POLITIQUE GENERALE
DE PROTECTION DES DONNEES A CARACTERE PERSONNEL

ARTEX
ASSURANCES

Date d'application	29/06/20
Auteur	DPO Consulting
Valideur	L. MAZOUZ

Diffusion		
☑ Confidentiel	☑Interne	☐Public

Suivi des mises à jour				
Date	Référence	Auteur	Objet	État
XX/XX/XXXX	V.X	XXX	XXX	Validé/Diffusé

1. PRESENTATION DE LA POLITIQUE

1.1 OBJECTIFS

ARTEX ASSURANCES s'engage à garantir la protection des données obtenues dans le cadre de son activité, ainsi qu'à se conformer aux lois et réglementations applicables en matière de Traitement de Données à Caractère Personnel et Données à Caractère Personnel Sensibles.

Cette politique a pour objectif d'assurer la mise en place par ARTEX ASSURANCES des principes imposés par le Règlement Européen n°2016/679 relatif à la protection des Données à Caractère Personnel, en date du 27 avril 2016, applicable depuis le 25 mai 2018 (ci-après RGPD).

Dans ce cadre, la Politique établit les standards minimums pour l'adoption par ARTEX ASSURANCES des exigences et standards minimums pour l'ensemble des traitements de données à caractère personnel.

1.2 CHAMP D'APPLICATION

La Politique a vocation à s'appliquer à tous les collaborateurs de tous les services d'ARTEX ASSURANCES.

Elle s'applique à toutes les Données à caractère personnel recueillies, traitées, partagées par ARTEX ASSURANCES en ligne et hors ligne, y compris :

- Le site Internet
- Les outils métiers utilisés par ARTEX ASSURANCES (tel que l'Extranet)
- Les emails
- Les conversations ou correspondances
- Les documents papiers

Une communication adéquate sur la Politique doit être réalisée par ARTEX ASSURANCES conformément à l'article « Sensibilisation et Formation » ci-dessous.

Sous réserve de dispositions législatives ou réglementaires contraires, la présente Politique doit être appliquée aux personnes ayant accès aux Données à caractère personnel d'ARTEX ASSURANCES ou à qui elles sont transmises.

Conformément au droit du travail applicable, la présente politique est rendue obligatoire et exécutoire auprès de tous les collaborateurs d'ARTEX ASSURANCES par le respect d'une clause du contrat de travail, ou par tout autre moyen approprié pour rendre la politique contraignante.

Conformément au droit du travail applicable, ARTEX ASSURANCES peut prendre des mesures disciplinaires à l'égard de ses propres collaborateurs, notamment en cas de non-respect des standards minimum de protection des Données à caractère personnel établis par la présente politique.

1.3 REVISION

Cette politique peut être mise à jour par le DPO d'ARTEX ASSURANCES afin de prendre en compte les évolutions de la législation et les pratiques en matière de protection des Données à caractère personnel. Ces modifications sont soumises à validation de la direction d'ARTEX ASSURANCES.

Une communication adéquate sera effectuée aux collaborateurs d'ARTEX ASSURANCES en cas de modifications.

2. DEFINITIONS

Analyse d'impact relative à la vie privée (AIVP) : analyse à effectuer par le Responsable de traitement pour les traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

Consentement : 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.

Délégué à la protection des données (DPO) : personne en charge de la protection des Données à caractère personnel traitées par un organisme.

Destinataire : 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.

Données à caractère personnel : toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «Personne Concernée») ; donc qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, un numéro de carte d'identité, un salaire, des données de santé, des informations de compte bancaire, des habitudes de conduite ou de consommation, des données de localisation, un identifiant en ligne, etc.

Données à caractère personnel sensibles : désigne les Données à caractère personnel telles que l'origine raciale ou ethnique, les opinions politiques, religieuses ou philosophiques, l'appartenance à une organisation syndicale, la santé physique ou mentale ou la vie sexuelle, les données génétiques et biométriques ainsi que les données relatives aux poursuites engagées pour une infraction commise ou présumée commise par la Personne concernée.

