Nos engagements RGPD

AXA Epargne Entreprise - mai 2018

Règlement Général sur la Protection des données

Madame, Monsieur,

Avec l'entrée en vigueur règlement européen sur la protection des données (RGPD), vous vous posez légitimement des questions sur la mise en conformité de notre société.

Ce document est là pour vous donner la transparence nécessaire sur les différentes mesures déployées et réaffirmer la volonté d'AXA Epargne Entreprise de protéger vos données.

1. Une activité de teneur de compte fortement réglementée

Les activités d'AXA Epargne Entreprise sont réglementées par de nombreux textes.

Outre la loi française dite « Informatique et Libertés », connue pour avoir très tôt été particulièrement protectrice des données personnelles, et aujourd'hui le RGPD, AXA Epargne Entreprise est également soumise à des normes et réglementations de protection particulièrement exigeantes pour le secteur bancaire (code monétaire et financier, recommandations de l'Autorité de contrôle prudentiel et de résolution, Règlement général AMF…).

Ces différents textes encadrent et sécurisent notre activité.

Comme teneur de compte, AXA Epargne Entreprise est donc, plus que les entreprises d'autres secteurs, particulièrement sensibilisée et responsabilisée sur la protection des données personnelles.

2. Un statut de responsable de traitement du fait de la spécificité de notre métier

De par la spécificité de ses activités, AXA Epargne Entreprise, lorsqu'elle intervient en tant que teneur de compte, se positionne comme responsable de traitement au sens de l'article 4 du RGPD, à savoir celui qui « détermine les finalités et les moyens du traitement ».

Elle remplit effectivement l'ensemble des critères en ce sens lorsqu'elle intervient comme teneur de compte, tels que détaillés par l'avis 1/2010 du G29, toujours d'actualité dans la mesure où l'article 4 du RGPD n'a pas modifié la définition de responsable de traitement, comme :

- « être responsable du traitement résulte essentiellement du fait qu'une entité a choisi de traiter des données à caractère personnel pour des finalités qui lui sont propres » en page 11,

- « le degré de contrôle réel exercé par une partie, l'image donnée aux personnes concernées et les attentes raisonnables que cette visibilité peut susciter chez ces dernières » en page 14.

- « la détermination des «moyens» englobe donc à la fois des questions techniques et d'organisation, auxquelles les sous-traitants peuvent tout aussi bien répondre (par exemple, «quel matériel informatique ou logiciel utiliser?»), et des aspects essentiels qui sont traditionnellement et intrinsèquement réservés à l'appréciation du responsable du traitement, tels que «quelles sont les données à traiter?», «pendant combien de temps doivent-elles être traitées?», «qui doit y avoir accès», etc. » (page 15),

- « la détermination de la finalité du traitement est réservée au responsable du traitement. Toute personne qui prend cette décision est donc un responsable du traitement (de fait) » en page 16.

Appliqué à un contrat d'épargne salariale, c'est bien AXA Epargne Entreprise, qui détermine la finalité principale du traitement de tenue de compte (ouverture de compte, gestion, lutte contre le blanchiment, lutte contre la fraude…) et les moyens essentiels pour la réalisation de ces traitements (sélection des données nécessaires, durée de conservation…).

Dans ce cadre, à titre d'exemple, une entreprise qui souhaiterait souscrire un contrat d'épargne salariale au bénéfice de ses salariés, interviendrait quant à elle en tant que responsable du traitement des données de ses salariés : ce traitement ayant pour finalité la gestion du contrat de travail incluant notamment la souscription par l'entreprise d'un contrat d'épargne salariale au bénéfice de ses salariés. Dans ce contexte cette entreprise pourrait être amenée à transférer les données de ses salariés à AXA Epargne Entreprise, teneur de compte. Il s'agirait donc d'un transfert de données de responsable de traitement dont la finalité est la gestion des ressources humaines à responsable de traitement dont la finalité est la gestion du contrat épargne salariale.

Ainsi, de par la spécificité du métier de teneur de compte, celui-ci n'est pas assimilable à un fournisseur ou prestataire de service qui aurait vocation à participer à tout ou partie d'un traitement de données personnelles comme sous-traitant. Il ne lui est pas délégué une tâche ou fonction qu'une entreprise souscriptrice d'épargne salariale pourrait exercer elle-même mais aurait choisi de lui confier.
Cela parce que la tenue de compte et la conservation de parts est est un métier qui exige un agrément et une expertise bien particulière.

