

Informations concernant le traitement des données à caractère personnel

Aréas Assurances, en tant que responsable de traitement doit fournir à ses clients les informations visées aux articles 13 et 14 du règlement général sur la protection des données 2016/679 du 27 avril 2016 (ci-après RGPD) dans les conditions de l'article 12, ainsi que celles prévues par la loi du n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée.

1. Nature des informations à fournir à la personne concernée

1.1. Informations à fournir résultant du RGPD

1.1.1 - Informations obligatoires communes à tous les traitements

Ces informations sont visées aux articles 13 (1) ou 14 (1) du RGPD, à savoir :

- l'identité et les coordonnées du responsable de traitement,
- les coordonnées du délégué à la protection des données,
- les finalités du traitement auquel sont destinées les données à caractère personnel ainsi que les bases juridiques du traitement,
- les destinataires ou catégories de destinataires des données à caractère personnel,
- l'existence de transferts de ces données vers des pays hors de l'Union européenne.

1.1.2 - Informations complémentaires communes à tous les traitements

Les informations complémentaires sont celles visées aux articles 13 (2) (3) et 14 (2) (4) du RGPD :

- la durée de conservation des données ou les critères utilisés pour déterminer cette durée,
- l'existence des droits au profit de la personne concernée :
 - son droit d'accès ;
 - son droit de rectification ;
 - son droit d'effacement ;
 - son droit de limitation du traitement ;
 - son droit à la portabilité des données ;
 - son droit d'opposition qui est présenté séparément de toute autre information.
- l'existence du droit de retirer son consentement à tout moment lorsque le traitement est fondé sur le consentement effectué avant le retrait de celui-ci,
- le droit d'introduire une réclamation auprès d'une autorité de contrôle,
- les conditions de transferts de données vers un pays tiers hors Union Européenne.

1.2. Les informations spécifiques à certains traitements

1.2.1 - Lutte contre la fraude en assurances

Premier niveau : Information générale des personnes concernées sur le dispositif de lutte contre la fraude pouvant conduire à l'inscription sur la liste des personnes à risque. Il existe des modalités d'information distinctes en fonction des personnes visées.

Les personnes concernées sont informées de l'existence du traitement de lutte contre la fraude, au moyen des documents qui leur sont communiqués au moment de la souscription du contrat, ou de tout autre support de communication échangé lors de l'exécution du contrat. En assurance automobile, cette information vise également la mise en œuvre du dispositif mutualisé des données des contrats, et des sinistres déclarés auprès des assureurs, mis en œuvre par l'Agence pour la Lutte contre la Fraude à l'Assurance (ALFA).

Second niveau : En cas de détection d'une anomalie, d'une incohérence ou d'un signalement susceptible de relever d'une fraude, Aréas Assurances a la possibilité d'inscrire une personne sur une « liste de personnes présentant un risque de fraude ». La personne concernée, susceptible d'être inscrite sur cette liste peut être un assuré, un prestataire, un professionnel de santé etc.

Au cours de la période d'investigation, la personne concernée peut être contactée, selon le type de fraude suspectée (assuré, partenaire, salarié etc.), pour apporter des explications complémentaires. Au terme des investigations, et en cas de décision prise produisant des effets juridiques pouvant conduire à l'inscription sur la liste des personnes à risque, il existe des modalités d'information distinctes en fonction des personnes visées (refus de prise charge, avertissement au salarié, rupture de contrat). Une information écrite et individuelle est adressée précisant les mesures prises par Aréas Assurances (conséquences de l'application du contrat concerné) et lui donnant la possibilité de présenter ses observations.

1.2.2 - Assurance complémentaire santé

Pour l'assurance complémentaire santé, le cas échéant, l'information quant à la réutilisation possible de ces données, à des fins de recherche, d'étude ou d'évaluation dans le cadre du Système National des Données de Santé (SNDS).

2. Droits de la personne concernée

2.1. Droit d'accès, de rectification, d'opposition

Le droit d'accès peut porter sur toutes les données à caractère personnel relatives à la personne concernée.

Il permet à la personne concernée de demander directement au responsable d'un fichier s'il détient des informations sur elle et demander la communication de l'intégralité de ces données.

