



AG2R LA MONDIALE

Mai 2018

# **POLITIQUE DE PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL**

Approuvée par le Comité de Direction de La Mondiale  
Europartner en date du 2 mai 2018.

# SOMMAIRE

1.	CONTEXTE D'APPLICATION .....	3
1.1.	Objectifs.....	3
1.2.	Enjeux.....	3
1.3.	Périmètre.....	3
2.	PRINCIPES .....	4
2.1.	Contexte Métier LA MONDIALE EUROPARTNER.....	4
2.2.	Responsabilisation des différents acteurs .....	4
2.3.	Transparence.....	4
2.4.	Proportionnalité des mesures de protection.....	4
2.5.	Support aux métiers.....	5
3.	CADRE ET PRINCIPES DE LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL.....	5
4.	RÔLES ET RESPONSABILITÉS .....	5
4.1.	Fonction protection des données.....	5
4.2.	Fonction système d'information.....	8
4.3.	Fonction sécurité.....	9
4.4.	Fonction juridique .....	9
4.5.	Fonctions gestion des risques, contrôle interne et conformité.....	10
4.6.	Fonction Audit Interne .....	10
4.7.	Responsables conjoints de traitements et sous-traitants.....	10
5.	GOVERNANCE ET REPORTING.....	10
5.1.	Comité protection des données à caractère personnel.....	10
6.	GLOSSAIRE .....	11



# 1. CONTEXTE D'APPLICATION

## 1.1. Objectifs

La présente politique de protection des données à caractère personnel (ci-après la « Politique ») énonce les principes de protection des données à caractère personnel dont la société LA MONDIALE EUROPARTNER S.A. (ci-après la « Société » ou « LA MONDIALE EUROPARTNER ») est dépositaire. Elle définit le cadre de l'organisation de cette protection et les rôles et responsabilités des acteurs qui interviennent dans les opérations de traitement des données à caractère personnel. Les principaux objectifs de la protection des données à caractère personnel sont d'assurer :

- le respect des droits et de la vie privée des personnes concernées ;
- le traitement loyal et transparent de leurs données à caractère personnel ;
- l'application de la réglementation et des bonnes pratiques professionnelles.

## 1.2. Enjeux

La Société s'est construite dans l'intérêt exclusif de ses assurés avec pour ambition de protéger leur vie, leurs proches et leur patrimoine. A ce titre elle se voit confier des informations qui touchent au privé et parfois à l'intime.

La confidentialité et la sécurité de ces informations est une condition de la confiance indispensable à ses activités et à son développement.

L'exercice des activités de la Société suppose le traitement de grandes quantités de données à caractère personnel qui constituent une part importante du patrimoine informationnel dont elle est responsable et une source de valeur tant pour elle que pour la communauté de ses assurés.

A l'égard de ses propres collaborateurs, dans le cadre de sa gestion des ressources humaines, la Société veut garantir le meilleur niveau de préservation des droits des salariés et de protection de leurs informations.

Le respect de la réglementation et des usages en matière de protection de la vie privée et des données à caractère personnel est une condition de légitimité et de crédibilité pour notre Société qui, par vocation, met la personne au cœur de son modèle économique et sociétal.

## 1.3. Périmètre

La Politique couvre :

- la société La MONDIALE EUROPARTNER et ses succursales ainsi que ses partenaires et ses sous-traitants ;
- l'ensemble des métiers de la Société, à savoir l'élaboration et la commercialisation de produits d'assurance-vie et de contrats de capitalisation ;
- L'ensemble des personnes dont les données sont traitées par la Société et notamment :
  - les clients, les assurés, les bénéficiaires et les prospects ;
  - les salariés et tous les autres collaborateurs ;
  - les personnels des partenaires et prestataires ;
  - les administrateurs, les contacts professionnels...



## 2. PRINCIPES

### 2.1. Contexte Métier LA MONDIALE EUROPARTNER

La Société se conforme aux dispositions légales et réglementaires et aux recommandations et décisions des autorités de contrôle de la protection des données dont elle dépend (la Commission Nationale pour la Protection des Données (CNPD) au Grand-Duché de Luxembourg).

Nous tenons compte des spécificités de nos activités qui déterminent des conditions particulières d'application des règles, notamment en matière de :

- traitement de catégories particulières de données au sens de la réglementation (données de santé en particulier) ;
- mise en œuvre de traitements de données sensibles ou spécialement protégées (ex : numéro d'identification fiscale) ;
- collecte indirecte des informations personnelles ;
- gestion d'informations confidentielles de ses clients et de ses collaborateurs.

