Norme de Pratique relative à l'utilisation et la protection des données massives, des données personnelles et des données de santé à caractère personnel - NPA 5

Préface

La présente Norme de Pratique Actuarielle (ci-après « NPA 5 ») est une norme professionnelle de catégorie 3 adoptée par l'Institut des actuaires le 16 novembre 2017. Elle vise à proposer un cadre d'utilisation des données applicables à tous les actuaires membres de l'Institut des actuaires (ci-après « l'actuaire ») face aux enjeux et aux risques liés à l'utilisation des **données massives** ou comportant des **données personnelles** ou des **données de santé à caractère personnel** (ci-après « les données »). Elle concerne tout « actuaire » amené à utiliser « ces données » dans les cadres, non-limitatifs, d'analyses comportementales, de segmentation et de profilage, ainsi que certains types de tarification.

1. Généralités

1.1. Objectifs

1.1.1. « NPA 5 » a pour objet de fixer les règles de bonne conduite dans l'exercice du métier de « l'actuaire » utilisant « les données », en insistant tout particulièrement sur les aspects d'intégrité, de compétence et de conformité aux réglementations en vigueur.

1.1.2. « NPA 5 » entend donner un cadre pratique au rôle que l'actuaire doit jouer :

a. Dans la protection de la vie privée des citoyens telle qu'affirmée en 1948 par la Déclaration universelle des droits de l'homme des Nations unies ;

b. Dans l'appréciation de la proportionnalité entre les objectifs poursuivis et « les données » utilisées ;

c. Dans l'utilisation raisonnée et parcimonieuse « des données » ;

d. Dans la confiance des citoyens dans l'usage « des données » les concernant.

1.1.3. « NPA 5 » a également pour but de permettre à « l'actuaire » d'adapter sa conduite en fonction des conditions dans lesquelles il accède à « ces données » de façon à promouvoir les bonnes pratiques au sein de son entourage professionnel sur la conduite qu'il s'est engagé à respecter mais aussi sur les réglementations en vigueur.

Version approuvée par l'Assemblée générale de **l'Institut des actuaires**
le 16 novembre 2017 »

1.2. Territorialité

1.2.1. La territorialité de « NPA 5» s'étend quel que soit le lieu d'exercice de « l'actuaire » (monde entier), sans qu'elle ne prédomine sur la législation locale en vigueur, qui demeure opposable en premier chef à « l'actuaire ».

1.3. Définitions

1.3.1. **Données massives** : ensemble de données comportant de très nombreux enregistrements multicritères, structuré ou non devenu si volumineux qu'il dépasse les capacités d'analyse et l'intuition humaines et nécessitent le traitement par des algorithmes et des outils informatiques adaptés.

1.3.2. **Données personnelles** : ensemble de données relatives à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres (article 2 de la loi informatique et liberté)[1]. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès « l'actuaire », peu importe que ces informations soient confidentielles ou publiques.

1.3.3. **Données de santé à caractère personnel** : ensemble de données médicales relatives à une personne physique mais aussi toute combinaison de données qui permettrait d'indiquer un état de santé physique ou mental passé, présent ou futur.

2. Règles générales de bonne conduite

2.1. Pratiques principales

Conformément à l'article 3.2 du Code de déontologie de l'Institut des actuaires, applicable à tout membre de l'Institut des actuaires, « *dans le cadre de ses travaux actuariels, l'actuaire doit préciser les données, les hypothèses et les méthodes utilisées. Il doit faire ressortir la sensibilité des résultats aux hypothèses et aux choix de modélisation* ».

2.1.1. « L'actuaire » doit indiquer de façon concise et précise l'origine interne ou externe « des données », l'utilisation ou la réutilisation, les contrôles effectués ainsi que les résultats de ses travaux. Il formule les remarques nécessaires pour faire comprendre la portée réelle et les limites des résultats, et rappeler les contraintes créées par les hypothèses.

[1] Par exemple : un nom, une photo, une empreinte, une adresse postale, une adresse mail, un numéro de téléphone, un numéro de sécurité sociale, un matricule interne, une adresse IP, un identifiant de connexion informatique, un enregistrement vocal, …

2.1.2. Il doit préférer l'usage de **données personnelles** anonymisées et à défaut rendre impossible la ré-identification des individus dans la mesure des techniques et technologies existantes. Dans le cas où les travaux de « l'actuaire » ne nécessitent pas l'usage de **données personnelles** non-anonymes, la norme impose l'utilisation de données anonymisées.