Finalités de traitement : l'objectif poursuivi par le Traitement de données à caractère personnel ou l'objectif principal d'une application informatique de Données à caractère personnel.

Législation applicable : ensemble de réglementation relative à la protection des Données à caractère personnel, à savoir le Règlement européen n°2016/679 relatif à la protection des Données à Caractère Personnel, la Loi informatique et libertés modifiée, et toute autre réglementation qui y serait relative.

Personne concernée : individu sur lequel porte les « Données à caractère personnel » et qui peut être identifié ou distingué des autres, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à ses caractéristiques physiques, mentales, économiques, comportementales, ou sociales. Cela inclut les clients, prospects, et collaborateurs anciens et actuels.

Responsable de traitement : personne physique ou morale qui décide quelles Données à caractère personnel sont collectées, pourquoi et comment elles sont collectées et traitées.
Au sens du Règlement Européen sur la protection des Données à caractère personnel, le Responsable de traitement sera entendu au sens général comme le Gérant de la société, et par délégation de pouvoir, les Associés ou les Responsables métier.

Sous-traitant : toute personne physique ou morale, non employée du Responsable de traitement, qui traite des Données à caractère personnel au nom du Responsable de traitement et selon ses instructions (par exemple des prestataires ou fournisseurs). Les Responsables de traitement doivent assurer le maintien de la même obligation de diligence lorsqu'un Sous-traitant traite des Données à Caractère personnel en leur nom.

Tiers : toute personne physique ou morale, autorité publique, agence ou tout autre organisme autre que la Personne concernée, le Responsable du traitement, le Sous-traitant et les personnes qui, sous l'autorité directe du Responsable du traitement ou du Sous-traitant, sont habilitées ou autorisées à traiter les données.

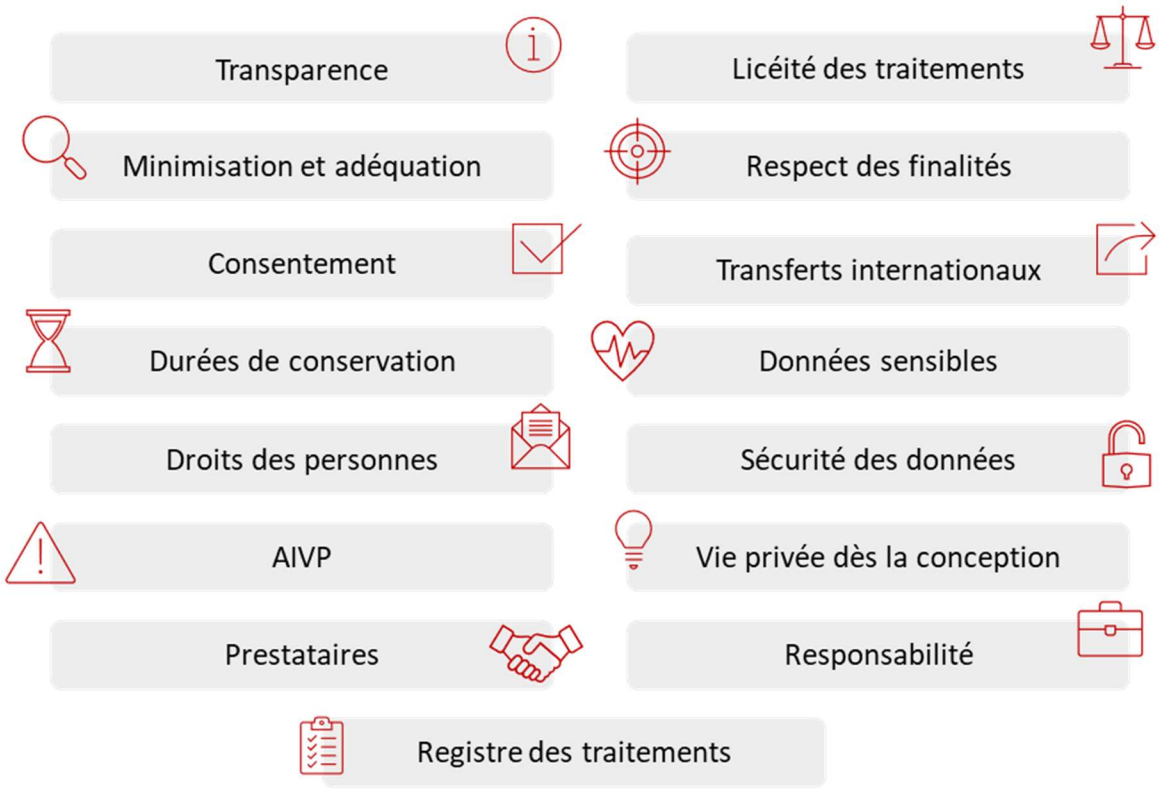
Traitement : toute opération effectuée sur des Données à caractère personnel telle que la collecte, l'accès, l'enregistrement, la copie, le transfert, la conservation, le stockage, le croisement, la modification, la structuration, la mise à disposition, la communication, l'enregistrement, la destruction, que ce soit de manière automatique, semi-automatique ou autre. Cette liste n'étant pas exhaustive.