Dans ce contexte, AXA Epargne Entreprise est légitime, en tant que responsable de traitement, à collecter, traiter et conserver, aussi longtemps que nécessaire, les données à caractère personnel dont elle a besoin pour exercer ses activités et remplir ses obligations.
L'article 28 du RGPD relatif au sous-traitant lui est ainsi inapplicable et il ne peut être exigé l'insertion des mentions et droits décrits à cet article au contrat d'épargne salariale, comme des normes particulières d'audit ou de sécurité, ou un questionnaire détaillé à compléter qui aurait pour objet la sous-traitance.
Toutefois, nous vous confirmons qu'en tant que responsable de traitement, AXA Epargne Entreprise assure évidemment la sécurité et la conformité de ses traitements avec la réglementation en vigueur et notamment le RGPD et la production de cette note a vocation à vous apporter les éléments nécessaires pour en juger.

3. Un DPO avec la double compétence data et sécurité

AXA Epargne Entreprise a fait le choix, en ma personne, d'un Data Protection Officer (DPO) qui exerce en même temps comme Chief Security Officer (CSO) avec des équipes dédiées.
De ce fait, la fonction bénéficie des leviers et compétences qui sont les miennes tant sur les aspects de protection des données personnelles que sur les aspects de de sécurité physique et logique de ces dernières.

Comme CSO, mes missions sont notamment de :

- veiller à la confidentialité et l'intégrité du système d'information (SI) et des informations qu'il contient en contrôlant les droits accès, habilitations et dérogations,
- définir et assurer la mise en œuvre des règles de sécurité à prendre en compte lors de la conception, le déploiement et la gestion de chaque activité d'AXA Epargne Entreprise,
- s'assurer que les collaborateurs sont conscients des enjeux, de leurs responsabilités en matière de sécurité des SI et qu'ils maîtrisent les comportements à adopter,
- identifier, gérer et traiter les risques encourus,
- gérer les incidents de sécurité et identifier et traiter les causes à l'origine des incidents de sécurité du SI.

Comme DPO, mes missions sont notamment de :

- assurer et contrôler la sécurité, l'intégrité et la confidentialité des données,
- assurer la sensibilisation et la formation des différentes parties prenantes,
- tenir à jour la liste des traitements de données à caractère personnel et en contrôler la conformité,
- conseiller les différentes entités de l'entreprise,
- garantir les droits de l'ensemble des adhérents (droits d'accès, de rectification, d'opposition...),
- veiller à la conformité continue d'AXA Epargne Entreprise au RGPD.

Pour garantir la bonne fin des missions qui m'ont été confiées, AXA Epargne Entreprise s'est imposée des politiques rigoureuses, à jour du RGPD, comme sa politique générale de sécurité des systèmes d'information et sa politique relative à la protection des données à caractère personnel.

4. Des contrôles internes et externes réguliers

AXA Epargne Entreprise fait par ailleurs l'objet de contrôles réguliers, qui garantissent une continuité et une qualité permanente de son niveau de protection des données :

- AXA Epargne Entreprise est auditée chaque année par ses Commissaires aux Comptes (Mazars et PWC) sur la gestion des droits d'accès à nos systèmes ainsi que sur d'autre sujets de sécurité,
- tous les sites web d'AXA Epargne Entreprise sont testés au moins une fois par an (tests d'intrusion) par des auditeurs externes tels que Ernst & Young, Deloitte ou Devoteam, qui sont régulièrement remis en concurrence pour éviter toute connivence,
- le département d'audit du groupe AXA , maison mère d'Axa Epargne Entreprise, vérifie régulièrement le niveau de sécurité d'AXA Epargne Entreprise,
- les autorités de tutelle des teneurs de compte et investisseurs de parts, l'ACPR, peuvent auditer la gestion du groupe AXA et ses filiales en matière de gouvernance de la sécurité,
- le DPO du groupe AXA réalise au moins trois fois dans l'année une revue de l'effectivité de la protection des données à caractère personnel mise en place par AXA Epargne Entreprise.

5. Un programme de mise en conformité complet

AXA Epargne Entreprisee a, comme toute entreprise européenne, mené un programme de mise en conformité au RGPD. Ce programme a débuté dès 2016 avec comme objectif une conformité complète en 2018.