Le droit de rectification permet à la personne concernée de demander la rectification des informations inexacts la concernant.

Aréas Assurances notifie la rectification à chaque destinataire auquel les données à caractère personnel ont été communiquées à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés.

Le droit d'opposition permet à la personne concernée de s'opposer, pour des motifs légitimes, à figurer dans un fichier. En matière de prospection, notamment commerciale, ce droit peut s'exercer sans avoir à justifier d'un motif légitime.

2.2. Droit à l'effacement

Le droit à l'effacement oblige Aréas Assurances à effacer dans les meilleurs délais les données de la personne concernée lorsqu'elles ne sont plus nécessaires au traitement ou lorsque le traitement cesse du fait du retrait du consentement, du droit d'opposition, de l'illicéité du traitement ou afin de respecter une obligation légale.

Aréas Assurances notifie l'effacement à chaque destinataire auquel les données à caractère personnel ont été communiquées à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés.

La personne concernée dispose enfin du droit de définir des directives relatives à la conservation à l'effacement et à la communication de ses données à caractère personnel après son décès.

2.3. Droit à la limitation du traitement

La personne concernée a le droit d'obtenir du responsable de traitement la suspension du traitement lorsqu'elle conteste l'exactitude des données.

L'exercice de ce droit sera limité à la capacité d'Aréas Assurances d'exécuter le contrat.

2.4. Droit à la portabilité des données

Le droit à la portabilité ne concerne que les données à caractère personnel fournies par la personne concernée et traitées sur la base de son consentement ou de l'exécution d'un contrat.

En application de ce droit à la portabilité, la personne concernée a le droit de recevoir les données à caractère personnel la concernant qu'elle a fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine. Elle dispose en outre du droit de transmettre ces données à un autre responsable du traitement sans obstacle du responsable du traitement auquel les données à caractère personnel ont été communiquées.

Les documents tels qu'un fichier PDF ou un courrier électronique reçu de la personne concernée ne sont pas portables, seules les informations contenues dans ces documents qui sont utilisées par Aréas Assurances et donc seules les informations structurées et renseignées dans les systèmes d'information d'Aréas Assurances sont portables.

2.5. Droit d'obtenir une intervention humaine

Aréas Assurances peut avoir recours à des décisions individuelles automatisées y compris le profilage au sens de l'article 22 du RGPD, c'est-à-dire des décisions produisant des effets juridiques concernant la personne concernée ou l'affectant de manière significative de façon similaire.

En effet, ces décisions peuvent être nécessaires à la conclusion ou à l'exécution d'un contrat entre la personne concernée et Aréas Assurances ou fondées sur le consentement explicite de la personne concernée.

Lorsqu'Aréas Assurances a recours à ce type de décision individuelle automatisée, la personne concernée a le droit d'obtenir une intervention humaine de la part du responsable du traitement, d'exprimer son point de vue et de contester la décision.

2.6. Droit de retirer son consentement

La personne concernée dispose, lorsque le traitement est fondé sur le consentement, d'un droit de retrait de son consentement. Par exemple, la personne concernée peut retirer son consentement à la réception d'offres commerciales par voies électronique.

2.7. Voies de recours de la personne concernée

Toute personne concernée a le droit d'introduire une réclamation auprès d'une autorité de contrôle dans l'État membre dans lequel se trouve sa résidence habituelle, son lieu de travail ou le lieu où la violation aurait été commise.

La personne concernée dispose en matière de voies de recours d'un droit :

- d'introduire une réclamation auprès d'une autorité de contrôle de protection des données (CNIL en France),
- à un recours juridictionnel effectif contre une autorité de contrôle de protection des données,

- à un recours juridictionnel effectif contre un responsable de traitement ou un sous-traitant devant les juridictions de l'État membre dans lequel le responsable du traitement ou le sous-traitant dispose d'un établissement ou devant les juridictions de l'État membre dans lequel la personne concernée a sa résidence habituelle,
- de se faire représenter y compris dans le cadre d'une action de groupe,
- à réparation.

