CONFERENCE

APPLICATION DU RGPD À LA RÉASSURANCE

Présentation APREF

Commission Juridique

GT Protection des données

apref
ASSOCIATION DES PROFESSIONNELS DE LA RÉASSURANCE EN FRANCE

Mardi 26 Juin 2018

SOMMAIRE

1 Données à caractère personnel, données sensibles et champ d'application

1) Données à caractère personnel

Définition : toute information se rapportant :

- à une personne physique identifiée ;
- à une personne physique qui peut être identifiée (ou « identifiable »), directement ou indirectement par référence à un identifiant. Dans ce cas, les données peuvent être :
    - directement identifiantes : nom et prénom, numéro d'identification, photo ou vidéo, e-mail nominatif, etc… ;
    - indirectement identifiantes : NIR, empreinte digitale, domicile, données de localisation, etc… ;
    - le recoupement d'informations anonymes : le fils du courtier habitant au 11, bd Raspail à Paris.

En pratique, données à caractère personnel traitées par un réassureur dans son activité de réassurance :

- les données des assurés et des tiers-victimes ;
- les données de ses interlocuteurs chez les cédantes, les courtiers et chez les autres réassureurs ou rétrocessionnaires.

1 Données à caractère personnel, données sensibles et champ d'application

2) <u>Données sensibles</u>

<u>Nature</u> : données sensibles, catégorie particulière de données personnelles

<u>Définition</u> :

- toute donnée révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale ;
- les données génétiques et biométriques (ajout du RGPD) et des données concernant la santé, la vie sexuelle ou l'orientation sexuelle.

<u>Traitement</u> :

- Principe : interdiction

- Dérogations (pour un réassureur dans son activité de réassurance) :
  - consentement explicite de la personne concernée ;
  - données manifestement rendues publiques par la personne concernée ;
  - traitement nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ;
  - traitement nécessaire pour des motifs d'intérêt public important (assurances obligatoires) ;
  - données anonymisées à bref délai selon un procédé agréé par la CNIL (ajout de la loi « Informatique et Libertés II »).

1 Données à caractère personnel, données sensibles et champ d'application

3) Champ d'application

Champ d'application matériel (inchangé) :

- traitement de données personnelles, automatisé en tout ou partie ;
- traitement non automatisé de données personnelles contenues ou appelées à figurer dans un fichier.

Champ d'application territorial (élargi par le RGPD)

- traitement réalisé dans le cadre des activités d'un établissement d'un réassureur sur le territoire de l'UE ;
- traitement relatif à des personnes concernées se trouvant sur le territoire de l'UE (si traitement lié à l'offre d'une prestation de services à ces personnes).

2 Le Réassureur, responsable de traitement ou sous-traitant ?

1) Définitions

Responsable de traitement:

« la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement » (Article 4.7).

Sous-traitant

« la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement » (Article 4.8).

2) Critères de détermination *(cf. Guide du Sous-traitant publié par la CNIL)*

- Autonomie : dans la détermination des finalités et des moyens d'un traitement ;
- Surveillance : Quel degré de contrôle et d'influence est exercé par l'autre partie ?
- Transparence : L'identité du partenaire qui traite des données personnelles est-elle connue des personnes concernées ?
- Conséquences : le réassureur, responsable de traitement car autonomie et absence de surveillance de la cédante dans le traitement des données personnelles fournies.

2 Le Réassureur, responsable de traitement ou sous-traitant ?

3) Obligations du responsable de traitement

- Mise en œuvre de mesures techniques et organisationnelles appropriées (sécurisation des données, minimalisation, anonymisation, sélection et obligations renforcées des sous-traitants …);
- Documenter afin de pouvoir prouver la mise en œuvre de ces mesures techniques et organisationnelles: le réassureur doit être en mesure de prouver sa conformité aux obligations réglementaires.

4) L'exigence du consentement appliquée à la réassurance

- L'obtention du consentement est un élément central permettant la licéité de la collecte et du traitement (sauf si un autre cas de licéité prévu à l'article 6 du RGPD s'applique) ;
- Le réassureur doit être en mesure de prouver qu'il a été correctement obtenu et qu'il lui a été clairement attribué ;
- Le réassureur ne collectant pas directement les données personnelles, un certain nombre d'informations supplémentaires doivent être fournies à la personne concernée ;
- Le niveau de consentement requis est différent selon le type de données personnelles. En particulier, le recueil des données sensibles nécessite un «*consentement explicite*».