Parmi les nombreux chantiers de ce programme, il y a notamment :

- l'envoi d'une notice d'information à l'ensemble des adhérents pour leur expliquer leurs nouveaux droits,
- le déploiement d'une nouvelle mention conforme à l'article 13 du RGPD dans nos documents à destination des adhérents,
- la révision des contrats avec nos prestataires sous-traitants pour y insérer une nouvelle clause type et une annexe dédiée avec les mentions requises par l'article 28 du RGPD, ou encore
- une procédure de détection et de notification des violations de données à caractère personnel de l'article 33 du RGPD.

Ce programme a bénéficié des débats conduits au sein de l'association française de gestion auxquels participent l'ensemble des teneurs de compte et leurs experts en RGPD.

6. Un engagement de tout le groupe AXA sur la protection des données

Le groupe AXA s'est engagé depuis longtemps dans la protection des données personnelles, avec des standards d'exigence déployés au sein de toutes ses sociétés et publiquement affichés, qui anticipaient sur le RGPD.

Le groupe AXA a également fait valider des Binding Corporate Rules (BCR) pour des transferts internationaux de données à l'intérieur de son groupe qui respecte la réglementation (ces documents sont en ligne sur le site https://www.axa.com/fr/a-propos-d-axa/nos-engagements).

Je reste à votre entière disposition pour toute information complémentaire dont vous souhaiteriez disposer.

Jérôme CONSIGNY
Data protection Officer
Chief Security Officer
AXA France

Les engagements d'AXA Epargne Entreprise dans l'utilisation de mes données personnelles

En qualité de teneur de compte, **AXA Epargne Entreprise se positionne comme responsable de traitement au sens de l'article 4 du Règlement Général sur le Protection des Données (RGPD)**, à savoir celui qui « détermine les finalités et les moyens du traitement ».

Dans ce contexte, AXA Epargne Entreprise est légitime à collecter, traiter et conserver, dans le respect des normes de conservation applicables au secteur d'activité, les données à caractère personnel dont elle a besoin pour exercer ses activités et remplir ses obligations.

Les activités d'AXA Epargne Entreprise sont réglementées par de nombreux textes.

Outre les normes et réglementations concernant l'activité de tenue de compte en Epargne Salariale (Règlement général AMF, Code monétaire et financier, …), **AXA Epargne Entreprise est également soumise à la loi française dite « Informatique et Libertés »**, connue pour avoir très tôt été particulièrement protectrice des données personnelles, et au **Règlement Général sur la Protection des Données (RGPD)**.

Ces différents textes et réglementation encadrent et sécurisent notre activité.

Pourquoi AXA Epargne Entreprise utilise mes données à caractère personnel ?

AXA Epargne Entreprise utilise vos données à caractère personnel pour s'acquitter de ses différentes obligations légales et réglementaires concernant :

- **La tenue de compte** de conservation dans le cadre d'un dispositif d'épargne salariale.
- **La lutte contre le blanchiment des capitaux et contre le financement du terrorisme**, avec la mise en place d'une surveillance des contrats pouvant aboutir à la rédaction d'une déclaration de soupçon ou à une mesure de gel des avoirs, en application du Code monétaire et financier.
- **La lutte contre la fraude.**
- **La collecte de données relatives aux infractions**, condamnations et mesures de sûreté soit au moment de la souscription du contrat d'épargne salariale, soit en cours de son exécution ou dans le cadre de la gestion de contentieux.

À quelle occasion AXA Epargne Entreprise collecte mes données à caractère personnel ?

Dans le cadre de la gestion de votre compte d'épargne salariale, **AXA Epargne Entreprise est amenée à collecter, traiter et conserver vos données à caractère personnel**. Ces données sont transmises par votre employeur lors de la souscription du contrat et actualisées tout au long de la vie de votre dispositif.

AXA Epargne Entreprise pourra également vous demander de mettre à jour vos données personnelles et/ou de communiquer des informations complémentaires dans le cadre d'une opération (versement, remboursement, arbitrage, demande de transfert…).

Vos données à caractère personnel sont utilisées pour les finalités ci-après :

Exécuter vos opérations
(versement, remboursement, arbitrage, demande de transfert…)

S'assurer de votre identité

Répondre aux obligations légales et réglementaires
mentionnées ci-dessus

Quelles sont les informations à caractère personnel obligatoires collectées par AXA Epargne Entreprise ?