Transfert de données : toute communication, toute copie ou déplacement de données par l'intermédiaire d'un réseau, ou toute communication, toute copie ou déplacement de ces données d'un support à un autre, quel que soit ce support, dans la mesure où ces données ont vocation à faire l'objet d'un Traitement dans le pays destinataire.

Violation de données à caractère personnel : 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.

3. LES PRINCIPES DE PROTECTION DES DONNEES

La collecte et le traitement de Données à caractère personnel doivent respecter les principes minimums suivants et détaillés ci-après :



3.1 TRANSPARENCE ET LICEITE

Les Données à caractère personnel doivent être collectées et traitées de manière licite, loyale et transparente.

Le principe de transparence du Traitement exige que toute information relative au Traitement de ses Données à caractère personnel soit communiquée à la Personne concernée au moment de la collecte des données.

Le principe de licéité impose à ARTEX ASSURANCES de vérifier qu'il existe un fondement juridique à toute opération qui implique le traitement de Données à caractère personnel, parmi l'une des six bases légales du RGPD et notamment :

- Le traitement est nécessaire à l'exécution d'un contrat (ou de mesures précontractuelles) auquel la personne concernée est partie
    - *Exemple : les données collectées aux fins d'établir un devis assurance*

- Le traitement est nécessaire au respect d'une obligation légale à laquelle ARTEX ASSURANCES est soumise
    - *Exemple : la collecte du numéro de sécurité sociale des salariés*

- Le traitement est nécessaire aux fins des intérêts légitimes du responsable de traitement
    - *Exemple : la réception des demandes prospects/clients sur la messagerie gestion@artex-business.com ou via le formulaire de contact sur le site Internet*

- La personne concernée a consenti au traitement pour la finalité en question
    - *Exemple : la prospection commerciale B2C requière le consentement de la personne concernée.*

R01 Le Responsable de traitement doit collecter et traiter les Données à caractère personnel des Personnes concernées de manière licite, loyale et transparente.

3.2 CONSENTEMENT

Lorsque le Traitement de Données à caractère personnel repose sur le Consentement de la Personne concernée, le Responsable de traitement doit être en capacité de démontrer qu'il a recueilli le Consentement.

La Personne concernée doit être mise en mesure de retirer son consentement à tout moment. Le Responsable de traitement doit mettre en place et informer la Personne concernée des moyens à sa disposition permettant de retirer son consentement, notamment à travers les mentions d'information fournies au moment de la collecte des Données.

En interne, le Responsable de traitement doit mettre en place une procédure lui permettant d'implémenter les consentements et les retraits de consentements dans les applications utilisées et dans le système d'information.

R02 La Personne concernée doit être capacité de retirer son consentement. Dès lors, le Responsable de traitement doit cesser immédiatement le Traitement dont la Personne concernée fait l'objet.

