

23/05/2019

# Protection des données personnelles chez CNP Assurances sous le Règlement Général Protection des Données

Retour d'expérience : changements (organisation, change  
management)

assurer tous  
les avènements

Martina Duchonova  
DPO Groupe  
Délégue à la protection  
des données



# Sommaire



1

Présentation de CNP Assurances

2

Focus sur les changements dans l'organisation

3

Focus sur les changements dans le change management

4

Questions/Réponses

1

## **Présentation de CNP Assurances**



## Chiffres-clés

- ▶ 35 millions d'assurés en prévoyance/protection\* et 14 millions d'assurés en épargne/retraite dans le monde
- ▶ 2 continents : l'Europe et l'Amérique latine
- ▶ 5 170 collaborateurs
- ▶ 32,1 Md€ de CA en 2017
- ▶ 310 Md€\*\* d'encours moyens nets en 2017

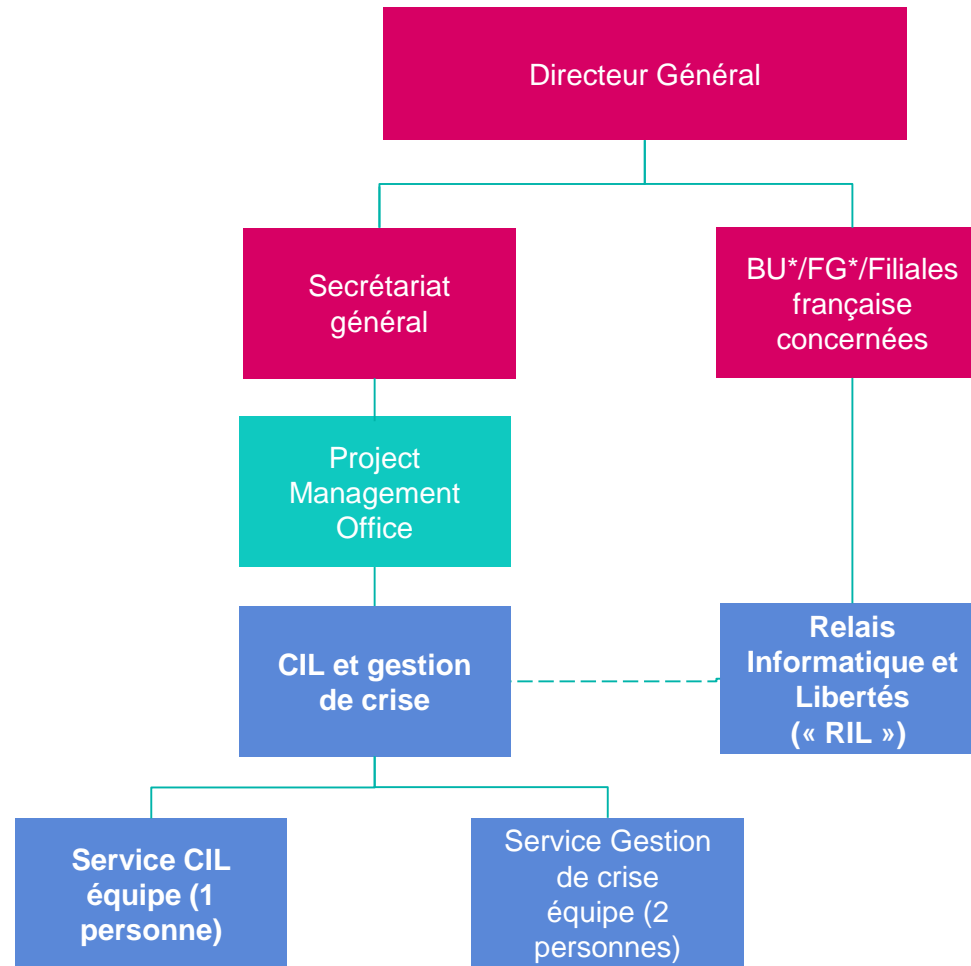
\* *Prévoyance/protection : prévoyance, santé, assurance emprunteur et IARD*

