Actualité de la Protection Sociale

Assurances Collectives
SACEI
Journée « Assurance de Personnes »

Jeudi 20 septembre 2018

Denis FENDT
DGA
Directeur du Développement

ADREA mutuelle apréva EOVIMCD mutuelle

GROUPE AESIO

SOMMAIRE

Regards croisés sur des évaluations de marché envisageables pour les Organismes Assureurs, les souscripteurs et leurs conseils avec François LUSSON, Actuaire Associé (Actense)

1

Préambule : le Groupe AESIO

LA PUISSANCE D'UN GROUPE LEADER EN ASSURANCE DE PERSONNES : QUELQUES CHIFFRES CLÉS

- **3 000 000** de personnes protégées
- **40 000** entreprises adhérentes
- 360 agences
- **3 700** collaborateurs
- Plus de **300%** de marge de solvabilité
- **1,5 milliard** de fonds propres
- **1,7 milliard** de chiffre d'affaires
- **31** offres (santé) de branches en recommandations
- CCN du Personnel des organismes de SS (recommandation/apérition)

2

Directive Distribution Assurance

INTRODUCTION

LA DIRECTIVE DISTRIBUTION ASSURANCE S'INSCRIT DANS UN CADRE REGLEMENTAIRE QUI A POUR PRINCIPAL OBJECTIF LA PROTECTION DU CONSOMMATEUR.

LE CADRE JURIDIQUE ET REGLEMENTAIRE DDA 2018

- Directive Distribution Assurance:
  - Date d'entrée en vigueur : 1er Octobre 2018
  - Ordonnance transposant la DDA a été publiée au JO le 16/05
  - Date d'entrée en vigueur des exigences sur les formations : 23 Février 2019

- De nombreuses exigences sur les thèmes suivants :
  - Gouvernance et surveillance des produits
  - Prévention et gestion des conflits d'intérêts
  - Formalisation du conseil
  - Professionnalisation

LES TRAVAUX DE MISE EN CONFORMITE DDA 2018 (1/2)

- Participation Ateliers FNMF / Réunions ACPR : Remontée de questions sur des thématiques précises par le comité opérationnel juridique.
- Réalisation des Fiches IPID.
- Gouvernance et Surveillance des Produits :
  - La politique GSP a été rédigée puis présentée et validée par le Conseil d'administration Groupe AESIO.
- Evolution du Formulaire Devoir de conseil.
- Définition du dispositif de Distribution du Groupe AESIO.
- Formation des équipes de la Direction Développement à la DDA et à son application opérationnelle.
- Sensibilisation des collaborateurs du Groupe AESIO à la DDA grâce à la diffusion d'un film sur les principaux changements engendrés par la DDA.

LES TRAVAUX DE MISE EN CONFORMITE DDA 2018 (2/2)

- Vérification de l'honorabilité des commerciaux (en cours).
- Prévention des conflits d'intérêts (en cours).
- Formalisation des règles à respecter concernant la rémunération (en cours).
- Détermination de contrôles liés au respect des exigences de la DDA (à planifier).
- Mise en conformité avec les partenaires distributeurs / assureurs.

En 2019, les travaux de mise en conformité avec la DDA vont se poursuivre notamment en ce qui concerne les formations et les compétences des acteurs concernés.

3

Règlement Général Protection Données à caractère personnel

LE RGPD DANS UN CONTEXTE DE RENFORCEMENT DES DROITS DES CONSOMMATEURS

1978 — **Loi informatique et liberté**

1995 — **Directive 95/46/CE sur la protection des données**

2004 — **Loi 2004 – 001 Transposition de la Directive 95/46/CE en droit français**

2014 — **Pack conformité CNIL pour les assureurs**

2016 — **Loi sur la république numérique** — **RGPD**

2018 — Loi CNIL 3 — **25 Mai 2018** entrée en application RGPD — Règlement e-privacy

- L'esprit du RGPD vise à répondre aux objectifs suivants :
  - Organiser une gouvernance sur la protection des données
  - Renforcer les droits des personnes
  - Responsabiliser les tiers (prestataires et sous-traitants) des données

- Respecter les droits et libertés fondamentales des individus (prospects, clients, collaborateurs, partenaires… et en assurer la protection

LES OBLIGATIONS RÉGLEMENTAIRES

Quels principes respecter ?

10 thématiques clés abordées

- Consentement
- Gouvernance
- Documentation
- Formation
- Droit à la personne
- Stockage et durée de conservation
- Respect vie privée dès conception
- Sécurité et gestion des incidents
- Sous-traitance
- Transfert hors UE

Gouvernance

Les organismes traitant de données personnelles doivent déterminer les rôles et responsabilités associés à ces traitements.

Sous-traitance

Le Responsable de traitement doit s'assurer que ses sous-traitants présentent des garanties suffisantes et les sous-traitants doivent respecter de nouvelles obligations vis-à-vis du responsable.

Le consentement

Certains traitements doivent faire l'objet d'un consentement.

Définition : « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ».

