Gérant de Virole Conseil Formation
Un grand nombre d'entreprises ont traité les risques qui pèsent sur leurs systèmes d'information par l'application de règles et de bonnes pratiques mises en œuvre par les informaticiens de manière quasi auto justifiée. Mais ces derniers sont peu habitués à conduire une analyse de risque orientée « métiers », graduée selon une échelle définie et endossée au final par la direction générale. Le DPO ne va-t-il pas rencontrer plusieurs difficultés pour faire appliquer la bonne méthode par l'ensemble des parties prenantes ? Faut-il suivre la démarche proposée par la CNIL de manière exhaustive ou faut-il adapter la méthode à son contexte ? Quels sont les pièges à éviter ? Jusqu'à quel niveau faut-il pousser l'analyse ? Comment formaliser les règles de protection ? Comment présenter les résultats de l'analyse au Responsable du Traitement afin qu'il puisse la valider en toute connaissance de cause ? Quelle répartition des tâches entre les acteurs concernés ? Comment intégrer la démarche EIVP dans la gestion de projets de manière coordonnée ? Afin de proposer une démarche pragmatique, l'animateur modélisera plusieurs scenarii, adaptés à la maturité de l'organisme et au type de traitement.

Smart city : source de progrès ou vie sous surveillance constante ? – Malika-Maud DUQUET, Membre de la 10 ème promotion du Mastère Spécialisé « Management et Protection des Données Personnelles » de l'ISEP
L'expression « ville intelligente » désigne une agglomération utilisant les technologies de l'information et de la communication pour « améliorer » la qualité des services urbains ou encore réduire leurs coûts. Outre les habitants et usagers, les parties prenantes sont nombreuses : collectivités, administrations concernés par l'aménagement du territoire et des villes, distributeurs d'énergie et d'eau, sociétés de transports, fournisseurs de réseaux télécoms, sociétés qui assurent la maintenance de l'infrastructure, etc. La smart city est aujourd'hui indissociable des objets connectés et s'appuie sur le traitement de nombreuses données personnelles des habitants. Or les « smart cities » ne seront sources de progrès que si elles sont des espaces de co-construction, avec des citoyens engagés et consentants… notamment aux traitements de leurs données à caractère personnel. Mais qui doit assurer la conformité globale des traitements mis en oeuvre au sein d'une smart city... et surtout comment ?

Quelle condition de licéité pour vos traitements ? Un choix cornélien… – Stéphanie FABER, Avocat à la cour, Squire Patton Boggs
Comme le faisait l'article 7 de la loi Informatique et Libertés de 2004, l'article 6 du RGPD liste les conditions dans lesquelles un traitement est licite (consentement, base légale, contrat, intérêt légitime, etc.). Avant de faire son choix – qui peut s'avérer crucial-, il faut bien réfléchir aux implications de chacune des pistes proposées, notamment en matière d'accès aux procédures constituant le « guichet unique » ou de droits des personnes concernées. Les conséquences opérationnelles sont plus importantes que soupçonnées et il est difficile de changer de fondement un fois le traitement mis en œuvre. De plus, le RGPD oblige à faire figurer « la base juridique du traitement » dans les informations qu'il faut porter à la connaissance des personnes concernées. L'intervenante, de façon très pragmatique, présentera de façon comparative et synthétique les caractéristiques, avantages et inconvénients de chaque option.

Traitements RH : quels impacts aura le RGPD sur les relations de travail ? – Mariana OPRIS et Aurélie HARVENT LAFFONT, Juristes Consultantes RGPD, Actecil Groupe
Le Règlement européen aura inévitablement des conséquences dans les relations de travail, d'autant que les traitements mis en œuvre dans le domaine RH sont nombreux et souvent sensibles (recrutement, évaluation, rémunération, formation, gestion des hauts potentiels, vote électronique, cybersurveillance, protection sociale…). Les DRH et leur DPO devront réfléchir à de nombreuses questions telles que : Qu'en est-il du droit à la portabilité des salariés ou du droit à l'oubli d'un ex-salarié ? Dans quels cas les RH peuvent-ils invoquer l'intérêt légitime pour justifier les traitements des données des salariés hors cadre contractuel ? Quels sont les traitements RH à risque pour lesquels une EIVP sera obligatoire ? Quelles sont les mesures organisationnelles à mettre en place pour faire face aux nouvelles obligations (ex. création d'un nouveau poste de DPO, actions de formations pour les salariés, création d'une culture entreprise autour de la protection de données) ? Quels impacts pour la gestion des salariés au sein de multinationales ? Faut-il anticiper des actions collectives en lien avec des litiges portant sur les données personnelles des salariés ?