### 2.2. Responsabilisation des différents acteurs

La Société met en place une organisation qui s'appuie sur les compétences et la responsabilisation des personnes impliquées dans des opérations liées aux données à caractère personnel. Nous sensibilisons et mettons en œuvre des formations dédiées à la protection des données afin de renforcer la vigilance et la connaissance de tous.

Les Directeurs, membres du Comité de Direction garantissent, chacun pour son domaine et collectivement pour les traitements transverses, la conformité des opérations de traitement aux règles de protection de la vie privée et des données des personnes internes et externes concernées par les activités qu'ils dirigent.

### 2.3. Transparence

La Société adopte une démarche loyale et transparente en matière de traitement des données à caractère personnel. A ce titre elle met en œuvre une information complète, claire et aisément accessible sur les traitements qu'elle met en œuvre et les droits des personnes concernées sur leurs données à caractère personnel.

Elle s'interdit de communiquer les données qui lui sont confiées sans information préalable ou sans accord des personnes concernées, sauf dans le cas où elle y est obligée par la loi.

Elle ne collecte ni ne traite d'informations sur les personnes à leur insu ou à des fins incompatibles avec celles pour lesquelles les données ont été collectées.

### 2.4. Proportionnalité des mesures de protection

La Société met œuvre une approche par les risques qui permet d'évaluer les risques sur les personnes concernées. Cette approche permet d'identifier les mesures organisationnelles ou techniques appropriées et efficaces pour la protection des données à caractère personnel.



## 2.5. Support aux métiers

La Société met en place une organisation et des moyens d'accompagnement des métiers pour qu'ils puissent réaliser leurs objectifs et développer des initiatives tout en s'assurant du respect de la vie privée des personnes concernées par les traitements qu'ils mettent en œuvre. Cet engagement permet de proposer des services adaptés à nos clients dans un environnement de confiance et de transparence.

## 3. CADRE ET PRINCIPES DE LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Les traitements des données à caractère personnel mis en œuvre par la Société sont encadrés par le règlement général sur la protection des données (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, ci-après le « Règlement ») ainsi que par toute législation et/ou réglementation mettant en œuvre ces dispositions.

La Société s'engage à ne mettre en œuvre que des traitements licites sur la base des fondements juridiques prévus par le Règlement : le consentement de la personne concernée, l'exécution d'un contrat conclu avec elle ou l'exécution de mesures précontractuelles prises à la demande de celle-ci, le respect d'une obligation légale ou l'intérêt légitime poursuivi par la Société dès lors que le traitement ne porte pas atteinte aux droits des personnes.

Elle ne collecte que les données nécessaires à des finalités légitimes et déterminées et assure une information complète des personnes sur l'utilisation et les durées de conservation de leurs données ainsi que sur leurs droits.

Elle garantit les droits des personnes sur leurs données personnelles (droit d'accès, de rectification, d'effacement et de portabilité) et sur les traitements (droit d'opposition ou de limitation et droit de ne pas faire l'objet d'une décision automatisée).

Elle met en place des mesures de sécurité proportionnées tenant compte de la sensibilité des données, de la nature des traitements et des risques encourus par les personnes en cas d'indisponibilité des traitements ou d'atteinte à l'intégrité ou la confidentialité des données. Elle prend en compte ces risques dès la conception des traitements.

En cas de recours à une prestation portant sur des données à caractère personnel, elle choisit des sous-traitants apportant des garanties suffisantes en matière de protection des données à caractère personnel.

## 4. RÔLES ET RESPONSABILITÉS

### 4.1. Fonction protection des données

#### 4.1.1. Responsable de traitement

Le responsable de traitement est la personne morale qui détermine la fin et les moyens du traitement. Il s'agit principalement de la Société, dans le cadre des activités qu'elle



exerce ou du personnel qu'elle emploie. Toutefois, cette dernière peut agir seule ou conjointement avec d'autres entités juridiques (voir notamment l'article 4.8. de la présente politique).

#### *4.1.2. Direction Générale*

Le Directeur Général et tous les membres du Comité de Direction approuvent la Politique. Le Directeur Général s'assure de sa mise en œuvre.

Il détermine, dans le cadre des délégations de pouvoirs, les responsabilités en matière de mise en œuvre des traitements de données à caractère personnel par les directions de la Société.