3. Destinataires

3.1. Destinataires communs à tous les traitements

Peuvent seuls dans les limites de leurs attributions respectives avoir accès aux données à caractère personnel :

- **dans le cadre des missions habituelles qui leurs sont assignées et dont ils doivent répondre :**
 - les personnels chargés de la passation, la gestion et l'exécution des contrats ;
 - les délégataires de gestion, les intermédiaires d'assurance, les partenaires ;
 - les prestataires ;
 - les co-responsables de traitement ;
 - les sous-traitants, ou les entités du groupe d'assurance auquel appartient Aréas Assurances dans le cadre de l'exercice de leurs missions ;
 - les organismes d'assurance chargés dans le cadre d'un contrat de partenariat de gérer les contrats d'assurance du responsable de traitement, y compris dans le cadre d'un réseau de soins ;
 - s'il y a lieu les organismes d'assurance des personnes impliquées ou offrant des prestations complémentaires ;
 - s'il y a lieu les co-assureurs et réassureurs ainsi que les organismes professionnels et les fonds de garanties ;
 - les personnes intervenant au contrat tels que les avocats, experts, auxiliaires de justice et officiers ministériels, curateurs, tuteurs, enquêteurs et professionnels de santé, médecins conseils et le personnel habilité ;
 - les organismes sociaux lorsque les régimes sociaux interviennent dans le règlement des sinistres ou lorsque les organismes d'assurances offrent des garanties complémentaires à celles des régimes sociaux ;
 - les organismes et associations pratiquant la prévention, l'action sociale ou la gestion de réalisations sanitaires et sociales.
- **en qualité de personnes intéressées au contrat :**
 - les souscripteurs, les assurés, les adhérents et les bénéficiaires des contrats ; et s'il y a lieu leurs ayants-droit et représentants ;
 - s'il y a lieu les bénéficiaires d'une cession ou d'une subrogation des droits relatifs au contrat ;
 - s'il y a lieu le responsable, les victimes et leurs mandataires ; les témoins, les tiers intéressés à l'exécution du contrat.
- **en qualité de personnes habilitées au titre des tiers autorisés :**
 - s'il y a lieu les juridictions concernées, les arbitres, les médiateurs ;
 - les ministères concernés, autorités de tutelle et de contrôle et tous organismes publics habilités à les recevoir ;
 - les services chargés du contrôle tels que les commissaires aux comptes et les auditeurs ainsi que les services chargés du contrôle interne.

3.2. Destinataires spécifiques à certains traitements

a) Dans le cadre de la consultation du Répertoire National d'Identification des Personnes Physiques (RNIPP) par l'intermédiaire de l'Association pour la Gestion des Informations sur le Risque en Assurance (AGIRA)

Les personnes habilitées à recevoir communication de ces données sont :

- au sein de l'AGIRA :
 - les gestionnaires habituels chargés de l'exploitation des fichiers.
- au sein des organismes d'assurance :
 - les gestionnaires habilités disposant de certificats individuels.

b) Dans le cadre de la lutte contre la fraude

- aux fins de lutte contre la fraude interne :
 - les personnes habilitées de la direction des ressources humaines pour des requêtes ponctuelles et individuelles réalisées dans le cadre d'enquêtes internes consécutives à la détection d'une fraude ;
 - le conseil de discipline saisi en cas de fraude ;
 - les représentants du personnel dans le cadre de l'accompagnement d'un salarié mis en cause pour fraude.
- aux fins de lutte contre la fraude interne et externe :
 - les personnels en relation avec la clientèle et les gestionnaires de contrats et de sinistres ;
 - les autres entités d'un même groupe dès lors qu'elles sont concernées par la fraude ou interviennent dans la gestion des dossiers ou de maîtrise du risque de fraude ;
 - les personnels habilités en charge de la lutte contre la fraude, de la lutte anti-blanchiment et du contrôle interne, les inspecteurs, enquêteurs, experts, et auditeurs ;
 - le personnel habilité de la direction générale, la direction juridique ou du service du contentieux pour la gestion des contentieux ;
 - le personnel habilité des sous-traitants.