\*\**Données chiffrées : résultats 2017*

2

**Focus sur les changements dans  
l'organisation**

# L'organisation de la fonction avant GDPR



— Lien hiérarchique

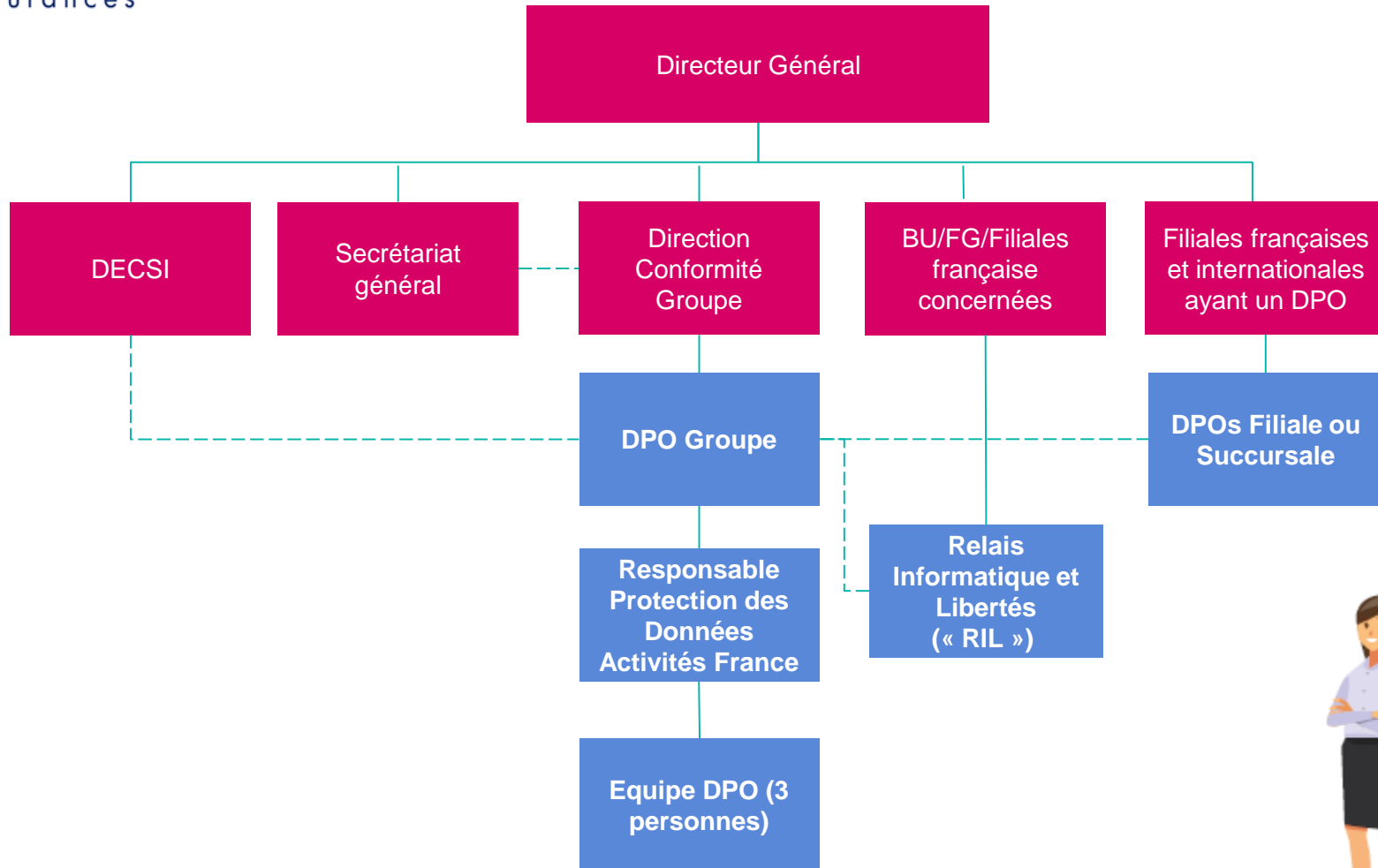
- - - Lien fonctionnel

\* BU – Business Unit

FG – Fonction Groupe



# L'organisation actuelle de la fonction DPO



— Lien hiérarchique

- - - Lien fonctionnel

# Changements dans la gouvernance et dans l'organisation des sujets opérationnels

- ✓ Application du GDPR à toutes les filiales du Groupe CNP Assurance à l'international (Politique Groupe)
- ✓ Mise en place du RACI et du guide des RILs en France
- ✓ Mise en place d'un réseau à l'international (nomination DPOs + calls + séminaires + visites sur sites, ...)
- ✓ Prise en compte de principes « privacy by design » et « d'accountability » :
  - ✓ Mise en place de nouveaux chemins de traitement et de validation des projets/produits/services (procédure) →
  - ✓ Mise en place de nouveaux chemins de validation de qualification des tiers et de processus de contractualisation (procédure + outil)
  - ✓ Reconstruction du processus de création d'une fiche de traitement et création d'un outil PIA et d'un registre de traitement (procédure + outils)
  - ✓ Mise en place de processus de gestion des violations des données à caractère personnel (procédure + suivi)
  - ✓ Amélioration du processus de gestion des droits des personnes (procédures + suivi) et amélioration du processus de mise en place et modifications des mentions d'informations (procédure + suivi)
  - ✓ Création des contrôles (procédure + processus + suivi)

## Sommaire

- / Définition et principes du Privacy by Design
- / Responsabilité du traitement de données concerné par le projet
- / Parties prenantes d'un projet et leurs rôles
- / Rappel des différents rôles du consultant interne PMO & Processus
- / Les questions à se poser avant le déploiement d'un projet