Le Directeur Général désigne un délégué à la protection des données (ci-après le « DPD » ou le « Délégué à la protection des données ») et s'assure que ce dernier dispose des moyens nécessaires à l'exercice de ses missions comme le prévoit la réglementation. Il approuve les engagements de protection des données à caractère personnel portés à la connaissance des personnes concernées par les traitements mis en œuvre par la Société.

#### *4.1.3. Responsable de la mise en œuvre du traitement*

Chaque Directeur met en place dans son périmètre de responsabilité l'organisation permettant de garantir que les traitements de données à caractère personnel respectent la présente Politique. C'est le « responsable de la mise en œuvre des traitements » pour les activités qui lui sont rattachées.

Le responsable de la mise en œuvre du traitement est à l'origine du besoin justifiant la mise en place d'un traitement. Il est le garant de la conformité du traitement, de la mise à jour de la documentation de celui-ci et de la coordination des acteurs assurant son exécution. Différents acteurs peuvent être mis à contribution pour la mise en œuvre d'un traitement, notamment :

- le responsable ou chef de projet : il assure la mise en œuvre des règles de gestion Métier et l'exécution opérationnelle du traitement ;
- le responsable informatique : il assure la mise en œuvre des traitements informatiques et des conceptions techniques du traitement ;
- les collaborateurs au sein de la Direction : ils conduisent les opérations conformément aux règles et procédures utiles au bon déroulement du traitement ;
- le partenaire ou sous-traitant : il assure l'exécution de tout ou partie du traitement pour le compte de la Société.

#### *4.1.4. Relai à la protection des données à caractère personnel*

Le responsable de la mise en œuvre du traitement désigne, dès lors que la nature des activités et des traitements mis en œuvre le justifie, et en concertation avec le DPD, un relai de ce dernier en charge de mettre en œuvre la politique et les procédures dans son périmètre, et lui fournit le temps et les moyens d'assurer pleinement ses missions de relai.

Une telle désignation est spécialement utile pour :

- le périmètre du digital qui couvre les activités, gouvernance et qualité des données, expérience clients, marketing, services numériques et innovation très concernées par la protection des données à caractère personnel ;
- le Département Informatique, en raison du nombre de fonctions et d'acteurs de ce département impliqués dans la mise en œuvre de solutions de traitement de données à caractère personnel ;
- la Direction des Ressources Humaines, qui met en œuvre les systèmes de gestion des informations des collaborateurs de la Société.



Les missions de relai à la protection des données personnelles et de référent « qualité et usages data métier » peuvent être attribuées à une même personne. Lorsque ces missions sont affectées à des titulaires différents, ces derniers coopèrent sur les chantiers concernant les données de personnes physiques.

Les coordonnées des relais à la protection des données personnelles désignés conformément au présent article sont transmises au Délégué à la protection des données.

### **Rôle du relai à la protection des données personnelles**

Le relai possède une vision globale des activités et des processus au sein de sa Direction, ce qui lui permet :

- de relayer les principes et les règles de protection des données au sein de sa Direction ;
- de sensibiliser les acteurs au sein de sa Direction à la protection des données à caractère personnel ;
- de constituer un premier niveau de réponse et de conseil sur les bonnes pratiques de protection des données à caractère personnel au sein de sa Direction ;
- de contribuer à la mise en œuvre des mesures de protection des données ;
- d'alerter le DPD et le responsable de la mise en œuvre du traitement en cas de constatation d'une non-conformité aux règles et/ou mesures relatives à la protection des données à caractère personnel.

#### ***4.1.5. Délégué à la protection des données (DPD)***

Compte tenu des opérations de traitement, du nombre et de la nature des données à caractère personnel que la Société est amenée à collecter et à traiter, elle est soumise à l'obligation de désignation d'un Délégué à la protection des données à caractère personnel.

### **Fonctions de délégué à la protection des données**

Le Délégué à la protection des données :

- est associé de manière appropriée et en temps utile, à toutes les questions relatives à la protection des données à caractère personnel;
- lui sont fournies les ressources nécessaires à l'exercice de ses missions et à l'entretien de ses connaissances ;
- il peut accéder aux données et aux opérations de traitement ;
- il remplit sa mission de façon indépendante et rapporte directement au Comité de Direction ;
- qu'il peut être directement contacté par les personnes concernées par les traitements ;
- qu'il est soumis au secret professionnel ou à une obligation de confidentialité en ce qui concerne l'exercice de ses missions.



