Communiqué de presse 27 janvier 2014

Données personnelles

Nette amélioration de l'Index AFCDP du Droit d'accès

A l'occasion de la journée mondiale de la vie privée l'AFCDP (Association Française des Correspondants à la protection des Données à caractère Personnel) publie son Index annuel du droit d'accès. Au titre de la loi Informatique & Libertés, chacun peut exercer un droit d'accès à ses données personnelles. La veille de sa conférence annuelle et dans le cadre de sa participation à l'initiative « *Education au Numérique, Grande cause nationale 2014* », l'AFCDP publie sa mesure de l'effectivité de ce droit. L'édition 2014 montre un net progrès.

41% des organismes sollicités ont fait une réponse conforme au droit. *Même s'il reste une marge de progression importante, cet indicateur montre* ***un net progrès*** *par rapport aux relevés des années précédentes (il était de 18% en 2010, lors de la 1ère édition).*

La journée européenne de la protection des données à caractère personnel est une initiative du Conseil de l'Europe, soutenue par la Commission européenne, qui a proclamé solennellement le 28 janvier de chaque année « journée de la protection des données à caractère personnel ». En 2009, les Etats-Unis et le Canada se sont joints à l'initiative, avec pour objectif de sensibiliser les citoyens à leurs droits pour promouvoir la protection de leurs données personnelles et le respect de leurs libertés et droits fondamentaux, et en particulier de leur vie privée.

C'est à cette occasion que l'association française représentative de la profession de CIL (Correspondant Informatique et Libertés) a dévoilé en janvier 2010 son tout premier « **Index AFCDP du Droit d'Accès** ».

L'association publie aujourd'hui la quatrième édition de cet Index, en partenariat avec la grande école ISEP (Institut Supérieur d'Electronique de Paris). Cet indicateur est basé sur les travaux effectués par les participants du Mastère Spécialisé « Management et Protection des Données à Caractère Personnel ». Dans le cadre de ce cursus, les participants – souvent des Correspondants Informatique et Libertés en poste ou de futur *Data Protection Officer* - mènent plusieurs projets, dont l'un consiste à exercer leur droit d'accès.

La promotion 2012-2013 **a ainsi sollicité 224 organismes, privés et publics** (contre 207, 226 et 198 les années précédentes).

Au titre de la loi dite « Informatique et Libertés » (article 39), toute personne justifiant de son identité a ainsi le droit d'interroger le responsable d'un fichier ou d'un traitement de données personnelles pour savoir s'il détient des informations sur elle, et le cas échéant d'en obtenir communication, et ceci sans avoir à fournir de justification.

Les étudiants ont exercé leur droit d'accès sur place et par courrier (électronique et postal) auprès d'organismes avec lesquels ils pensaient probable le fait que ceux-ci soient détenteurs de données personnelles les concernant et qui couvrent les différents aspects de la « vie

quotidienne d'un citoyen »: emploi/formation, logement, banques/ assurances, commerce, santé, sociétés de l'information & de la communication, administrations...

Si cet Index ne prétend pas être représentatif de l'ensemble des entreprises, il correspond toutefois aux organismes les plus fréquemment en contact avec le public. Dans sa nature, l'échantillon est raisonnablement comparable d'une année sur l'autre (mêmes secteurs d'activité) et la méthode mise en œuvre est identique.

L'AFCDP inscrit la publication de cet Index dans le cadre de sa participation à l'initiative pilotée par la CNIL « Education au Numérique : Grande cause nationale 2014 », les membres du collectif considérant qu'il y a urgence à diffuser une culture du numérique afin de permettre à chacun d'entre nous de devenir un citoyen numérique informé et responsable, capable de profiter des potentialités de cet univers et d'y exercer de manière effective ses droits et devoirs.

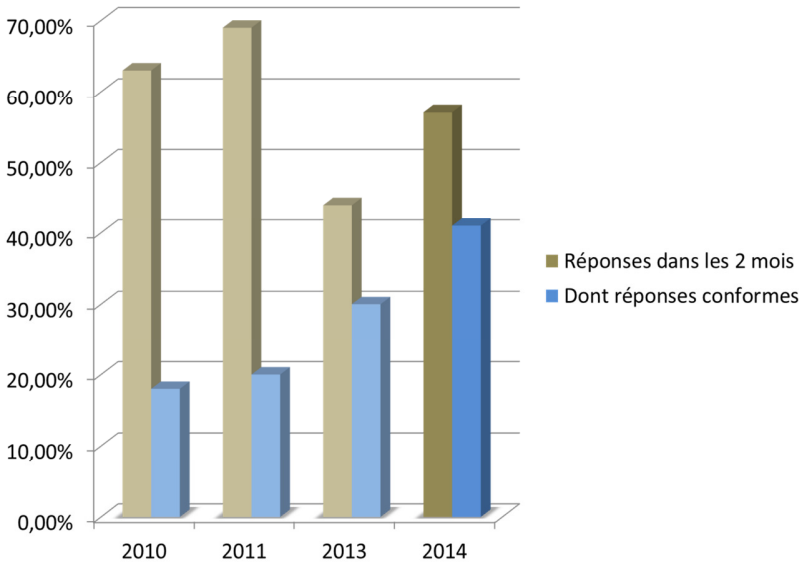
57% des entités testées ont répondu dans les deux mois :