2 Le Réassureur, responsable de traitement ou sous-traitant ?

5) <u>Sécurité des données à caractère personnel</u>

- Le réassureur doit mettre en œuvre les mesures techniques et organisationnelles appropriées aux fins de garantir un niveau de sécurité adapté au risque.

- Si malgré la mise en place de ces mesures, une violation des données à caractère personnel survient, les articles 33 et 34 du RGPD imposent au réassureur :

  - Une notification de ladite violation auprès de la CNIL dans les 72 heures au plus tard après en avoir pris connaissance si elle présente un risque pour les personnes concernées ;

  - Une communication de cette violation aux personnes concernées dans les meilleurs délais si elle présente un risque élevé pour ces personnes (sauf mesures rendant les données incompréhensibles).

- La notification et la communication (dans des termes clairs et simples) comprennent :

  - Une description de la violation des données et des conséquences probables ;
  - Une communication du nom et des coordonnées du Délégué à la protection des données ;
  - Une description des mesures prises ou que le réassureur propose de prendre pour remédier à la violation des données et le cas échéant en atténuer les conséquences.

3 L'Analyse d'impact relative à la protection des données

1) <u>Analyse d'impact relatives à la vie privée (ou PIA)</u>

- Le RGPD, une approche de la protection des données par les risques :
  - Le terme « risque » est employé plus d'une centaine de fois dans le RGPD ;
- L'analyse d'impact : « L'exemple révélateur de cette philosophie du RGPD »

  Elle poursuit un double objectif :
  - Évaluer la nécessité et la proportionnalité du traitement ;
  - Évaluer les risques pour les droits et libertés des personnes concernées engendrés par le traitement (cette gestion des risques se retrouve dans l'outil PIA disponible sur le site de la CNIL).

3 L'Analyse d'impact relative à la protection des données

2) <u>Les traitements concernés par l'analyse d'impact</u>

Une analyse d'impact doit être effectuée dès qu'un traitement présente un risque élevé sur les droits et libertés des personnes concernées.

- L'article 35 du RGPD vise trois types de traitement :
  - Évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, fondée sur un traitement automatisé, y compris le profilage, et sur la base de laquelle sont prises des décisions produisant des effets juridiques à l'égard d'une personne physique ou l'affectant de manière significative de façon similaire ;
  - Traitement à grande échelle de catégories particulières de données visées à l'article 9, paragraphe 1 (les données sensibles), ou les données à caractère personnel relatives à des condamnations pénales et à des infractions;
  - Surveillance systématique à grande échelle d'une zone accessible au public.
- Conseil / Recommandation du G29 : vérifier la présence ou non d'un ou plusieurs critères prédéfinis pour identifier d'autres traitements devant faire l'objet d'une analyse d'impact.

4 Le Délégué à la Protection des Données (DPD)

1) Désignation d'un DPD (ou DPO)

Cas de désignation obligatoire

- Traitement effectué par une autorité publique ou un organisme public ;
- Activités de base du responsable du traitement : opérations de traitement exigeant un suivi régulier et systématique à grande échelle des personnes concernées ;
- Activités de base du responsable du traitement : traitement à grande échelle de données sensibles ou de données sur des condamnations pénales et des infractions.

En cas de désignation volontaire : application de toutes les dispositions du RGPD sur la désignation, la fonction et les missions du DPO.

Désignation par un réassureur

- Lignes directrices du G29 : traitement des données de clients par une compagnie d'assurance ou une banque, traitement «à grande échelle» ;
- Par analogie : traitement de données d'assurés et de victimes par un réassureur, traitement « à grande échelle » impliquant la désignation d'un DPO.

Localisation

- Principe : DPO joignable par toute personne intéressée ;
- Recommandation : DPO dans l'UE même si réassureur établi hors UE.

4 Le Délégué à la Protection des Données (DPD)

2) Missions du DPO

Missions issues du RGPD

- informer et conseiller le réassureur et ses employés en charge d'un traitement sur la réglementation externe et interne, avec sensibilisation et formation de ces employés ;
- contrôler le respect de la réglementation externe et interne ;
- dispenser des conseils sur les analyses d'impact et vérifier l'exécution de celles-ci ;
- coopérer avec la CNIL et être le point de contact avec celle-ci.