3.3 FINALITE DETERMINEE, MINIMISATION ET ADEQUATION DE LA COLLECTE

Le Responsable de traitement doit déterminer la finalité du traitement, c'est à dire qu'il doit définir les objectifs du Traitement qu'il va mettre en œuvre. Les Données collectées pour une Finalité précise ne doivent pas être utilisées pour une Finalité ultérieure différente de la première

R03 Les Données à Caractère Personnel ne doivent être collectées que pour un/des objectif(s) déterminé(s), explicite(s) et légitime(s). Cela doit se faire en amont de la collecte des Données et du Traitement.

Les Données à caractère personnel collectées pour une Finalité doivent être pertinentes et non excessives par rapport au but poursuivi par le Traitement. Autrement dit, seules les Données à caractère personnel strictement nécessaires à la/les finalités doivent être collectées.

Les Données à caractère personnel ne doivent pas être collectées dans l'hypothèse où elles pourraient ultérieurement être utiles, ou en vue d'une autre finalité qui n'est pas encore déterminée.

Les Données à caractère personnel collectées doivent être exactes, complètes, et mises à jour si nécessaire.

R04 Les Données à caractère personnel collectées par le Responsable de traitement doivent être pertinentes et non excessives vis-à-vis du but poursuivi par le Traitement. Elles doivent également être exactes, complètes et mises à jour si nécessaire.

3.4 CONSERVATION LIMITEE

Les Données à caractère personnel ne doivent pas être conservées plus longtemps que nécessaire au regard des finalités pour lesquelles elles sont collectées, sauf si une loi contraire s'applique.

La durée maximale de conservation des Données est déterminée en fonction de la Finalité de chaque Traitement. Les éléments suivants sont pris en compte pour déterminer la durée de conservation des données :

- Les obligations légales ;
- Les recommandations de la CNIL ;
- Les meilleures pratiques dans chaque domaine concerné ;
- Les besoins opérationnels.

A l'exception des cas dans lesquels il existe une obligation d'archivage, les Données qui ne présentent plus d'intérêt doivent être supprimées sans délai dès lors qu'elles ne présentent plus d'intérêt pour l'objectif poursuivi.

Pour en savoir plus, veuillez consulter le Référentiel des durées de conservation.

R05 Les Données à caractère personnel doivent être effacées dès qu'elles ne sont plus nécessaires à la finalité pour laquelle elles ont été collectées.

3.5 SECURITE ET CONFIDENTIALITE DES DONNEES

ARTEX ASSURANCES doit prendre des mesures raisonnables pour mettre en place des systèmes organisationnels efficaces et des mesures physiques et techniques lors de la collecte, de l'utilisation, la transmission et le transfert, le stockage ainsi que la destruction des Données à caractère personnel.

Ces mesures ont pour objectif de :

- empêcher des personnes non autorisées d'avoir accès aux systèmes de Traitement des données d'information pour traiter ou utiliser des Données à caractère personnel ;
- s'assurer de l'accès à ces Données par les seules personnes habilitées, et dans la limite de la finalité pour laquelle les données ont été collectées ;
- s'assurer que les personnes habilitées n'ont accès qu'aux données auxquelles elles sont autorisées à accéder ;
- s'assurer qu'il est possible de contrôler et de vérifier si les Données à caractère personnel ont été ajoutées, modifiées ou supprimées des systèmes de Traitement de données et si tel est le cas, par qui ;
- s'assurer que les Données à caractère personnel sont protégées contre la destruction accidentelle ou la perte ;
- s'assurer que les Données à caractère personnel collectées pour des finalités différentes peuvent être traitées séparément ;
- s'assurer que l'anonymisation des Données à caractère personnel est effective lorsqu'elle est requise par une loi locale pour mettre en œuvre le Traitement.

R06 Le Responsable de traitement doit mettre en œuvre des mesures techniques et opérationnelles appropriées afin d'assurer la sécurité des Données à caractère personnel, et prévenir tout accès ou divulgation non autorisée.

3.6 TRANSFERTS INTERNATIONAUX DES DONNEES

Pour tout Transfert de Données en dehors de l'Union européenne, il est nécessaire de vérifier si le pays figure dans la liste des pays offrant un niveau adéquat de protection des données à travers le lien suivant : https://www.cnil.fr/fr/la-protection-des-donnees-dans-le-monde

Si le pays est inclus dans la liste des pays adéquats, le Transfert est autorisé et aucune formalité préalable n'est à accomplir.