Sur les 224 organismes contactés, **72% ont réagi**, ce qui marque une nette progression par rapport à l'année précédente et un retour sur les niveaux des Index précédents.

Mais « réagir » ne veut pas dire respecter ses obligations légales. En effet, pour être valide, la réponse doit parvenir en moins de deux mois, ce qui n'était pas le cas de 30 réponses.

Index AFCDP 2014 du droit d'accès : **57% des entités sollicitées ont répondu dans les deux mois impartis par le cadre légal** (en marron sur le graphique).

Seuls 1% des organismes sollicités demandent une contribution financière avec des montants de quelques euros (dans quelques cas la somme est annoncée pour couvrir les frais d'affranchissement, alors que la loi n'évoque la possibilité que de demander une participation aux frais de reproduction).



Davantage de réponses conformes à la loi Informatique et Libertés :

Cependant répondre dans les deux mois requis ne signifie pas non plus que cette réponse soit conforme. Les participants du Mastère Spécialisé « Informatique et Libertés » de l'ISEP ont donc jugé du **degré de conformité des réponses obtenues** dans les deux mois.

Au total, de l'avis des membres du Mastère Spécialisé, **41% des organismes sollicités ont fait une réponse conforme au droit**, jugée très satisfaisante ou totalement satisfaisante, dont le respect du délai de deux mois (en bleu sur le graphique). Cet indicateur montre **un clair progrès par rapport aux relevés des années précédentes** (passé de 18% en 2010 à 41% cette année).

Les « spécificités » de l'Index 2014

Les membres de la promotion ISEP 2012-2013 ont fait les constats suivants :

☹ Un demandeur a été menacé par l'entreprise sollicitée… son Correspondant Informatique et Libertés était fort mécontent d'être importuné et méconnaissant visiblement la loi Informatique et Libertés !

☹ Une grande banque ne trouve aucune donnée concernant… l'un de ses clients fidèle.

☹ Un magazine de la presse consumériste interprète à tort la demande comme faisant référence à un abonnement.

☹ Une très grande entreprise du CAC40 se contente d'envoyer quelques photocopies, sans aucune lettre d'accompagnement, mais avec une petite note anonyme comportant ce simple mot : « *Voilà !* »

☹ Un grand magasin, visiblement non préparé à ce genre d'exercice, met en copie le demandeur, qui assiste amusé aux échanges d'email internes, et aux multiples « rebonds » entre les différents services, dont aucun ne veut se saisir de la demande.

☹ Plusieurs hôpitaux ont fait la confusion avec des demandes d'accès au dossier médical – accès payant au titre d'une autre loi, celle du 4 mars 2002, dite "Kouchner", relative aux droits des malades et à la qualité du système de santé– … et se sont empressés de joindre une facture à leur envoi !

MAIS…

☺ Une banque (Le Crédit Agricole des Savoies) a communiqué le scoring et proposé de rembourser les frais postaux engagés par le demandeur.

☺ Le Secours Catholique a parfaitement répondu à la demande et indiqué spontanément la procédure à suivre pour bénéficier de la liste Robinson.

☺ Amazon Luxembourg adresse un courrier recommandé avec accusé de réception annonçant l'envoi d'un CD chiffré – ce courrier comprend les mots de passe pour accéder au dossier puis pour lire les fichiers. Le CD est également reçu en courrier recommandé avec accusé de réception.

Il a également été observé qu'en Pologne, pour limiter les demandes abusives, chaque personne concernée ne peut envoyer qu'une seule demande tous les six mois à un même responsable de traitement. L'Espagne a adopté un principe similaire, avec un intervalle de douze mois. En Belgique, le délai de réponse est de 45 jours, de 40 jours au Royaume-Uni, de 15 jours en Italie, de 4 semaines au Danemark (contre deux mois en France).

Si la proposition de règlement européen actuellement à l'étude à Bruxelles était adoptée dans sa forme actuelle, ce délai serait uniformément passé à un mois.

La Grèce, l'Espagne et la Suède imposent au responsable de traitement de communiquer

systématiquement l'origine des données traitées. Les responsables de traitement britannique et italiens peuvent demander une participation financière même si aucune donnée personnelle n'a été trouvée.