Des **informations d'identification** et de contact : **date entrée dans l'entreprise, nom, prénom, numéro de sécurité sociale, date de naissance, ville et pays de naissance, nationalité, situation familiale, secteur d'activité professionnelle, adresse postale du domicile, pays de résidence, e-mail professionnel et/ou personnel, numéro de téléphone…**

Mes droits sur mes données personnelles

Je peux demander l'accès, la rectification, l'effacement ou la portabilité de mes données, définir des directives relatives à leur sort après mon décès, choisir d'en limiter l'usage ou m'opposer à leur traitement.
Si j'ai donné une autorisation spéciale et expresse pour l'utilisation de certaines de mes données, je peux la retirer à tout moment sous réserve qu'il ne s'agisse pas d'informations qui conditionnent l'application de mon contrat.
Je peux écrire au délégué à la protection des données pour exercer mes droits par e-mail (**service.informationclient@axa.fr**) ou par courrier (AXA France - Service Information Client - 313 Terrasses de l'Arche 92727 Nanterre Cedex). En cas de réclamation, je peux choisir de saisir la CNIL.

Pourquoi AXA Epargne Entreprise me pose des questions et me demande des justificatifs lorsque je fais un versement supérieur à 8 000 € ?

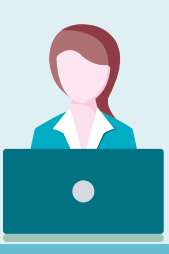
Compte tenu des risques que représentent le blanchiment de capitaux et le financement du terrorisme pour la société, les pouvoirs publics imposent aux entreprises du secteur financier (banques et assurances) de déceler, de façon précoce, à travers les opérations réalisées, les personnes susceptibles de participer à des activités illicites. Cela se traduit pour **AXA Epargne Entreprise par des obligations d'identification, de connaissance de ses clients et de vigilance constante** (1).

Le manquement à ces obligations peut entraîner des sanctions financières lourdes, voire des sanctions pénales. Pour ces raisons, AXA Epargne Entreprise peut être amenée à vous poser des questions sur votre situation professionnelle, sur votre patrimoine et vos revenus. Elle peut vous interroger sur l'origine des fonds versés sur votre contrat d'épargne salariale en application des articles L. 561-2 et suivants, ainsi que de l'article R. 561-16 du Code monétaire et financier :

- **En cas de versement supérieur à 8 000 €**, une déclaration d'origine des fonds vous sera demandée ainsi qu'une photocopie de votre carte nationale d'identité ou passeport en cours de validité.

- **En cas de versement supérieur à 50 000 €**, un justificatif d'origine des fonds de moins de 6 mois vous sera demandé ainsi qu'une photocopie de votre carte nationale d'identité ou passeport en cours de validité.

Puis-je refuser de répondre aux demandes d'informations et/ou de justificatifs d'AXA Epargne Entreprise ?



Lorsque AXA Epargne Entreprise n'a pas pu obtenir les informations ou les justificatifs nécessaires à son appréciation du risque de blanchiment ou de financement du terrorisme, elle a l'obligation de ne pas exécuter l'opération demandée (2).

Bon à savoir

- **Mes données à caractère personnel recueillies** par AXA Epargne Entreprise dans le cadre de la tenue des comptes ne peuvent pas être utilisées par AXA Epargne Entreprise et les sociétés du Groupe AXA en France à des fins de prospection commerciale sans accord express de ma part. Leur durée de conservation par AXA Épargne Entreprise est de trente ans conformément aux délais de prescription bancaire.
- **AXA Epargne Entreprise réalise des contrôles réguliers**, qui garantissent une continuité et une qualité permanente du niveau de protection de mes données.

Aller en haut de page

(1) Articles L. 561-5, L. 561-5-1 et L. 561-6 du code monétaire et financier.
(2) Articles L. 561-15, L. 561-23 et D. 561-33 du code monétaire et financier.

AXA Epargne Entreprise S.A. au capital de 19 770 132,20 €, Siren 428 191 027 RCS Nanterre, Siège social : 313 Terrasses de l'Arche 92727 Nanterre Cedex, Entreprise d'investissement, agréée en France par l'A.C.P.R. (4, place de Budapest - CS 92459 - 75436 Paris Cedex 09) sous le N°15573, habilitée à exercer la fonction de teneur de compte-conservateur de titres financiers, et à ce titre soumis au Code Monétaire et Financier.