

## Données personnelles - Index AFCDP du Droit d'accès

### Les résultats plafonnent : seuls 52,4 % des entités sollicitées ont répondu dans les deux mois impartis par le cadre légal

À 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. Le jour de sa conférence annuelle, l'AFCDP publie sa mesure de l'effectivité de ce droit. Après les progrès observés les premières années, l'édition 2017 montre que les résultats stagnent, alors même que les exigences vont prochainement être renforcées dans le cadre du règlement européen qui s'applique à partir du 25 mai 2018.

*« Alors que nos indicateurs montraient de réels progrès ces dernières années – mais il est vrai que nous partions de très loin – nous observons une stagnation dans le millésime 2017 : il reste toujours un trop fort pourcentage d'entreprises et d'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 en dessous des 40 % »* déclare Bruno Rasle, Délégué général de l'AFCDP et pilote de l'Index.

La journée mondiale de la protection des données à caractère personnel a 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 l'occasion de cette journée que l'association française représentative de la profession de CIL (Correspondant Informatique et Libertés) et de futur DPO (*Data Protection Officer*) a dévoilé en janvier 2010 son tout premier « Index AFCDP du Droit d'Accès ».

**L'association publie aujourd'hui l'édition 2017 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 2015-2016 a ainsi sollicité 160 organismes, privés et publics.](#)

## 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<sup>1</sup>.

## 52,4 % des entités testées ont répondu dans les deux mois

Sur les 160 organismes contactés, 60,3 % ont réagi (contre 61,3 % pour l'index précédent). Mais la réponse doit parvenir en moins de deux mois.

Au final, 52,4 % des entités sollicitées ont répondu dans les deux mois impartis par le cadre légal (contre 57 % pour l'index précédent). Ce taux constitue l'Index AFCDP du droit d'accès pour 2017.

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, 36,6 % des organismes sollicités ont fait une réponse conforme au droit, jugée satisfaisante ou très satisfaisante, dont le respect du délai de deux mois (contre 37,4 % pour l'index précédent).

Cet indicateur, qui avait fortement progressé ces dernières années, venant de 18 % en 2010, semble donc se stabiliser sous la barre des 40 %.

Les autres organismes ont retourné des réponses soit décevantes, incomplètes, incompréhensibles, voire « complètement à côté de la plaque ».

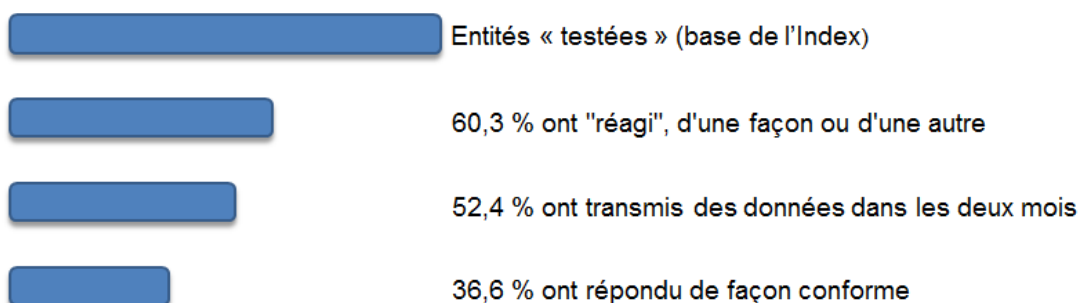
Seule une entité sollicitée demandait une contribution financière de quelques euros : finalement,

---

<sup>1</sup> Voir <https://www.legifrance.gouv.fr/affichCnil.do?id=CNILTEXT000026153467>

le chèque a été retourné avec les données personnelles demandées.

L'approche du règlement européen (RGPD), et son niveau de sanction porté jusqu'à 4 % du chiffre d'affaires mondial, influera-t-il sur les résultats du prochain Index ?



### Un droit appelé à être renforcé et homogénéisé

Les dispositions du règlement européen 2016/679 s'appliqueront à compter du 25 mai 2018.

D'application directe, elles prévoient un délai d'un mois (au lieu de deux actuellement en France) pour répondre à une demande de droit exercé par une personne concernée.

On rappellera qu'actuellement, si les responsables de traitement français ont 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. À l'inverse les finlandais peuvent prendre trois mois pour répondre.

Une fois les modalités de gestion du droit d'accès enfin homogénéisées au niveau européen, l'AFCDP compte proposer à ses homologues – réunit au sein de la *Confederation of European Data Protection Organisations* (CEDPO<sup>2</sup>), co-fondée par l'AFCDP – d'étendre l'Index au continent afin de pouvoir établir des comparaisons entre les états membres.