La promotion a également relevé plusieurs pratiques intéressantes utilisées par les entités testées pour vérifier l'identité du demandeur : Apple demande communication d'informations que seul le demandeur est sensé connaître, Amazon demande qu'un formulaire soit renseigné et lui soit retourné. A noter qu'au Royaume-Uni, la loi ne prévoit pas explicitement le besoin de vérifier l'identité du demandeur.

Sur le même sujet de la vérification d'identité du demandeur (il convient d'éviter de délivrer des données personnelles à des tiers non autorisés), la promotion s'est utilement penchée sur le cas spécifiques des demandes qui émanent des parents divorcés. Comment un responsable de traitement peut-il savoir si le demandeur a obtenu la responsabilité des enfants mineurs ?

Parmi les raisons des jugements négatifs portés par les « testeurs » on trouve : une totale incompréhension de leur demande; une absence de vérification de l'identité du demandeur ; la collecte de données non pertinentes ; la fourniture de données personnelles relatives à d'autres personnes ; des réponses incomplètes ou incompréhensibles; des durées de conservation non-adéquates avec la finalité du traitement.

Notons également à ce stade **la difficulté trop souvent éprouvée à trouver de l'information sur le site Web** des organismes pour exercer son droit d'accès.

Nombreux également sont les organismes dont les collaborateurs chargés de traiter ces demandes se montrent étonnés ou s'avouent incompétents sur ce sujet.

Rappelons qu'en avril 2009 la CNIL a prononcé une sanction pécuniaire de 7.000 euros rendue publique à l'encontre d'un fournisseur d'accès à internet qui n'avait répondu que partiellement aux demandes répétées d'une cliente souhaitant accéder à l'ensemble de ses informations personnelles détenues par la société.

A la fin du présent document est décrit le droit d'accès direct, l'un des droits fondamentaux des personnes au titre de la Loi dite « Informatique et Libertés ».

En savoir plus : Bruno RASLE, Délégué Général de l'AFCDP, Tel. Mobile. 06 1234 0884 delegue.general@afcdp.net

Remerciement :

Nous remercions les étudiants de la promotion 2012-2013 du Mastère Spécialisé de l'ISEP pour leur implication. Futurs Correspondants Informatique et Libertés, ils auront à cœur de mettre en place au sein de leur organisme les procédures permettant de répondre efficacement et de façon sécurisée aux demandes de droit d'accès exprimées par les personnes concernées.

Nous remercions Claire Levallois-Barth, docteur en droit et enseignant-chercheur à Télécom ParisTech, qui a dirigé les travaux de la promotion ISEP concernant le droit d'accès, Denis Beautier, Responsable des Mastères Spécialisés de l'ISEP pour son soutien, Flavia Caloprisco et Corentin Hellendorff qui ont apporté leur aide dans la mise en forme de cet Index..

Cet Index a été créé sur l'idée originale de Bruno Rasle, Délégué général de l'AFCDP.

A propos de l'AFCDP - www.afcdp.net

L'AFCDP a été créée dès 2004, dans le contexte de la modification de la Loi Informatique & Libertés qui a officialisé un nouveau métier, celui de « Correspondant à la protection des données à caractère personnel » (ou CIL, pour Correspondant Informatique & Libertés).

L'AFCDP est l'association représentative des CIL, mais elle rassemble largement. Au-delà des professionnels de la protection des données et des Correspondants désignés auprès de la CNIL, elle regroupe toutes les personnes intéressées par la protection des données à caractère personnel. La richesse de l'association réside – entre autres – dans la diversité des profils des adhérents : Correspondants Informatique & Libertés, délégués à la protection des données, juristes et avocats, spécialistes des ressources humaines, informaticiens, professionnels du marketing et du e-commerce, RSSI et experts en sécurité, qualiticiens, archivistes et Record Manager, déontologues, consultants, universitaires et étudiants.

Quelques membres de l'AFCDP : 3 Suisses, Accor, Adecco, AG2R La Mondiale, American Hospital of Paris, AXA, BP France, Carrefour, Cecurity.com, Caisse nationale des allocations familiales, Communauté Urbaine de Marseille Provence, Conseil Général de Seine-Maritime, CCIP, CPAM des Bouches du Rhône, Crédit Immobilier de France, Ecole Polytechnique, Fédération Nationale des Tiers de Confiance, France Telecom, IBM France, INRA, Groupe Casino, Legrand, Malakoff Mederic, Michelin, La Poste, Port autonome de Dunkerque, RATP, Région Haute Normandie, Région Lorraine, Sénat, SNCF, Ville de Paris, Ville de Saint-Etienne, Total...

Le Droit d'accès direct, au titre de la loi Informatique et Libertés

Au titre de la Loi dite « Informatique et Libertés » (article 39) et du Décret n°2005-1309 du 20 octobre 2005 modifié par le décret n°2007-451 du 25 mars 2007, l'un des tous premiers droits des personnes est **le droit d'accès**.

