Communiqué de presse – 26 janvier 2015

Données personnelles - Index AFCDP du Droit d'accès

Les résultats plafonnent

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 demander à accéder à ses données personnelles. La veille de sa conférence annuelle, l'AFCDP publie sa mesure de l'effectivité de ce droit. Après les progrès observés les années précédentes, l'édition 2015 montre que les résultats stagnent alors même que les exigences vont prochainement être renforcées dans le cadre du futur règlement européen.

« *Alors que nos indicateurs montraient de réels progrès de 2010 à 2014 – mais il est vrai que nous partions de très loin – nous observons une stagnation dans le millésime 2015 : il reste toujours environ 40 % des entreprises et des organismes qui ne savent visiblement pas quoi faire des demandes de droits d'accès, et le taux des responsables de traitement qui répondent dans les délais et de façon satisfaisante plafonne* » déclare Bruno Rasle, Délégué général de l'AFCDP et pilote de l'Index.

C'est à l'occasion de la journée de la protection des données à caractère personnel 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 ». Cette journée mondiale 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.

L'association publie aujourd'hui la cinquième édition de cet Index, en partenariat avec l'ISEP (Institut Supérieur d'Electronique de Paris, grande école). Cet indicateur est basé sur les travaux effectués par les membres 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. Confrontés ainsi à la réalité, il leur est demandé d'en tirer des enseignements pratiques et opérationnels afin que leur propre responsable de traitement réponde de façon conforme.

La promotion 2013-2014 a ainsi sollicité 163 organismes, privés et publics.

Au titre de la loi dite « Informatique et Libertés » (article 39), toute personne justifiant de son identité a 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...

Un « noyau dur », d'environ 40 % des entreprises, fait le mort

Cet Index, couplé aux mesures précédentes, semble montrer qu'environ 40 % des entreprises et des organismes publics ignorent toujours le droit d'accès et n'y apportent aucune réponse. Le plus surprenant est qu'un tiers de ces entités a désigné un CIL. Faut-il aller jusqu'à, pour ces professionnels de la conformité, mettre en place des tests basés sur le principe du « client mystère » afin de vérifier que leur procédure de gestion des demandes de droits d'accès est connue et appliquée ?

Les personnes concernées étant de mieux en mieux informées et conscientes de leurs droits, elles n'hésitent plus à déposer une plainte auprès de la CNIL, ce qui se traduit par des saisines de plus en plus nombreuses des responsables de traitement par la Commission Nationale Informatique et Libertés.

Certains dossiers débouchent sur des sanctions : 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, qu'en janvier 2011, une banque a subi une sanction pécuniaire de 1.000 euros et qu'en juin 2012, une société d'adduction et le traitement de l'eau du nord de la France a été sanctionnée à hauteur de 10.000 euros sur un motif similaire[1].

58,3 % des entités testées ont répondu dans les deux mois

Sur les 163 organismes contactés, 61,3 % ont réagi. Mais la réponse doit parvenir en moins de deux mois. Au final, **58,3% des entités sollicitées ont répondu dans les deux mois impartis par le cadre légal** (contre 57 % l'an dernier). Ce taux constitue l'Index AFCDP du droit d'accès pour 2015.

Cependant répondre dans les deux mois ne signifie pas non plus que cette réponse soit conforme à la loi. 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.

Plafonnement du taux des réponses conformes à la loi Informatique et Libertés

Au total, de l'avis des membres du Mastère Spécialisé, **37,4 % des organismes sollicités ont fait une réponse conforme au droit**, jugée satisfaisante ou très satisfaisante, dont le respect du délai de deux mois. Cet indicateur, qui avait fortement progressé ces dernières années, passant de 18 % en 2010 à 41% l'an dernier, semble donc se stabiliser sur la barre des 40 %.

---

[1] Voir www.cnil.fr/linstitution/missions/sanctionner/les-sanctions-prononcees-par-la-cnil

Les autres organismes ont retourné des réponses soit décevantes, très incomplètes, incompréhensibles, voire « complètement à côté de la plaque », et ce, pour certaines d'entre elles, malgré la présence d'un Correspondant Informatique et Libertés. Une analyse plus fine laisse penser à des erreurs d'aiguillage des courriers au sein des entreprises ou à une méconnaissance de la procédure à suivre. Dans tous ces cas, le CIL n'a visiblement pas été sollicité pour valider la réponse (une mutuelle retourne ainsi les données personnelles d'un tiers, tandis le chef de cabinet d'un maire indique que les « réponses se trouvent dans le magazine de la commune »).

Seules trois entités sollicités ont demandé une contribution financière avec des montants de quelques euros (dans un 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).

Un droit appelé à être renforcé et homogénéisé

Le projet de règlement européen destiné à remplacer la loi Informatique et Libertés gommera les différences qui existent actuellement entre les Etats membres.

Ainsi, en Angleterre, c'est au responsable de traitement de décider si plusieurs demandes successives provenant d'une même personne sont faites à « intervalle raisonnable », alors qu'au Danemark et en Pologne il faut laisser passer au moins six mois entre deux demandes, contre douze en Espagne et en Allemagne.

Si le responsable de traitement français a deux mois pour fournir les informations demandées, les anglais et les irlandais ne disposent que de quarante jours, les belges quarante-cinq jours et les danois trente. A l'inverse les finlandais peuvent prendre trois mois pour répondre. La proposition de règlement ne prévoit qu'un mois pour donner satisfaction à la personne concernée.

Si le responsable de traitement ne détient aucune information relative au demandeur, les lois grecques et finlandaises précise bien qu'il a l'obligation de répondre (qu'il ne détient rien).