Si le pays n'est pas inclus dans la liste des pays adéquats, la Procédure est la suivante :

- Vérifier si le partenaire/prestataire a adhéré au Privacy Shield (valable uniquement pour les USA) ;
- Faire signer des clauses contractuelles types de la Commission européenne au partenaire/prestataire.

3.7 TRAITEMENT DE DONNEES A CARACTERE PERSONNEL SENSIBLES

ARTEX ASSURANCES peut être amenée à collecter des Données à caractère personnel sensibles dans le cadre des Traitements mis en œuvre.

Ces Données ne peuvent être collectées et traitées que dans les cas suivants :

- Le consentement explicite de la personne concernée a été obtenu pour la finalité ;
- Le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail, de la sécurité sociale et de la protection sociale ou par une convention collective conclue prévue par une réglementation spécifique locale ;
- Le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique, dans le cas où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement ;
- Le traitement porte sur des données à caractère personnel qui sont manifestement rendues publiques par la personne concernée ;
- Le traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ou chaque fois que des juridictions agissent dans le cadre de leur fonction juridictionnelle ;
- Le traitement est nécessaire pour des motifs d'intérêt public important, sur la base d'une législation nationale locale qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la personne concernée ;
- Le traitement est nécessaire aux fins de la médecine préventive ou de la médecine du travail, de l'appréciation de la capacité de travail du travailleur, de diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et des services de soins de santé ou de protection sociale ou en vertu d'un contrat conclu avec un professionnel de la santé ;
- Le traitement est nécessaire pour des motifs d'intérêt public dans le domaine de la santé publique ;
- Le traitement est nécessaire à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques.

Le Responsable de Traitement doit conserver la preuve du fondement légal l'autorisant à traiter les données à caractère personnel sensibles.

L'accès à ces Données à caractère personnel sensibles doit être limité et elles ne peuvent être utilisées que pour les finalités pour lesquelles elles ont été collectées. Les mesures de sécurité adéquates doivent être mises en place pour empêcher la perte, la dégradation ou le vol de ces données.

4. RELATIONS AVEC LES PERSONNES CONCERNEES

4.1 INFORMATION DES PERSONNES CONCERNEES

En amont de la collecte de Données à caractère personnel, le Responsable de traitement doit informer la Personne concernée du Traitement de ces données. Le RGPD impose de fournir l'ensemble des informations suivantes à la Personne concernée :

- L'identité et les coordonnées du Responsable de traitement
  - *ARTEX ASSURANCES, 32 rue de la petite bilange - 49400 SAUMUR - R.C.S. Angers 812923746*
- Toutes les finalités de traitements (i.e. objectif poursuivi par l'opération de traitement)
  - *Exemples de finalités : gestion des contrats, suivi de la relation client, téléprospection, etc.*
- Les coordonnées du DPO
  - *Une adresse mail générique a été créée : dpo@artex-assurances.com*
- La base juridique du traitement et le cas échéant, les intérêts légitimes poursuivis
  - *Rappel : un traitement de données repose toujours sur l'une des six bases légales prévues par le RGPD (exemple : exécution d'un contrat)*
- La durée de conservation ou les critères de détermination de cette durée
  - *Les données des clients sont conservées pendant toute la durée de la relation contractuelle, archivées puis supprimées à l'issue du délai de prescription applicable*
- Le cas échéant, les destinataires ou catégories de destinataires
  - *Les destinataires sont les personnes physiques ou morales, à qui les données sont communiquées. Il s'agit autant des destinataires externes (ex : compagnies d'assurances) et internes (service habilité à accéder aux données)*
- Les droits des personnes concernées
  - *La mention de ces droits doit être faite à chaque collecte de Données à caractère personnel*
- Le cas échéant, l'existence d'un transfert de données hors Union Européenne ainsi que les informations et garanties qui s'y rattachent
  - *Le transfert de données hors de l'UE vers ARTEX BUSINESS*
- Le cas échéant, l'existence d'une obligation pour la personne concernée de fournir ses données ainsi que la conséquence de la non-fourniture des données.
  - *Le formulaire de collecte des données contiendra des astérisques (*) pour indiquer les données obligatoires*
- Le cas échéant, le droit de retirer son consentement pour les traitements basés sur le consentement
  - *Les personnes peuvent s'opposer à la téléprospection et en sont informées lors de l'appel*
- Le cas échéant, l'existence d'une prise de décision automatisée
  - *Il faut donner des informations simples permettant à la personne concernée de comprendre les raisons et les conséquences pour la personne de la décision, sans donner d'explication complexe sur les algorithmes utilisés (ex : prise de décision par scoring).*
- Le cas échéant, l'existence d'un traitement ultérieur pour une autre finalité et les informations qui s'y rattachent
  - *Par exemple : les données sont collectées au moment de l'inscription et seront utilisées, en cas d'acceptation du dossier, pour la gestion administrative de la vie étudiante*