Toute personne justifiant de son identité a ainsi le droit d'interroger le responsable d'un fichier ou d'un traitement de données personnelles pour savoir s'il détient des informations sur elle, et le cas échéant d'en obtenir communication, et ceci sans avoir à fournir de justification.

En exerçant son droit d'accès, la personne peut s'informer : des finalités du traitement, du type de données enregistrées, de l'origine et des destinataires des données, des éventuels transferts de ces informations vers des pays n'appartenant pas à l'Union Européenne.

Elle peut en outre obtenir des explications sur le procédé informatique qui a contribué à produire une décision la concernant.

L'exercice du droit d'accès permet de contrôler l'exactitude des données et, au besoin, de les faire rectifier ou effacer.

Le Responsable du Traitement doit répondre :

…après s'être assuré de l'identité du demandeur (à adapter à la sensibilité du traitement); sous deux mois (« *Le silence gardé pendant plus de deux mois par le responsable du traitement sur une demande vaut décision de refus* ») ; complètement ; clairement ; gratuitement ou quasiment (« *Le responsable du traitement peut subordonner la délivrance de cette copie au paiement d'une somme qui ne peut excéder le coût de la reproduction* »).

Quelles informations fournir ?

Le Responsable du traitement doit naturellement fournir les données fournies par la personne... mais pas seulement. Doivent notamment être communiqués : les données créées par l'organisme (avec grille de lecture si besoin) ; le contenu des zones de libre commentaire (bloc-notes) ; et plus si demandé :

- la logique et les caractéristiques du traitement ;
- l'origine des données ;
- les éventuels destinataires des données. (L'héritier d'une personne décédée qui souhaite la mise à jour des données concernant le défunt – et donc y accéder - doit, lors de sa demande, apporter la preuve de sa qualité d'héritier par la production d'un acte de notoriété ou d'un livret de famille.

Le rôle du Correspondant Informatique et Libertés (CIL) concernant le droit d'accès :

Organiser la gestion des droits des personnes (réception des demandes – y compris celles exprimées sur place, vérification adéquate d'identité, traitement proprement dit, respect des délais, conformité de la réponse, etc.); sensibiliser et former le personnel ; s'assurer de la présence d'informations claires et pertinentes permettant l'exercice de ce droit ; superviser (au besoin, valider les réponses) et agir en soutien des opérationnels; concevoir des indicateurs pertinents; reporter le suivi de la gestion du droit d'accès dans son bilan annuel.

Quelques recommandations pour les Responsables de traitement :

Préparez vous pour moins de stress et moins d'erreur ;

N'essayez pas de rendre difficile le droit d'accès ;

Privilégiez le courrier postal qui permet plus facilement de vérifier l'identité du demandeur ;

Soyez clair dans la démarche que doit suivre la personne ;

Impliquez vos services courrier, relations clients, réclamations et litiges, etc.

Réfléchissez au droit d'accès sur place ;

Ne répondez pas trop vite, mais bien (et de façon sécurisé) ;

Positivez : vous tenez là une opportunité de contact avec l'un de vos clients.

Les limites du droit d'accès :

La loi Informatique et Libertés, dans son article 39 indique que « *Le responsable du traitement peut s'opposer aux demandes manifestement abusives, notamment par leur nombre, leur caractère répétitif ou systématique. En cas de contestation, la charge de la preuve du caractère manifestement abusif des demandes incombe au responsable auprès duquel elles sont adressées* ».

Le droit d'accès doit s'exercer dans le respect du droit des tiers (par exemple, il n'est pas

possible de demander à accéder aux données concernant son conjoint ; un salarié d'une entreprise ne peut obtenir des données relatives à un autre salarié. En matière de ressources humaines : les salariés ne peuvent accéder aux données prévisionnelles de carrière (potentiel de carrière, classement).

De même il est estimé que l'instrumentalisation du droit d'accès pour d'autres fins que celles visées par la Loi Informatique et Libertés (c'est-à-dire pouvoir exercer ses droits de rectification et de suppression si besoin) ne respecte pas l'esprit du texte.

Pour aller plus loin :

La CNIL a mis en ligne courant 2010 sur son site Web un Guide Droit d'accès, qui s'étend au droit d'accès indirect.

Ce guide a été rédigé à l'attention des personnes qui souhaitent exercer leur droit.

Parmi les conseils dispensés, on y trouve le passage suivant : « *N'oubliez pas qu'il est de votre intérêt de fournir toutes précisions utiles pour permettre le traitement rapide de votre demande par la société ou l'administration. Par exemple, indiquez votre matricule, votre numéro de compte bancaire, d'allocataire, de client, etc.* »