Dès lors qu'ils sont directement concernés par une fraude, peuvent être destinataires des données relatives à cette fraude, les personnels habilités :

- des autres organismes d'assurance ou intermédiaires intervenant dans le cadre de dossier présentant une fraude,

- des organismes sociaux lorsque les régimes sociaux interviennent dans le règlement des sinistres ou lorsque les organismes d'assurances offrent des garanties complémentaires à celles des régimes sociaux,
- des organismes professionnels intervenant dans le cadre de dossiers présentant une fraude,
- les auxiliaires de justice et officiers ministériels,
- l'autorité judiciaire, médiateur, arbitre saisis d'un litige,
- les organismes tiers autorisés par une disposition légale à obtenir la communication de données à caractère personnel relatives à des précontentieux, contentieux ou condamnations,
- s'il y a lieu les victimes de fraudes ou leurs représentants.

La communication de ces données ne donne pas lieu à la création d'un fichier concernant les données relatives aux fraudes et mutualisé entre les destinataires.

Par exception et suite à l'autorisation de la CNIL, le dispositif ALFA mutualise des données des contrats d'assurance automobile et des sinistres déclarés auprès des assureurs pour lutter contre la fraude (?) en assurance.

c) Dans le cadre de la lutte contre le blanchiment des capitaux et le financement du terrorisme

- parmi les responsables de traitement :
 - les personnes en relation avec la clientèle et les gestionnaires de contrat et de sinistre pour les clients dont ils ont la charge à l'exception des informations relatives aux déclarations de soupçon ;
 - les personnes habilitées à prendre la décision de nouer ou de maintenir une relation d'affaires avec une personne politiquement exposée (PPE) ;
 - les personnels habilités du (ou des) service(s) chargé(s) de la lutte contre le blanchiment, notamment ceux ayant la qualité de correspondant ou de déclarant Tracfin, au sein des services de contrôle, d'audit ou juridique d'Aréas Assurances.
- parmi les autorités compétentes :
 - la cellule de renseignement financier Tracfin du ministère de l'économie, des finances et de l'industrie ;
 - les autorités de contrôle compétentes au sens de l'article L 561-36 du Code monétaire et financier (CMF) ;
 - pour les données relatives aux personnes qui font l'objet d'une mesure de gel des avoirs, la Direction générale du Trésor ;
 - les autorités de contrôle compétentes des autres états membres de la Communauté européenne, des états partie à l'accord sur l'Espace économique européen et des états où sont applicables les accords conclus avec l'Autorité de Contrôle Prudentiel et de Résolution ou l'Autorité des Marchés Financiers en application des dispositions prévues aux articles L 632-7 et L 632-13 du CMF.
- parmi les autres organismes financiers :
 - dans le respect des conditions posées au II de l'article L 561-7 du CMF, les personnes visées à l'article 1^{er} de la présente autorisation unique ;
 - dans le respect des conditions posées à l'article L 561-20 du CMF, les personnels habilités des autres organismes au sens de l'article 1^{er}, les compagnies financières et les compagnies financières holding mixtes, lorsqu'ils appartiennent à un même groupe tel que défini au III de l'article L 511-20 du CMF ou à l'article L 334-2 du Code des assurances, en ce qui concerne l'existence et le contenu de la déclaration de soupçon ;
 - dans le respect des conditions posées à l'article L 561-21 du CMF, les autres organismes au sens de l'article 1^{er} qui interviennent pour le même client dans la même transaction, en ce qui concerne l'existence et le contenu de la déclaration de soupçon.

4. Durées de conservation

En cas de conclusion d'un contrat d'assurance

Les données personnelles communiquées par les personnes intéressées ou générées du fait du contrat, sont conservées par Aréas Assurances conformément à la durée nécessaire à l'exécution du contrat. Ces données sont ensuite archivées selon les durées de prescriptions légales.

En l'absence de conclusion d'un contrat :

- les données de santé peuvent être conservées par Aréas Assurances pendant une durée de deux ans en archive courante et trois ans en archive intermédiaire à des fins probatoires dans l'hypothèse où l'assuré contesterait le refus d'assurance du responsable de traitement,
- s'agissant des autres données et notamment en matière de prospection commerciale, elles peuvent être conservées pendant un délai de trois ans à compter de leur collecte par Aréas Assurances ou du dernier contact émanant du prospect (demande de renseignements ou de documentation, par exemple).