2.1.3. Tant que de besoin, « L'actuaire » veille à informer son entourage professionnel qu'il est soumis à cette obligation et cherche à en promouvoir l'application ;

2.1.4. Si l'utilisation des **données personnelles** est une nécessité pour ses travaux, « l'actuaire » doit veiller à assurer la traçabilité des dites données, à identifier les risques pris et à en rendre compte au Délégué à la Protection des Données (DPO ou Data Protection Officer) ou, à défaut à toute personne en responsabilité sur ces domaines. Il doit normalement utiliser lors de ses traitements des techniques de pseudonymisation.

Conformément à l'article 3.2 du Code de déontologie de l'Institut des actuaires, applicable à tout membre de l'Institut des actuaires, « *l'actuaire ne fournit ses services que dans la mesure où il s'estime compétent pour le faire ou bénéficie d'un encadrement lui permettant de sécuriser son travail et ses résultats.* »

2.1.5. « L'actuaire » doit disposer des compétences technologiques et logicielles adaptées à l'utilisation des **données personnelles** et veiller à maintenir ses compétences à jour. Dans le cadre de travaux sur des **données massives**, « l'actuaire » apprécie la mise à jour de ses compétences en lien avec les méthodes et techniques généralement reconnues et appliquées dans ce cadre.

2.2. Aspects comportementaux

Conformément à l'article 3.6 du Code de déontologie de l'Institut des actuaires, applicable à tout membre de l'Institut des actuaires, « *l'actuaire ne fournit pas de services s'il a des motifs de croire qu'ils peuvent être utilisés à contrevenir à la loi ou à la réglementation …* ».

2.2.1. « L'actuaire » doit considérer les textes de référence suivants sans que cette liste ne soit exhaustive :

a. En France, la Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés ;

b. En France, le « pack de conformité assurance » de novembre 2014 établi par les familles de l'assurance en concertation avec la CNIL ;

c. En France, l'article 226-13 du code pénal relatif aux sanctions en cas de non-respect du secret professionnel ;

d. En Europe, le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement

des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) dit règlement RGPD ;

e. En Europe, la Directive 2004/113/CE du Conseil du 13 décembre 2004 mettant en œuvre le principe de l'égalité de traitement entre les femmes et les hommes dans l'accès des biens et services et la fourniture de biens et services.

Conformément à l'article 3.6 du Code de déontologie de l'Institut des actuaires, applicable à tout membre de l'Institut des actuaires, « *... dans le cadre d'utilisation de nouvelles techniques, l'actuaire vérifie que l'utilisation qui pourra être faite de ses travaux respecte les réglementations en vigueur, en particulier sur la confidentialité et la non-discrimination.* »

2.2.2. « L'actuaire » ne doit pas contribuer directement ou indirectement à une atteinte à la protection des **données personnelles** ;

2.2.3. « L'actuaire » ne doit pas conserver des **données personnelles** sur une durée plus longue que celle initialement prévue sans accord explicite du Délégué à la Protection des Données (DPO ou Data Protection Officer) ou, à défaut à toute personne en responsabilité sur ce domaine. Ce point est particulièrement important dans le cadre du « droit à l'oubli » consacré par la Loi « Informatique et Libertés » et le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 ainsi que par la jurisprudence de la Cour de justice de l'Union européenne.

L'actuaire doit considérer la possibilité de détruire les **données personnelles** en cas de demande de la personne physique concernée, ou d'exiger qu'elles soient anonymisées définitivement en effaçant de façon permanente tout lien entre les données personnes et la personne physique.

2.2.4. « L'actuaire » doit veiller à l'application des règles de traitement, de réception, d'utilisation, de transfert et de stockage des informations qui lui sont strictement nécessaires dans les meilleures conditions de sécurité (disponibilité, intégrité, confidentialité) et de protection, et cherche à promouvoir au sein de son organisation les bonnes pratiques en la matière. Il se doit de recommander si nécessaire la destruction des informations ou l'archivage sécurisé des données, à des fins scientifiques, plutôt que la suppression pure et simple des informations, sous réserve de respecter les règles d'anonymisation ;

2.2.5. « L'actuaire » prête une attention particulière aux limites de ses travaux ou de leur domaine de validité, de la péremption de ses travaux[2]. Dans le cas de l'utilisation d'algorithmes particuliers, il précisera l'existence de moyens de vérification ou de contrôle.