Dans le cadre d'une collecte indirecte des Données à Caractère Personnel par exemple à partir d'une base de données fournie par un partenaire et/ou tout autre tiers, le Responsable de Traitement doit fournir, en plus, l'information aux Personnes concernées sur la source de la collecte. *Exemple : les prospects sont informés que leurs données ont été collectées auprès d'un fournisseur de data (ex : CARTEGIE).*

Ces informations doivent être fournies au moment de la collecte de données.

R07 Les Personnes concernées doivent recevoir l'information au plus tard au moment de la collecte de façon concise, transparente, compréhensible et aisément accessible.

De façon générale, un renvoi vers la politique de confidentialité doit être fait à chaque collecte de données, mais les supports de collecte (formulaires et applications en ligne, documents papiers, etc.) doivent impérativement mentionner les informations suivantes :

- L'identité du Responsable de Traitement ;
- La/Les finalités du traitement ;
- Les droits des personnes concernées.

Lorsque les données sont collectées de façon indirecte, il faudra informer les personnes concernées au plus tard au moment de la première communication.

De manière générale, les informations sont communiquées aux Personnes Concernées de manière suivante :

- Pour les prospects et clients, la Charte de protection des données (accessible sur le site Internet)
- Pour les employés, via la Charte de protection des données employés

4.2 DROITS DES PERSONNES CONCERNEES

Les Personnes concernées ont les droits suivants concernant le traitement de leurs Données à caractère personnel :

- Le **droit d'être informé** sur les traitements de Données à caractère personnel mis en œuvre ;
- Le **droit de demander l'accès** aux données les concernant, y compris sous forme de liste fournie par écrit ou par voie électronique ;
- Le **droit de demander la rectification des données**, lorsqu'elles sont inexactes ;
- Le **droit de demander la suppression** des données si cela est légalement possible ;
- Le **droit d'obtenir la limitation** du Traitement de leurs Données à caractère personnel lorsque cela est légalement possible ;
- Le **droit de s'opposer au Traitement** de leurs Données à caractère personnel ;
- Le **droit de demander la portabilité** de leurs Données à caractère personnel ;
- Le droit de donner des directives sur le sort de leurs Données à caractère personnel après leur mort.

Les réponses aux demandes des Personnes concernées doivent être effectuées dans un délai maximum d'un mois. Ce délai peut être prolongé de deux mois si la demande est complexe. Dans ce cas, la Personne doit être notifiée de la prolongation du délai de réponse. Les éléments communiqués doivent être aisément compréhensibles

R08 Le Responsable de traitement met en place une organisation interne spécifique afin de traiter les demandes des Personnes Concernées. Les modalités de cette organisation sont détaillées dans une Procédure de gestion des demandes d'exercice de droits.

5. GESTION DES VIOLATIONS DE DONNEES

Il existe trois catégories de Violations de Données à caractère personnel :

- Une violation de confidentialité a lieu lorsque les Données à caractère personnel sont compromises à travers un accès non autorisé, résultant en une fuite de données des personnes concernées ;

- Une violation d'intégrité a lieu lorsqu'une altération non voulue intervient sur les Données, causant ainsi des erreurs et défaillances dans le traitement ;
- Une violation de disponibilité a lieu lorsque des Données à caractère personnel sont perdues ou deviennent inaccessibles, rendant ainsi impossible la fourniture de services à la personne concernée.