Autres missions confiées en pratique au DPO

- constituer et actualiser une documentation contenant les preuves de la conformité à la réglementation ;
- tenir le registre des traitements ;
- notifier une violation de données à la CNIL ;
- répondre aux demandes de droit d'accès des personnes concernées.

4 Le Délégué à la Protection des Données (DPD)

3) <u>Fonction de DPO</u>

<u>Le DPO doit :</u>

- être associé à toutes les questions sur la protection des données personnelles ;
- être doté des ressources nécessaires pour exercer ces missions ;
- disposer d'un accès aux données personnelles et aux opérations de traitement ;
- pouvoir entretenir ses connaissances spécialisées ;
- faire directement rapport au niveau le plus élevé de la direction du responsable du réassureur.

<u>Dans l'exercice de ses missions, le DPO :</u>

- ne peut être relevé de ses fonctions ou pénalisé dans l'exercice de ses missions ;
- est soumis au secret professionnel ou à une obligation de confidentialité.

5 Transfert de données à caractère personnel hors UE

1) <u>Transfert vers un pays dont la protection est jugée adéquat par l'UE</u> (pays tiers ou Organisations Internationales) : aucune autorisation de la CNIL préalable n'est nécessaire.

2) <u>Transfert de données vers un pays qui n'est pas reconnu par l'UE comme bénéficiant d'une protection adéquate</u>

Un réassureur peut effectuer un tel transfert sans autorisation de la CNIL s'il justifie de garanties appropriées qui peuvent prendre la forme soit :

- d'un instrument juridiquement contraignant et exécutoire entre les autorités et organismes publics ;
- de règles d'entreprises contraignantes (ce corps de règles doit toutefois recueillir l'approbation préalable de l'autorité de contrôle de l'établissement qui les édicte) ;
- de clauses types de protection des données adoptées par la Commission ;
- de clauses types de protection des données adoptées par une autorité de contrôle et approuvées par la Commission ;
- d'un code de conduite ;
- d'un mécanisme de certification approuvé conformément à l'article 42 du RGPD ;
- de certaines décisions de justice.

5 Transfert de données à caractère personnel hors UE

3) <u>Dérogations au principe d'interdiction des transferts (article 49)</u>

- Le RGPD reprend également les dérogations au principe d'interdiction des transferts qui étaient déjà prévues par la directive 95/46 Ce du 24 octobre 1995, et à l'article 69 de la loi Informatique et Libertés du 6 janvier 1978. On en citera notamment deux:

  - La personne concernée a donné son consentement explicite suite à une information relative; aux risques résultant de ce transfert ;
  - Le transfert est nécessaire à la constatation, l'exercice ou la défense de droits en justice.

- Le deuxième alinéa du 1 de l'article 49 prévoit une ultime possibilité de transfert. Toutefois cette exception est limitée à des cas ponctuels et exceptionnels et ne doivent pas concerner des transferts répétitifs, massifs ou structurels de données personnelles.

6 INFORMATIONS COMPLEMENTAIRES

1) Preuve de la conformité

- Avant le RGPD : preuve par la CNIL de la non-conformité d'un réassureur à la réglementation ;
- Après le RGPD : preuve par le réassureur qu'il est conforme à tout moment à la réglementation (traçabilité et preuve du respect de chaque obligation du RGPD).

2) Sanctions administratives de la CNIL

- 20 M€ ou 4% du chiffre d'affaires annuel mondial (infractions les plus graves) ;
- 10 M€ ou 2% du chiffre d'affaires annuel mondial (autres infractions).

3) Suppression des déclarations préalables à la CNIL.

4) Tenue d'un registre des traitements

- Obligatoire pour un réassureur comptant plus de 250 salariés ;
- Obligatoire pour un réassureur comptant moins de 250 salariés si :
  - traitement comportant un risque pour les personnes concernées
  - traitement comportant des données sensibles.

CONTRIBUTEURS AU GT PROTECTION DES DONNÉES

- Cécile Koczan (HANNOVER Re)
- Eloïse Sorin (SCOR)
- Arnaud Verrey (CCR)
- Guillaume Lachaud (SWISS RE)
- Julien Vigeoz (XL CATLIN)

POUR PLUS D'INFORMATIONS SUR L' APREF & LA RÉASSURANCE

Notre site internet : www.apref.org

Notre Situation : 26, Boulevard Haussmann (6ème étage)

Notre compte Twitter : @Apref_Reass