## **Missions du délégué à la protection des données**

La réglementation fixe également un cadre de missions qui se décline comme suit dans notre Société :

### √ Missions d'information et de conseil :

Le DPD, avec l'appui du Département Informatique (en ce qui concerne les problématiques liées aux enjeux de conformité des Systèmes d'Information), du Département Communication et de la Direction des Ressources humaines, contribue à mettre en place des actions d'information, de sensibilisation et de formation des collaborateurs de la Société afin de favoriser une culture de la protection des données à caractère personnel et de permettre l'acquisition de compétences spécifiques dans les activités où elles sont utiles.

Il apporte un conseil aux Directions et aux acteurs des Systèmes d'Information pour la mise en œuvre de traitements de données à caractère personnel que ce soit dans le cadre de projets d'évolution des systèmes d'information ou d'opérations de toutes natures impliquant la collecte, le transfert, la conservation ou l'utilisation de données à caractère personnel. Dans ce cadre, il effectue toute recommandation aux acteurs des Systèmes d'Information destinée à favoriser un meilleur niveau de conformité légale des traitements impactant des données à caractère personnel.

Il conduit ou intervient pour avis dans les analyses d'impact relatives à la protection des données à caractère personnel.

### √ Missions de contrôle :

Il contrôle l'application des dispositions réglementaires en matière de protection des données à caractère personnel par la Société et ses sous-traitants, notamment en s'appuyant sur la fonction de contrôle interne en place.

Il est autorisé à prendre toute initiative pour conduire les vérifications, et les directions contrôlées coopèrent à leur réalisation. Il rend compte des résultats de ces contrôles aux responsables concernés et à la Direction Générale.

### √ Missions d'interlocuteur de l'autorité de contrôle :

Le DPD est désigné auprès de l'autorité de contrôle, avec laquelle il coopère, il est le point de contact de cette dernière y compris pour les consultations préalables à la mise en œuvre de traitements à risques pour les personnes.

Il reçoit et instruit les réclamations des personnes relatives à tout traitement de données à caractère personnel et coopère avec la CNPD dans le cadre de l'instruction des plaintes reçues par l'autorité.

## **4.2. Fonction système d'information**

En charge du développement, de l'intégration et de l'exploitation des systèmes automatisés de traitement, cette fonction dont la responsabilité est confiée au Département Informatique conçoit et met en œuvre une organisation et des solutions informatiques internes ou sous-traitées qui respectent les principes et les exigences de la





réglementation et de cette politique, à savoir :

- l'approche par les risques et la prise en compte des risques pour la vie privée et les données à caractère personnel en amont des projets et dans le cadre des choix de solutions ;
- l'utilisation de méthodes de conception et de développement respectant les principes du privacy by design ;
- la définition et la mise en œuvre de méthodes, de solutions de développement et de fonctionnement respectant par défaut la primauté du respect de la vie privée des personnes dont les données sont gérées (privacy by default) ;
- la mise en œuvre des solutions organisationnelles et techniques permettant d'assurer des niveaux de sécurité et de disponibilité adéquats et de respecter les droits sur les données à caractère personnel (droit d'accès, d'opposition, à l'effacement, à la portabilité, à la limitation) ;
- le respect des règles relatives aux transferts des données hors de l'Union européenne.

### 4.3. Fonction sécurité

La Société met en œuvre des politiques et des procédures de sécurité et de continuité garantissant la disponibilité, l'intégrité et la confidentialité des données à caractère personnel.

Le Département Informatique supervise la mise en œuvre de ces dispositifs.

À partir d'analyses des risques, il proportionne les mesures de sécurité au niveau de sensibilité des traitements en fonction des menaces qui pèseraient sur les personnes en cas d'atteinte à leurs données.

Il réévalue périodiquement l'efficacité des mesures mises en œuvre et les adapte en tenant compte de l'évolution des risques et de l'état de l'art en matière de protection.

Il pilote la réalisation des évaluations d'impacts sur la vie privée et la gestion des incidents de sécurité notamment à la notification des violations de données à caractère personnel.

### 4.4. Fonction juridique

La Direction Juridique sécurise les engagements de la Société en matière de protection des données à caractère personnel au travers de la rédaction et de la validation des contrats, conventions et supports d'information.

Elle apporte ses conseils au DPD dans la gestion des réclamations et des plaintes, et dans le cadre des relations avec la CNPD.