Durées de conservation : la purge automatique des données nous sauvera-t-elle ? – Anne-Sophie CASAL, juriste protection des données personnelles, Pierre DEBARY, ingénieur cybersécurité, Digitemis
L'un des principes fondateur du RGPD - comme il l'était pour la directive de 1995 - dispose qu'une fois que l'objectif poursuivi par le traitement est atteint, il n'y a plus lieu de conserver les données et qu'elles doivent être supprimées. Si chacun connait la difficulté à définir la « bonne » durée de conservation des données, encore faut-il qu'un processus de purge ait été défini... et réellement mis en œuvre sur le terrain afin d'assurer l'effacement irrémédiable des informations traitées. Ce même processus peut-il être utilisé lors d'une demande de « droit à l'oubli » ou de demande de suppression ponctuelle ? Durant cette intervention, émaillée d'exemples pratiques et animée conjointement par une ancienne juriste de la CNIL et un ingénieur SSI, seront présentées les axes de réflexion à suivre pour se conformer aux durées de rétention règlementaires et contractuelles, combinant politique de suivi, de contrôle et de purge des traitements. Quelle organisation faut-il mettre en place ? Quelles techniques permettent de suivre efficacement le cycle de vie des données ? Quelles garanties suis-je en mesure de fournir aux autorités de contrôle ? Combien de temps faut-il consacrer à cette tâche récurrente ?

Privacy by Dx : mode d'emploi pour les entreprises – Johanna CARVAIS-PALUT, CIL, Groupe Malakoff Médéric, Administrateur de l'AFCDP
Privacy by Design et Privacy by Default, deux nouvelles obligations qui s'imposent aux responsables de traitement dans le cadre du RGPD, ont déjà fait couler beaucoup d'encre. Pourtant ces notions restent difficiles à appréhender, la seconde approche étant sans doute la moins facile à mettre en place. Découvrez comment le groupe Malakoff Médéric a choisi de donner vie à ces deux concepts. Des exemples illustreront concrètement la prise en compte de ces principes et devraient donner quelques pistes pour embarquer les autres directions en interne dans ce changement de paradigme.

Comment adapter le PIA aux secteurs Banque et Assurance ? – Matthieu GRALL, CNIL, Chef du Service Expertise technologique, Philippe SALAÜN, CIL/DPO de CNP Assurances, Secrétaire général de l'AFCDP, membre du Forum des Compétences

Paris

L'AFCDP a convié cette année le Forum des Compétences (focalisé sur les secteurs Banques et Assurances). Cette Association associe régulièrement les Autorités de contrôle (ACPR, ANSSI, Préfecture Police, et CNIL) à ses travaux pour faire avancer la réflexion au niveau de la Sécurité des SI de la Place Financière. Il s'agit ici de présenter comment mettre en place le Privacy Impact Assessment, nouvelle exigence du GDPR, au sein de ce type d'établissement considérant le fait que la Finance dispose déjà de méthode d'analyse de risques IT. Quelles organisations sont nécessaires ? Quels rôles et responsabilités du DPO et autres acteurs de la Sécurité sont à attribuer ? Quelles instances doivent être adaptées afin d'être efficace ? Quelles méthodes adaptées ? De nombreux cas de figures seront évoqués et pourront inspirer les adhérents à quelques mois du 25 mai 2018.

Cybersécurité et RGPD : trois cas réels à méditer – Mailys LEMAITRE, juriste &consultante protection des données, et Pierre D'HUY, expert cybersécurité, Devoteam
Ça n'arrive pas qu'aux autres. Une juriste spécialiste du droit de la protection des données et un expert en cybersécurité présentent trois cas bien réels – mais décrits de façon à préserver l'anonymat des entreprises concernées – qu'il est bon d'analyser : Quelle était la nature de l'évènement survenu ? Quelles ont été les conséquences compromettantes pour la cybersécurité ? Quelles solutions ont été retenues ? Quelles mesures ont été mises en place ? Quelles bonnes pratiques adopter pour ne pas vivre les mêmes cauchemars ? Une intervention qui couvrira aussi bien les aspects techniques et organisationnels que juridiques à l'aune du RGPD. Mots de passe facilement compromis, connexion risquée car non sécurisée ou encore accès presque libre à des données confidentielles, les cas couverts permettront de (re)démontrer tout l'intérêt d'implémenter les bonnes mesures de sécurité pour protéger efficacement les données.