- / Processus de gestion de projet pilotée par la BU/FG commanditaire
- / Processus de gestion de projet avec un accompagnement d'un chef de projet DECSI
- / Processus de gestion de projet avec un accompagnement d'un chef de projet PMO & Processus
- / Liste des RIL
- / Glossaire



3

**Focus sur les  
changements dans le  
change management**



# La sensibilisation a débuté bien avant 2016 et s'est poursuivie en 2017 ....

- ✓ **Des actions de sensibilisation globale ont eu lieu durant plus de 10 ans :**
  - ✓ Information des collaborateurs sur le risque de « non-conformité Informatique et Libertés » dans le dispositif de contrôle interne dès 2000
  - ✓ Site intranet avec un onglet dédiée à la sensibilisation « Informatique et Libertés » : actualité, procédures, fiches pratiques en 2008
  - ✓ Quiz facultatif en ligne de 100 questions avec 3 niveaux d'expertise sur les fondamentaux de la protection des données à caractère personnel (« DCP ») en 2010
  - ✓ Sensibilisation des Comités de Direction des Business Units lancée en 2010
  - ✓ Sensibilisation sur les thèmes spécifiques (facebook, DCP,...) en duo avec un avocat spécialisé
  - ✓ ...
- ✓ **Actions de sensibilisation et de gestion du changement ont eu lieu en 2017 :**
  - ✓ Sensibilisation générale des acteurs concernés via les comités cités
  - ✓ Digital Days avec un stand sur la protection des DCP sur les nouvelles technologies
  - ✓ Formation en présentiel sur les fondamentaux de la protection des DCP
  - ✓ MooC sur les fondamentaux RGPD indexé sur l'intéressement financier de l'entreprise : 85% de QCM validés

# ....la sensibilisation s'est poursuivie en 2018

- ✓ Poursuite des comités projet RGPD + lancement des comités RILs
- ✓ Vidéo du Directeur Général diffusé à tous les collaborateurs du Groupe le 25 mai 2018 : jour « J »
- ✓ Matinée « Remerciements des acteurs projets » en présence du Directeur Général :

- ✓ stands, affiches, gâteaux aux couleurs du RGPD, goodies,...