La Direction Juridique prend en charge les litiges et contentieux nés de l'application de la réglementation. Dans ce cadre, elle assure la relation avec les professions judiciaires et la représentation auprès de tribunaux et de la CNPD en cas de procédure pouvant conduire à une sanction.



## 4.5. Fonctions gestion des risques, contrôle interne et conformité

La gestion des risques pour les données à caractère personnel se conforme à la politique et s'inscrit dans l'organisation de gestion des risques opérationnels et de la conformité de la Société.

Le DPD rend compte de la gestion de ces risques auprès du Comité des risques. La gestion des risques, dans le cadre de la protection des données personnelles, vise à évaluer les risques encourus pour la vie privée des personnes concernées.

Les contrôleurs internes de la Société et les correspondants risques opérationnels (CRO) recensent et évaluent les risques et suivent la mise en œuvre des actions de maîtrise pour les réduire, ils rendent compte de cette gestion, déclarent et instruisent les incidents dans ce domaine. Ils participent aux analyses d'impacts sur la vie privée mis en œuvre conformément à la réglementation pour les traitements à risques.

Le dispositif de gestion de risque en matière de protection des données à caractère personnel s'inscrit également dans la gestion du risque de non-conformité en collaboration avec la fonction conformité de la Société.

## 4.6. Fonction Audit Interne

L'audit interne entend annuellement le DPD, il intègre à son programme des missions visant à évaluer la protection des données à caractère personnel au sein de la Société.

## 4.7. Responsables conjoints de traitements et sous-traitants

Lorsque la Société détermine conjointement les finalités et les moyens du traitement avec un autre Responsable de traitement, ils sont responsables conjoints du traitement. Dans cette hypothèse, la Société met en place des conventions définissant de manière transparente les obligations respectives des parties aux fins d'assurer le respect des exigences de la réglementation, notamment en ce qui concerne l'exercice des droits de la personne concernée, et leurs obligations respectives quant à la communication des informations qui doivent être portées à la connaissance des personnes concernées.

Lorsqu'un traitement doit être effectué pour le compte de la Société celle-ci fait uniquement appel à des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du Règlement et de la présente politique et garantisse la protection des droits de la personne concernée.

# 5. GOUVERNANCE ET REPORTING

## 5.1. Comité protection des données à caractère personnel

La Société met en place une instance de suivi et d'échanges autour de la protection des données à caractère personnel.

### ***Participants :***

- Les membres du Comité de Direction ;



- Le Délégué à la Protection des Données ;
- Les référents opérationnels de chaque Direction.

### **Fréquence :**

Semestriel

### **Objet :**

- Décrire et partager l'état global de la protection des données personnelles au sein de la Société (présentation des indicateurs pertinents) ;
- Prendre connaissance des résultats d'audits et de contrôles et suivre la mise en œuvre des actions d'amélioration ;
- Suivre le plan des formations et les actions de sensibilisation.

Il est rendu compte de ces travaux en Comité de Direction et en Comité des risques.

## 6. GLOSSAIRE

**Données à caractère personnel** : toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»). Est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

**Données sensibles** : toutes les données qui relèvent de l'origine raciale ou ethnique, des opinions politiques, des convictions religieuses ou philosophiques ou de l'appartenance syndicale, ainsi que les données génétiques, les données biométriques, les données concernant la santé ou des données concernant la vie sexuelle sont considérées comme données sensibles.

**Traitement** : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

**Responsable du 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. Lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.

**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.



**Destinataire** : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel, qu'il s'agisse ou non d'un tiers. Toutefois, les autorités publiques qui sont susceptibles de recevoir communication de données à caractère personnel dans le cadre d'une mission d'enquête particulière conformément au droit de l'Union ou au droit d'un État membre ne sont pas considérées comme des destinataires ; le traitement de ces données par les autorités publiques en question est conforme aux règles applicables en matière de protection des données en fonction des finalités du traitement.

**Violation de données à caractère personnel** : une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.

**Autorité de contrôle** : une autorité publique indépendante qui est instituée par un État membre, pour le Luxembourg : la Commission nationale pour la protection des données (CNPD).

**Profilage** : toute forme de traitement automatisé de données à caractère personnel consistant à utiliser ces données à caractère personnel pour évaluer certains aspects personnels relatifs à une personne physique, notamment pour analyser ou prédire des éléments concernant le rendement au travail, la situation économique, la santé, les préférences personnelles, les intérêts, la fiabilité, le comportement, la localisation ou les déplacements de cette personne physique.