Le consentement mis à nu – Andrea MARTELLETTI, CIL et Consultant protection et management des données à caractère personnel, Oxalia Data Protection
Le consentement est l'un des fondements possibles des traitements de données à caractère personnel. Qu'était-il, que sera-t-il avec le RGPD et comment le maîtriser ? Après avoir partagé sa vision sur ce qu'est le consentement, ses différentes modalités et montré des exemples concrets de recueil du consentement, l'intervenant présentera une étude comparative du consentement avant/après le RGPD. Les différents types de consentement prévus par le RGPD seront évoqués (classique, catégories particulières de données, prospection commerciale, cookies) ainsi que les différentes méthodes de gestion des consentements (exemples de clauses, dispositifs de recueil, gestion des retraits).

Blockchain : les enjeux de la confiance et de la conformité – Garance MATHIAS, Avocat fondateur, et Aline ALFER, Avocat, Mathias Avocats - Amandine KASHANI-POOR, CIL, Agence Française de Développement (AFD) juriste &consultante
Les applications utilisant la technologie blockchain peuvent impliquer le traitement des données à caractère personnel. Disruptive et vecteur d'innovations qui vont probablement révolutionner notre quotidien comme l'a fait Internet, cette technologie est-elle « compatible » avec le RGPD ? Ainsi, il convient de s'interroger sur l'identification du responsable du traitement : les concepteurs des applications de smart contrats pourraient-ils être ainsi qualifiés ? D'autres tiers le pourraient-ils ? Quels sont les impacts contractuels au regard de la protection des données à caractère personnel ? Comment assurer de manière opérationnelle que les droits des individus dont les données font l'objet d'un traitement seront respectés (information, consentement, droit d'accès, droit de rectification, etc.) ? Quid de la durée de conservation effective ? Des exemples permettront d'illustrer le propos, notamment dans le domaine de la santé.

Violations de données : comment les détecter et surtout les gérer ? – Elsa MOREL, CIL et Manager RGPD, Hervé MORIZOT, Associé fondateur du cabinet Formind Consulting
Avec le RGPD, les incidents de sécurité portant sur des données à caractère personnel sont fortement cadrés. Leur notification à la CNIL- si possible sous 72h - exige une détection quasi immédiate, de la part des sous-traitants et/ou du responsable de traitement, ce qui reste assez hypothétique. La présentation, basée sur des retours d'expérience concrets, éclairera les orientations des responsables de traitement sur deux volets essentiels : La détection des violations proprement dite et la gestion de crise. La présentation, très concrète sur les processus et solutions mises en œuvre ou en cours de déploiement, restera neutre vis-à-vis des fournisseurs de solutions, se concentrant sur le triptyque « problématique – approche – résultats ».

Les relations entre fournisseur et sous-traitant dans le cadre du RGPD - c'est tout un sketch ! – Isabelle CADIAU, Data Protection Legal Manager, Sanofi, Nathalie LANERET, Group DPO, Capgemini, Stéphanie FABER, Avocat à la cour, Squire Patton Boggs
Le RGDP opère une redéfinition des rôles et obligations respectifs des responsables de traitement et des sous-traitants. Sous l'aspect concret et ludique de petites scénettes, cet atelier a pour objectif de mettre en avant les problématiques rencontrées dans le cadre des négociations contractuelles entre ces acteurs qui doivent parvenir à trouver un équilibre acceptable pour chacun. Avec Isabelle Cadiau, dans le rôle du Responsable de traitement/Client), Nathalie Laneret dans le rôle du Sous-traitant/Fournisseur et Stéphanie Faber dans le rôle du narrateur.

Données post-mortem : des pratiques numériques à un régime juridique – Lucien CASTEX, Chercheur à l'Institut de recherche Médias, Cultures, Communication et Numérique, Université Sorbonne Nouvelle - Paris-III
La persistance des données numériques, après le décès des usagers, soulève aujourd'hui un certain nombre de questions. Que deviennent les données identitaires des usagers après leur décès ? S'en préoccupent-ils de leur vivant ? Comment sont-elles gérées par les proches ? Comment les acteurs du web, tels que Google ou Facebook, y font-ils face ? Lucien Castex, chercheur, clarifiera le régime juridique qui devrait s'appliquer aux données après la mort et présentera les résultats de recherche du projet ENEID (Eternité Numérique).