Respect vie privée dès conception

L'objectif du Privacy By Design est de penser la protection des données dès la conception des projets c'est-à-dire de s'assurer de la pertinence des données collectées, comprendre les risques pour les personnes concernées, anticiper la transparence et le droit d'accès…

Documentation

L'accountability (ou documentation) nécessite de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données.

Il s'agit de construire un registre des traitements et de le mettre à jour et de rédiger et appliquer des politiques et procédures.

LES OBLIGATIONS RÉGLEMENTAIRES

Quels principes respecter ?

10 thématiques clés abordées

- Consentement
- Gouvernance
- Documentation
- Formation
- Droit à la personne
- Stockage et durée de conservation
- Respect vie privée dès conception
- Sécurité et gestion des incidents
- Sous-traitance
- Transfert hors UE

Droits à la personne

Les organismes doivent être en capacité de répondre à une demande d'exercice de droit d'une personne concernée par un traitement (droit d'accès, de rectification, d'effacement, de portabilité, droit à la limitation du traitement, d'opposition ou de détermination du sort post mortem de ses données).

Formation

Les collaborateurs intervenant sur des traitements de données personnes doivent être formés afin d'appliquer les principes réglementaires.

Sécurité et gestion des incidents

Les traitements doivent bénéficier d'un sécurité physique et organisationnelle adéquate. En cas de violation de données, l'organisme a l'obligation d'en notifier la CNIL, et dans le cas où la violation induit des risques élevés pour les droits et libertés des personnes, il doit également notifier les personnes concernées.

Stockage et durée de conservation

Les données ne peuvent être conservées que pour une durée limitée. Cette durée est déterminée légalement ou par le Responsable de traitement.

Transfert hors UE

Les données ne peuvent être transférées hors de l'Union Européenne que si ce transfert présente des garanties suffisantes (consentement, règles contraignantes d'entreprise, clauses contractuelles types de la commission européenne).

DES RISQUES FORTS

- Renforcement des sanctions administratives (4% du CA annuel mondial ou 20 M€)
- Sanctions s'appliquent au Responsable de Traitement et au sous-traitant
- Sanctions pénales et/ou civiles des dirigeants
- Obligation de communiquer sur les violations de données
- Impact sur l'image de marque

Risques médiatiques élevés
La CNIL rendra publiques les manquements et les sanctions

Sanctions pénales lourdes
Jusqu'à 5 ans d'emprisonnement pour le responsable des traitements

Sanctions opérationnelles
La CNIL peut prononcer des injonctions de cessation de traitements et la mise en conformité sous astreinte

Sanctions pécuniaires fortes
Jusqu'à 20 millions d'€ ou 4% du CA

PRINCIPAUX TRAVAUX RGPD 2018

- Le DPO a été désigné au niveau du Groupe AESIO.
- Des relais DPO ont été identifiés dans les 4 entités du Groupe AESIO.
  - Création d'une équipe transverse d'experts
- Un réseau de correspondants DCP et de responsables de traitement a été mise en place.
- Une comitologie RGPD a été mise en place.
- Chaque entité dispose de sa Charte de protection des données en ligne.
- La politique de protection des données a été rédigée.
- Chaque entité du Groupe AESIO dispose de son registre des traitements et d'une analyse de sa maturité.
- Les travaux liés à la sécurisation des données sont menés par les DSI.
- Le recensement des tiers avec échanges de données personnelles est en cours de finalisation
- Un programme de mise en conformité RGPD a été rédigé : il identifie les principaux chantiers de mise en conformité à mener avec une priorisation et un timing défini.

PROGRAMME DE MISE EN CONFORMITE RGPD

Le Programme de mise en conformité RGPD est réparti en 16 Chantiers

1 Politique	2 Accountability	3 Formation	4 Registre
5 DPO	6 Licéité des traitements	7 Minimisation	8 Durées de conservation
9 Contrôle et Audit	10 PIA	11 Privacy	12 Transparence
13 Gestion des droits	14 Audits CNIL	15 Gestion des Tiers	16 Sécurité

4

La fin des désignations

LA FIN PROGRAMMÉE DES DÉSIGNATIONS (1/2)

- 17/12/2015: la CJUE rappelle l'obligation de transparence impliquant un degré de publicité adéquat permettant une ouverture à la concurrence et le contrôle de l'impartialité de la procédure d'attribution (AO Klesia dans l'immobilier et AG2R dans la boulangerie)
- 2016: le conseil d'état éreinte les clauses de désignation en boulangerie et en pharmacie d'officine
- 2017: la cour de cassation annule pour de bon la désignation d'AG2R en boulangerie

- Les derniers accords vont tomber + un regroupement des branches va s'opérer

3. LA FIN DES DESIGNATIONS (2/2)

- Le Comité Paritaire de Suivi
- Référencement-Labellisation / Recommandation
- Qu’attendre du rapprochement des Branches en la matière ?

Merci de
votre attention

Denis FENDT

•

Directeur Général Adjoint

Directeur du Développement

•

Groupe AESIO
25 place de la Madeleine – 75008 Paris
www.aesio.fr