Toute faille de sécurité affectant les Données à caractère personnel doit être notifiée à la CNIL dans un délai maximal de 72h lorsqu'elle représente un risque pour les droits et libertés des Personnes concernées. La notification s'effectue en ligne via le téléservice sécurisé de la CNIL : https://notifications.cnil.fr/notifications/index

R09 Une notification aux Personnes concernées est obligatoire lorsque la violation représente un risque élevé pour les droits et libertés des Personnes concernées et doit être effectuée dans un les meilleurs délais. Pour en savoir plus, consultez la Politique de gestion des violations de données.

6. DOCUMENTATION ET GESTION DES RISQUES (« *ACCOUNTABILITY* »)

Le Responsable de traitement doit conserver toutes les preuves du respect des lois ou réglementations additionnelles devant être respectées au regard des traitements inscrits dans le registre des traitements.

6.1 LE REGISTRE DES TRAITEMENTS

Le Responsable de traitement tient à jour un registre des traitements qui contient les informations suivantes :

- Le nom et les coordonnées du Responsable de traitement, et le cas échéant celles du responsable conjoint du traitement, du représentant du Responsable de traitement, et du DPO ;
- Les finalités du traitement ;
- Une description des catégories des personnes concernées et des catégories de Données à caractère personnel ;
- Les catégories de destinataires auxquels les Données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou à une organisation internationale ;
- Le cas échéant, les transferts de Données à caractère personnel vers un pays tiers ou de cette organisation internationale ainsi que les documents attestant de l'existence de garanties appropriées ;
- Les délais prévus pour l'effacement des différentes catégories de données ;
- Une description générale des mesures de sécurités techniques et organisationnelles mises en œuvre.

Le registre des activités de traitements est susceptible d'évoluer, au regard des mises à jour à réaliser lorsqu'un traitement évolue. Le Responsable de traitement a donc une obligation de mise à jour du registre des traitements.

Le registre des activités de traitements doit être mis à jour dès qu'une modification est réalisée sur le traitement en question, telle qu'un changement d'adresse, de finalité, de mesures de sécurité (techniques et/ou organisationnelles), voire la suppression du traitement.

R10 Le Responsable de traitement tient un registre des activités de traitement qui recense tous les Traitements de Données à caractère personnel qu'il effectue. Ce registre doit évoluer selon les évolutions des Traitements ou de leur suppression.

6.2 PROTECTION DES DONNEES DES LA CONCEPTION ET PAR DEFAUT

Pour tout nouveau projet impliquant le traitement de Données à caractère personnel, ARTEX ASSURANCES prend en compte le Privacy By Design et le Privacy By Default.

A cet effet, ARTEX ASSURANCES met en place des mesures visant à protéger les Données à caractère personnel dès la conception du projet, mais aussi tout au long du projet et du cycle de vie de la donnée (de la collecte à la destruction).