Open data : Quoi, quand, comment et pour qui ? – Sandrine MATHON, responsable du Domaine Ressources de la Direction du Numérique de la Ville de Toulouse et de la Communauté Urbaine
La donnée ouverte est une donnée numérique dont l'accès et l'usage sont laissés libres aux réutilisateurs. Elle peut être d'origine publique ou privée, produite notamment par une collectivité, un service public ou une entreprise. Elle est diffusée de manière structurée selon une méthode et une licence garantissant son libre accès et détaillant les modalités juridiques de réutilisation par tous notamment mais sans restriction technique ou financière. L'ouverture des données (open data) est à la fois un mouvement, une philosophie d'accès à l'information et une pratique de publication de données librement accessibles et exploitables. Elle s'inscrit dans une tendance qui considère l'information publique comme un bien commun dont la diffusion est d'intérêt public et général. En théorie, elle ne devrait contenir que très rarement des données à caractère personnel. De quelle façon un Délégué à la protection des données doit-il accompagner un projet d'Open data ?

Je viens d'être désigné CIL au sein d'un CHU : je commence par quoi ? – Moufid HAJJAR, Médecin DIM et CIL, CHU de Bordeaux, Administrateur de l'AFCDP
Les établissements de soins regorgent de données personnelles – dont des données dites « sensibles » - et présentent des spécificités. Dans un contexte contraint, quel est le « chemin » que doit emprunter un CIL nouvellement désigné et destiné à être confirmé dans ses missions en tant que DPO, pour entamer ses travaux, en évitant l'indigestion et la confrontation avec les directions métiers ? Quelles sont les erreurs à ne pas commettre ? Quel plan d'action adopter ?

e-Administration : la conformité comme gage de confiance – Flore BONHOMME, CIL de la Région Normandie
La dématérialisation des services administratifs, aussi bien ceux de l'Etat que des administrations ou des collectivités, participe de la qualité du service rendu au public. Elle nécessite cependant une grande rigueur, indispensable pour en assurer la conformité et la sécurité, facteurs indispensables de confiance. Les CIL - et bientôt les DPD - sont des acteurs majeurs de ces efforts, notamment dans les processus d'homologation Rgs (Référentiel général de sécurité). Les intervenants évoqueront des cas concrets faisant ressortir les apports d'un CIL et du futur DPD.

Comment rassurer les utilisateurs sur l'utilisation de leurs données personnelles ? – Ghita TAOUJNI, Directrice Marketing Numérique et Data de France Télévisions
Dans un contexte de montée inquiétante d'une société de surveillance et de sensibilité croissante des citoyens à la protection de leur vie privée, le groupe France Télévisions, qui voulait prolonger la relation de confiance avec son public à l'expérience numérique, a publié en 2014 une charte de la protection des données qui porte sur trois engagements fondamentaux : Transparence, Sécurité, Utilité. En 2017, un nouveau clip vidéo mettant en scène les célébrités des différentes chaines du service public est venu couronner un remarquable effort pour rendre les mentions informatique et libertés accessibles, complètes, claires et conviviales. Découvrez les dessous de cette démarche ambitieuse.

Synergie entre DPO et Archiviste – JOHAN VAN DAMME, DPO & RSSI et RAFFAELLA GUSTAPANE, Archiviste, Cour des Comptes européenne
Il semble naturel que DPO et Archiviste/Record Manager entretiennent d'étroites relations et coopèrent, ne serait-ce que sur la grande question des durées de conservation. Mais est-ce le seul sujet que ces deux professionnels ont en commun ? M. Van Damme et Mme Gustapane nous feront part de leur expérience, de leurs réalisations et réussites et donneront quelques clés pour une synergie mutuellement profitable.

Témoignage d'un DPO du secteur Banque – Antoine PICHOT, DPO de la Société Générale
La Société Générale a officialisé en octobre 2017 la nomination d'Antoine Pichot au poste de DPO, qui aura pour mission de veiller à la conformité du groupe avec le RGPD. Quelle gouvernance mettre en place ? Quelle organisation ? Quelles priorités ? Quel budget ? Quelles interactions avec le responsable de traitement et les directions Métiers ? Comment décliner les règles en fonction du contexte local et des différents métiers de la Banque ? Pour une grande banque comme Société Générale, avant d'être un enjeu de conformité, GDPR est un enjeu stratégique de relation client », prévient le nouveau DPO.

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 bis Rue Saint Dominique, 75007 Paris

Cette manifestation bénéficie du soutien des sociétés CNP Assurances, Ageris Priv@cy, Squire Patton Boggs, Actecil, Digitemis, Devoteam, Mathias Avocats, Oxalia Data Protection, ISEP Formation Continue, Formind, DPO Consulting, DPM, Conscio Technologies, Œil pour Œil, BRM Avocats, Deloitte