[2] Par exemple, robustesse des hypothèses et cohérence des résultats dans le temps, domaine de confiance des algorithmes…

2.2.6. « L'actuaire » est tenu à se sensibiliser contre les risques cyber et en particulier ceux relatifs au vol et au détournement de données et prendre des mesures limitant l'accessibilité aux données et aux travaux sous sa responsabilité afin de limiter les risques de détournement. La présente norme impose à l'actuaire un devoir d'alerte s'il identifie un risque de vol ou détournement auquel il ne peut remédier par ses propres moyens au sein de son organisation.

2.3. Présentation des résultats, maîtrise technique et engagement actuariel

En vertu de l'article 3.11 du Code de déontologie de l'Institut des actuaires, applicable à tout membre de l'Institut des actuaires, « *l'actuaire s'impose de contrôler les travaux préparatoires à l'élaboration de son avis. Il doit également s'assurer de la bonne compréhension des outils et méthodes utilisées pour établir les résultats.* ».

2.3.1. « L'actuaire » doit contrôler et fournir les outils de contrôle de ses travaux. Dans le cas des données personnelles et des données massives, ce sujet est particulièrement sensible. « L'actuaire » doit en particulier envisager dans le cas d'outils inusuels ou faisant appel à des librairies « open sources » de documenter son contrôle par l'usage d'outils alternatifs ou par d'autres méthodes appropriées[3]. Il s'impose le cas échéant de faire état des éventuelles limites des outils utilisés notamment lorsque ces derniers disposent d'un manque de documentation.

2.4. **«** L'actuaire » s'engage à ne pas créer ni à utiliser en conscience des outils erronés et / ou malveillants.

2.5. « L'actuaire » doit, en cas de suspicion d'outils erronés et / ou malveillants, prendre les mesures de protection des intérêts de son employeur, de ses clients et de la communauté actuarielle.

2.6. « L'actuaire » s'oblige à limiter les risques découlant des outils qu'il produit que ceux-ci soient destinés à un public restreint ou qu'ils soient considérés comme de libre accès. Il s'engage à proposer aux utilisateurs une notice d'usage des outils qu'il produit mentionnant les limites identifiées dans l'usage desdits outils. Si « l'actuaire » ne contrôle pas directement leur usage, il prend toutes les mesures et précautions pour en éviter une utilisation inadaptée par d'autres que lui.

2.6.1. « L'actuaire » en situation de tarification peut être amené à discriminer de façon indirecte. Afin d'éviter des risques de discrimination (sexe, nationalité par exemple), l'actuaire doit alors vérifier non seulement qu'il n'utilise pas de variables explicitement

[3] Par exemple, l'actuaire essayera dans la mesure du possible de vérifier que l'open source ne contient aucune ligne de code apparemment inappropriée ou sans lien avec son objectif.

discriminantes au regard des réglementations en vigueur mais que, par l'utilisation de variables externes, il n'obtient pas in fine une discrimination de son tarif. Pour cela, « l'actuaire » pourra s'appuyer sur des approches ex ante ou ex post :

a. Non-discrimination par construction (pas de variables discriminantes directes ou indirectes) ;

b. Explicativité par construction (justification du pouvoir explicatif de chaque variable utilisée) ;

c. Approche ex post. Par exemple, on mesurera la prime des hommes par rapport à la prime des femmes sur un échantillon réel.

2.6.2. Les critères de segmentation doivent être liés aux pratiques de marché et définis par des objectifs exacts, pertinents et proportionnels pour le risque. Ils doivent être opposables à un tiers, en ce sens qu'il ne puisse être démontré qu'aucun traitement discriminatoire n'a été effectué.

3. Règles spécifiques aux données de santé à caractère personnel et secret professionnel

3.1. Concernant le secret professionnel, « l'actuaire » doit savoir que pour que le délit soit caractérisé, peu importe qu'il y ait préjudice ou que la personne concernée par une éventuelle violation du secret professionnel ait effectivement porté plainte.

3.2. « L'actuaire » doit également savoir que chaque personne physique est seule dépositaire du secret concernant son propre état de santé et que seul un médecin peut correspondre avec cette personne physique sur son état de santé par écrit et par oral. C'est un médecin qui porte la responsabilité d'autoriser d'autres individus à exploiter des données de santé à caractère personnel dans le respect du secret professionnel.