### Les « spécificités » de l'Index 2017

Voici quelques appréciations des membres de la promotion ISEP 2015-2016 :

😊 « Agréablement surprise d'apprendre qu'un CIL a été désigné dans ma commune ! La personne désignée est archiviste »

😊 « Le CIL m'a contacté à la suite de ma relance, pour me demander de bien vouloir prouver mon identité. J'ai reçu ensuite, dans le délais prévu, toutes les données que j'attendais »

😊 « J'ai vraiment l'impression que l'envoi était complet. Il était accompagné d'un courrier qui explique la démarche et qui va même jusqu'à me préciser quelles sont les données personnelles qui ne sont pas collectées. La réponse était signée du CIL »

---

<sup>2</sup> [www.cedpo.eu/about-cedpo](http://www.cedpo.eu/about-cedpo)

## MAIS...

- ☹ « Ils refusent de me fournir les données en l'absence de procédure judiciaire ! »
- ☹ « On me renvoie sans arrêt d'un service à un autre... mais j'attends toujours la réponse »
- ☹ « Mes données m'ont été envoyées sans être sécurisée, dans un simple courriel »
- ☹ « La société n'a pas pris la précaution de vérifier mon identité – ce qui signifie qu'elle aurait pu transmettre mes données personnelles à un tiers, à mon insu... »
- ☹ « La réaction première de l'entreprise – qui n'a pas de CIL - était complètement « à côté de la plaque ». Ils ont compris que je voulais supprimer mon compte fidélité ! Après explications, ils m'ont assuré faire le nécessaire, mais, au final, je n'ai jamais reçu les données attendues »
- ☹ « Ils ont interprété ma demande comme un souhait de suppression... du coup mon compte a été effacé et je n'ai plus accès à rien ! »
- ☹ « Leur site Web faisait très sérieux et leur mention d'information pouvait laisser croire à une certaine conformité. Ce n'était en fait que de la poudre aux yeux »

Ces appréciations sont dans la lignée de celles faites par les promotions précédentes, dont voici un florilège :

- Une grande banque ne trouve aucune donnée concernant... l'un de ses clients fidèle ;
- 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 cabinet de recrutement affirme avoir procédé à la purge des données ... mais est capable de les produire par la suite ;
- Une entreprise répond qu'elle juge la demande « abusive » et affirme qu'elle n'y répondra que « contrainte par le Procureur de la République » ;
- « Tout ça, c'est du pipeau ! », réaction entendue au téléphone (Profession réglementée dans le domaine du Droit) ;
- « Vous devriez être flatté de figurer dans notre base de données ! » - Collecte déloyale d'informations et refus de communication des informations détenues ;
- « Ces informations sont confidentielles et sont stockées sur des serveurs sécurisés. Je n'y ai pas accès et c'est trop compliqué de demander à chaque service de donner les informations » ;
- « Nous vous confirmons que nous avons bien vos données personnelles »... oui, mais, lesquelles ?
- « Il s'agit des données de l'entreprise, je n'ai pas le droit de vous les transmettre » ;
- « Je tiens tout d'abord à vous rassurer quant au contenu de nos fichiers, ils ne comportent aucune données personnelles pris au sens étymologique du terme ».

Parmi les raisons récurrentes 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<sup>3</sup>; 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 incompetents 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](mailto:delegue.general@afcdp.net)

Agence Ozinfos – Hugo Baillet/Natacha Minier [afcdp@ozinfos.com](mailto:afcdp@ozinfos.com) Tel. 01 42 35 47 35 / 01 42 35 47 27

#### **Remerciement :**

Nous remercions les étudiants de la promotion 2015-2016 du Mastère Spécialisé de l'ISEP pour leur implication. Futurs Correspondants Informatique et Libertés et Délégués à la Protection des Données dans le cadre du RGPD, 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.

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-](http://www.afcdp.net/-Index-du-Droit-d-acces-)

**A propos de l'AFCDP** - [www.afcdp.net](http://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) – futurs Délégués à la Protection des Données (ou DPO, pour Data Protection Officer).

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, qualitatifs, 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...

---

<sup>3</sup> 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 ».

## 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 chaîne 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 ;
- Positivement : 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*<sup>4</sup>, 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.* »

---

<sup>4</sup> [http://www.cnil.fr/fileadmin/documents/Guides\\_pratiques/CNIL\\_Droit\\_d\\_acces.pdf](http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL_Droit_d_acces.pdf)