5. Mesures de sécurité

5.1. Mesures générales de sécurité

Aréas Assurances a adopté des mesures appropriées afin de garantir un niveau de sécurité adapté aux risques présentés par les traitements mis en œuvre. Ainsi, Aréas Assurances prend toutes précautions utiles, notamment techniques et organisationnelles, pour préserver la sécurité, l'intégrité, la disponibilité et la confidentialité des données traitées, et notamment pour empêcher qu'elles soient déformées, endommagées ou que des tiers non autorisés puissent en prendre connaissance.

Aréas Assurances a défini une politique de sécurité adaptée aux risques présentés par les traitements. Celle-ci décrit les objectifs de sécurité, et les mesures de sécurité physique, logique et organisationnelle permettant de les atteindre.

Une gestion des habilitations permet de limiter l'accès aux données aux seules personnes dûment habilitées et autorisées à en connaître en fonction de leur profil.

Les accès aux traitements de données nécessitent une authentification des personnes accédant aux données au moyen d'un identifiant et d'un mot de passe individuels, robustes et régulièrement renouvelés.

Les conditions d'administration du système d'information prévoient l'existence de systèmes automatiques de traçabilité (journaux, audits etc.).

En cas de violation de données à caractère personnel susceptible d'engendrer un risque pour les droits et libertés des personnes physiques, le responsable du traitement doit la notifier, dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à l'autorité de protection des données compétente (CNIL).

Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le responsable du traitement communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, à moins que cette communication ne soit pas nécessaire en vertu des dérogations prévues à l'article 34 du RGPD.

5.2. Mesures de sécurité spécifique à l'utilisation d'un service de communication au public en ligne

Dans le cas de l'utilisation d'un service de communication au public en ligne, Aréas Assurance a pris les mesures nécessaires pour se prémunir contre toute atteinte à la confidentialité des données traitées.

Les données transitant sur des canaux de communication non sécurisés font ainsi l'objet de mesures techniques visant à les rendre incompréhensibles à toute personne non autorisée à y avoir accès.

5.3. Mesures de sécurité spécifiques au traitement des données de santé

S'agissant des données de santé, Aréas Assurances s'engage à respecter les dispositions prévues par le Code de bonne conduite annexé à la convention AERAS concernant la collecte et l'utilisation de données relatives à l'état de santé en vue de la souscription ou de l'exécution d'un contrat d'assurance.

5.4. Mesures de sécurités spécifiques au traitement des données par l'AGIRA

Les accès individuels à la base AGIRA s'effectuent après authentification mutuelle du système hébergeant le traitement et de l'utilisateur par le biais de certificats délivrés par le réseau d'accès aux données de l'assurance et de la messagerie sécurisée (RADAMESS). L'identification des machines connectées au traitement est également faite par des certificats de même nature.

Le certificat doit être nominatif et les mesures appropriées sont prises de manière à garantir qu'il ne sera utilisé que par son titulaire.

Aréas Assurances conserve l'historique des requêtes ponctuelles effectuée sous sa responsabilité et peut accéder aux interrogations conservées par l'AGIRA. Celle-ci garde une trace de toute interrogation pendant un an.

Toutes les connexions au traitement de données à caractères personnel font l'objet d'un chiffrement. Tous les envois dématérialisés entre l'INSEE et l'AGIRA font l'objet d'un chiffrement dont la clé est fournie sous pli séparé, en recommandé, avec accusé de réception. Les transmissions de la clé et des données se font successivement, en deux plis distincts, les données n'étant envoyées qu'après retour à l'INSEE de l'accusé de réception du courrier contenant la clé.

6. Transferts de données vers l'étranger

Certains transferts de données à caractère personnel peuvent être réalisés vers des pays tiers à l'Union européenne, qui ne sont pas membres de l'Espace économique européen dans le respect des dispositions du RGPD.

En outre :

- le niveau de protection des personnes physiques ou des données à caractère personnel garanti par le règlement ne doit pas être compromis,
- Aréas Assurances informe le cas échéant les personnes concernées de l'existence d'un transfert de données vers des pays tiers, et ce conformément aux dispositions des articles 13 et 14 du règlement 2016/679 du 27 avril 2016,
- Aréas Assurances s'engage, sur simple demande de la personne concernée, à apporter une information complète sur la finalité du transfert, les données transférées, les destinataires exacts des informations et les moyens mis en œuvre pour encadrer ce transfert.