4. Règles spécifiques aux risques et aux enjeux des données de santé à caractère personnel

Outre les articles 3.6 et 3.7 du Code de déontologie de l'Institut des actuaires, « l'actuaire » ayant accès à des **données de santé à caractère personnel** doit appliquer les règles de bonne conduite et les principes exposés ci-après.

4.1. Traitement et stockage des données de santé à caractère personnel

4.1.1. « L'actuaire » ne doit – en aucun cas - utiliser de **données de santé à caractère personnel** sans y avoir expressément été autorisé par un médecin, à moins que les données aient été préalablement anonymisées par un autre que lui, c'est-à-dire qu'elles ne peuvent – en aucun cas - être reliées directement ou indirectement avec l'identité des personnes physiques concernées. En cas de réception indue de fichiers de données personnelles de santé non anonymisées, il est fortement recommandé de réclamer ce même fichier, mais anonymisé, et de détruire le précédant en en informant celui qui a rompu la chaine de confidentialité.

4.1.2. « L'actuaire » doit s'attacher à contribuer activement, dans la limite des moyens à sa disposition, à faire adapter les processus dans son entourage professionnel de façon à promouvoir la protection des données de santé à caractère personnel.

4.1.3. S'il y est autorisé par un médecin, l'actuaire veille à traiter des données de santé à caractère personnel, dans le respect des réglementations en vigueur et en veillant particulièrement à anonymiser ou pseudonymiser les informations dès que cela est possible aux fins des traitements dont la charge lui est confiée.

4.1.4. « L'actuaire » s'impose de veiller à l'application des règles de stockage des informations qui lui sont strictement nécessaires dans les meilleures conditions de sécurité et de protection, et s'engage à promouvoir au sein de son entourage professionnel les bonnes pratiques en la matière si besoin.

4.2. Conditions de respect du secret professionnel dans le cadre des données de santé à caractère personnel

4.2.1. « L'actuaire » est tenu au respect du secret professionnel et à la protection des **données de santé à caractère personnel** lorsqu'il est autorisé à les utiliser sous la responsabilité d'un médecin[4].

4.2.2. Si « l'actuaire » n'est pas autorisé à recevoir ou à avoir accès à des **données de santé à caractère personnel** :

[4] Il est ici rappelé un extrait de l'article 104 du Code de déontologie de l'Ordre des Médecins (édition 2017) ou Code de la Santé publique R.4127-104
« Le médecin […] est tenu au secret envers l'administration ou l'organisme qui fait appel à ses services. Il ne peut et ne doit lui fournir que ses conclusions sur le plan administratif, sans indiquer les raisons d'ordre médical qui les motivent.
Les renseignements médicaux nominatifs ou indirectement nominatifs contenus dans les dossiers établis par ce médecin ne peuvent être communiqués ni aux personnes étrangères au service médical ni à un autre organisme. »

a. Il s'interdit de traiter ces données non-anonymisées et s'oblige à se placer sous l'autorité d'un médecin pour le faire notamment en demandant formellement au médecin conseil de son employeur cette autorisation si ses missions l'imposent ;

b. Ou il doit réclamer l'anonymisation effective de ces données de façon à ce que soit définitivement supprimée toute information permettant une identification individuelle directe ou indirecte, avant d'opérer ses travaux.

4.2.3. Lorsque « l'actuaire » reçoit ou accède à des **données de santé à caractère personnel**, il s'assure du respect du secret professionnel au sein des procédures de son entourage professionnel et s'oblige à signaler et proposer la correction de tout risque de manquement observé et vérifie - dans la mesure de ses possibilités d'action - que ces données ont été collectées avec le consentement libre et éclairé des personnes physiques concernées.

5. Spécificités pour « l'actuaire » en situation de Délégué à la protection des données (Data Protection Officer)

5.1.1. « L'actuaire » exerçant la fonction de Délégué à la protection des données (cf. RGDP Art.37 et suivants) est visé par l'article 3.17 du code de déontologie au titre des fonctions visées par la réglementation. A ce titre, il doit se doter de tous les moyens nécessaires au bon exercice de sa fonction.

5.1.2. Il doit, en particulier, s'assurer qu'il est à jour dans ses connaissances techniques pour disposer des compétences nécessaires pour :

a. Contrôler l'ensemble des travaux préparatoires à l'élaboration de son avis ;

b. S'assurer de sa bonne compréhension des outils et méthodes utilisées pour établir les résultats.

5.1.3. Il s'appuie en particulier sur NPA 5 pour mener à bien ses travaux et en communiquer de façon adaptée les hypothèses et limites.