En Autriche, les responsables de traitements doivent transmettre les raisons sociales des sous-traitants, en Grèce ils doivent préciser les modifications apportées aux traitements depuis la dernière demande de la personne, en France il faut indiquer s'il y a des flux transfrontières.

La Grèce, l'Espagne et la Suède imposent au responsable de traitement de communiquer systématiquement l'origine des données traitées. Les responsables de traitement britanniques et italiens peuvent demander une participation financière même si aucune donnée personnelle n'a été trouvée.

En Angleterre et en Irlande, la demande présentée sur place est seulement possible s'il c'est trop difficile ou coûteux d'envoyer les informations au demandeur.

Les membres du DAPIX (Working Party on Information Exchange and Data Protection), qui étudient le projet de règlement pour le compte du Conseil de l'Union européenne, ont parfaitement identifié les points de débat. Dans la dernière version consolidée de leur document de travail[2], on relève que leurs discussions portent essentiellement sur la charge financière que

[2] *Note 15395/14 Council of the European Union, 19 december 2014*, disponible sur http://amberhawk.typepad.com/files/dapix-text-eu-council-dp-reg-december-2014.pdf

représente la traitement de ces demandes pour les entreprises, et sur la nécessité de préciser à quelle fréquence une personne peut exercer son droit d'accès.

Les « spécificités » de l'Index 2015

Les membres de la promotion ISEP 2013-2014 ont fait les constats suivants :

☺ Une banque en ligne a apposé la mention « Confidentiel » sur chaque page contenant des données personnelles et a transmis les documents par pli recommandé.

☺ Une entreprise du secteur grande distribution prend des précautions afin de vérifier l'identité du demandeur : elle demande la copie d'un justificatif de domicile quand l'adresse donnée lors de l'adhésion à son programme de fidélité est différente de celle mentionnée sur la carte d'identité et ce afin d'éviter tout risque de transmission des données à un tiers homonyme.

☺ Une assurance, qui a fourni un millier de pages, a néanmoins pris soin d'anonymiser les champs mentionnant des tiers. Les zones à masquer ont été blanchies avec un correcteur puis le dossier a été copié afin que le demandeur ne puisse avoir accès aux données des tiers en grattant le masquage.

MAIS…

☹ Une grande banque retourne au demandeur son propre courrier, ouvert et inséré dans une autre enveloppe marquée d'un point d'interrogation, sans aucun courrier d'accompagnement.

☹ Le bénévole d'une association semble outré de la demande : « *Souhaitant limiter les dépenses de fonctionnement administratif de l'association, je réponds à votre lettre par un mail. N'ayant rien d'autre à ajouter, je vous prie de tirer vous-même la conclusion qu'il vous plaira concernant des frais que vous avez occasionnés à l'association par votre réclamation* ».

☹ Plusieurs entreprises ont communiqué des informations difficilement compréhensibles. Pourtant, comme le stipule pourtant l'article 95 du décret n°2005-1309 du 20 octobre 2005, « *Les codes, sigles et abréviations figurant dans les documents délivrés par le responsable de traitement en réponse à une demande doivent être explicités, si nécessaire sous la forme d'un lexique* ».

☹ Un fabricant de matériel informatique commence par exiger la fourniture des numéros de série des appareils en possession du demandeur (?). Après communication, cette société a demandé à recevoir la copie des factures d'achat – qui ont été fournies également. Sans résultat.

☹ Une université n'a pas fourni les réponses attendues (diplômes et date d'obtention) mais a transmis des informations qui soulève la question de leur durée de conservation : l'établissement conserve des dossiers de candidatures vieux de plus de vingt-cinq ans, même si les étudiants n'ont pas été retenus ou n'ont pas suivi de cursus au sein de l'établissement.

☹ Un établissement bancaire auprès duquel le demandeur possède plusieurs comptes depuis plus de trente ans, a fourni la réponse suivante : « *Voici les données que nous avons concernant votre personne* » et s'est contenté de recopier les données figurant sur la pièce d'identité transmise (nom patronymique, nom marital, prénom, date et lieu de naissance, nationalité, genre et adresse).

☹ Une mutuelle a fourni des copies d'écran qui montrent en clair les noms des employés étant intervenus sur le dossier.

Parmi les raisons des jugements négatifs portés par les « testeurs » de l'ISEP 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 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.

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 2013-2014 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 également Denis Beautier, Responsable des Mastères Spécialisés de l'ISEP pour son soutien.

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

Les Index AFCDP du droit d'accès sont publiés, depuis 2010, sur la page www.afcdp.net/-Index-du-Droit-d-acces-

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.

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.

Plusieurs exigences du référentiel associé au Label « Gouvernance Informatique et Libertés » de la CNIL concernent la gestion du droit d'accès, dont l'exigence EG01 (« *Le demandeur met en place une procédure spécifique de gestion des réclamations et des demandes relatives à l'exercice des droits des personnes (accès, rectification et opposition) comprenant a minima les modalités d'exercice, la chaine de traitement et les délais de communication* ») et l'exigence EG02 (« *La procédure du demandeur prévoit que le CIL pilote la gestion des réclamations et demandes relatives à l'exercice des droits des personnes, notamment en étant informé de la réception de chaque demande, du traitement qui y est apporté, et en s'assurant du*

respect des délais. »)

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) ;
- Veillez à ce que la procédure de traitement des demandes soit connue de tous ;
- 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 du Droit d'accès*[3], 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.* »

3 http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL_Droit_d_acces.pdf