- ✓ une animation « dessiner ses idées et le RGPD »



## ...la sensibilisation s'est poursuivie en 2018

- ✓ **Montée en compétence du réseau de RIL :**  
séminaire d'une journée délocalisée animée par le Directeur de projet et le service DPO
- ✓ **Séminaire avec les DPOs des filiales internationales** animé par le DPO Groupe en novembre
- ✓ **MooC RGPD ciblé pour les informaticiens**
- ✓ **Formation en ligne sur les fondamentaux RGPD** faisant partie des modules pour validation d'une partie de l'intéressement
- ✓ **Formation sur les fondamentaux RGPD en présentiel**
- ✓ **Formation RGPD de l'ensemble du Comex**
- ✓ **Formation RGPD du Conseil d'Administration**



**Sommaire**

- Généralités, historique et principes du RGPD
- Impacts de l'application du RGPD
- Le RGPD chez CNP Assurances
- Sécurité des DCP

# Sensibilisation en 2019

- ✓ **Montée en compétence du réseau de RILs :**
  - ✓ Comités RIL toutes les 6 semaines
  - ✓ Formations spécifiques :
  - ✓ Comment construire une mention d'information sur un document de collecte →
  - ✓ Comment faire un PIA →
  
- ✓ **Montée en compétence de l'équipe DPO :**
  - ✓ Formation RGPD Assurances
  - ✓ Association de DPOs AFCDP : Université, réseau social professionnel, veille réglementaire
  - ✓ Conférences Privacy
  - ✓ Groupe de travail Protection des données personnelles au sein de la Fédération Française de l'Assurance
  - ✓ Réflexion en cours sur la certification de l'équipe DPO
  - ✓ MooC récent de la CNIL

## Sommaire

### Les mentions d'information

1. Définition : quelle est la définition d'une mention d'information ?
2. Les mentions types
3. Adaptation et réalisation d'une mention
4. Outils à disposition : référentiel d'accountability et tableau de suivi des mentions
5. Rappel du processus
6. Quizz

### L'exercice des droits

1. L'exercice de droits renforcé : délai, droits prévus par la LIL, droits prévus par le RGPD,...
2. Rappel du processus actuel
3. Quizz
4. Les difficultés rencontrées

## Sommaire

### Le registre des traitements et l'analyse d'impact sur la vie privée (PIA)

1. Qu'est-ce qu'un traitement de données ?
2. Qu'est-ce que le registre des traitements et le PIA ?
3. Quel est le contenu d'un PIA ?
4. Dans quels cas doit-on réaliser ou modifier un PIA ?
5. Processus des actions à mener dans le cas d'un nouveau traitement
6. Processus des actions à mener dans le cas de modification du PIA d'un traitement existant
7. Processus : Fin de vie d'un traitement

### Mode opératoire : Outil PIA

# Sensibilisation en 2019



Environ 1200  
collaborateurs formés  
en 2018 et en T1 2019

- ✓ Le 28 janvier 2019 : « Privacy Day » avec une animation sur plusieurs sites du Groupe CNP Assurances, et notamment en France sur 3 sites : « Comprendre le principe du Privacy By Design » avec brochure, guide, stand question/réponse
- ✓ Nouvel outil dédié au réseau de RIL comprenant la documentation RGPD : toolkit, bibliothèque pour chaque BU/FG
- ✓ Nouvel Intranet de la Direction de la Conformité Groupe avec un volet RGPD pour tous les collaborateurs
- ✓ Sensibilisation des assistantes de directions lors d'un séminaire annuel
- ✓ Sensibilisation des enfants des salariés à la protection des DCP
  
- ✓ Formation des collaborateurs sur les fondamentaux RGPD avec des cas pratiques et une partie dédiée à la Sécurité IT animée par RSSI : outil de vote en ligne par un outil Beekast
- ✓ Formation spécifique pour les collaborateurs de la DRH avec des cas pratiques : 2 sessions
- ✓ Formation obligatoire de la fonction Achats et des prescripteurs sur la «Contractualisation » avec des tiers comportant des cas pratiques – plusieurs sessions
- ✓ Formation spécifique obligatoire pour tous les informaticiens en présentiel : – plusieurs sessions
- ✓ A venir : réflexion sur la certification du dispositif de formation

# Importance et motivation d'une sensibilisation globale



- ✓ **Augmentation de la culture générale + création de bons réflexes**
- ✓ **Avantage concurrentiel**
- ✓ **Indispensable pour respecter le principe « privacy by design » (obligation réglementaire)**
- ✓ **Utile dans la vie professionnelle et dans la vie privée**

## **Tendance :**

- 1/ Continuité du change management chez CNP Assurances (pas de changements majeurs)**
- 2/ Renforcement du dispositif en France et déploiement à l'international**

4

**Questions/Réponses**