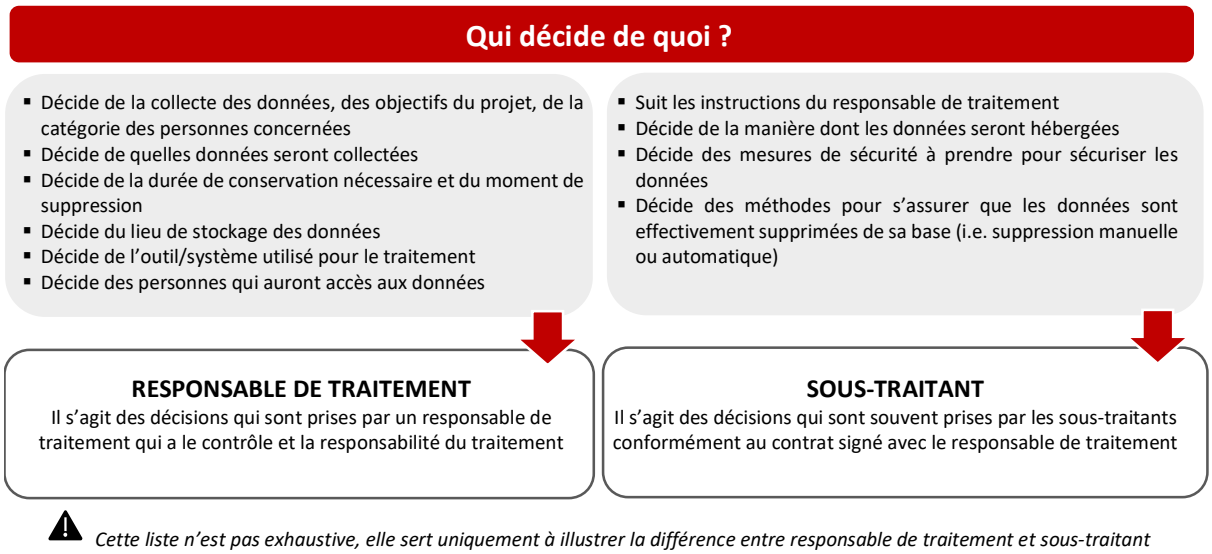
R11 La conception de tout nouveau projet impliquant un Traitement de données doit faire l'objet d'une analyse conformément à la Fiche pratique Privacy by Design.

6.3 L'ANALYSE D'IMPACT SUR LA VIE PRIVEE

Lorsqu'un traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, le Responsable de traitement doit effectuer une analyse de d'impact préalablement à sa mise en œuvre.

R12 L'analyse d'impact doit être menée par le collaborateur en charge du traitement, avec l'aide du DPO et du département IT conformément à la Fiche pratique analyse d'impact sur la protection des données.

7. GESTION DES PRESTATAIRES



⚠ *Cette liste n'est pas exhaustive, elle sert uniquement à illustrer la différence entre responsable de traitement et sous-traitant*

Le Responsable de traitement est tenu de sélectionner des Sous-traitants qui offrent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées afin que les Traitements répondent aux exigences du RGPD. ARTEX ASSURANCES doit ainsi s'assurer que le Prestataire qui traite des Données pour son compte :

- S'engage à mettre en œuvre et à maintenir les mesures techniques et organisationnelles de nature à garantir un niveau de sécurité, d'intégrité et de confidentialité adapté au risque du ou des traitements qui lui sont confiés
- S'interdit d'utiliser ou traiter les données à une fin autre que celle prévue par ledit contrat et qu'il n'acquiert aucun droit ou propriété sur les données et ne doit les communiquer à d'autres personnes même pour leur conservation
- Demande l'autorisation du Responsable de Traitement pour Sous-Traiter la prestation dont il a la charge
- Se conforme à une obligation générale d'assistance concernant les diligences de mises en conformité au RGPD à engager (réponse aux demandes des Personnes concernées, notification des violations de données, réalisation d'une AIVP…)

- Facilite la réalisation d'opérations d'audit par le Responsable de traitement.
- Supprime les Données à caractère personnel à l'issue de la relation contractuelle

8. ROLES ET RESPONSABILITES

Responsible (R) Accountable (A) Consulted (C) Informed (I)	**DPO**	**DSI**	**Direction**	**Service opérationnel**
S'assurer que les règles de protection des Données sont prises en compte pendant les phases de création et d'exécution des activités de traitements	AR	C	I	C
Fournir des conseils sur les impacts juridiques possible pour les nouveaux traitements	A-R	I	C	C
Effectuer une évaluation des risques (cybersécurité et impact sur la vie privée) et spécifier les mesures de sécurité appropriées	C	R-A	I	I
Valider l'AIVP et accepter les risques résiduels	C	C	A-R	C
Evaluer les tiers sur leur capacité à répondre aux exigences de sécurité	I	R-A	I	I
Contracter avec des parties externes	C	C	A-R	C
Implémenter des mesures techniques et organisationnelles de sécurité appropriées pour protéger les Données à caractère personnel contre la destruction/perte accidentelle ou illicite, divulgation non autorisée ou l'accès (violation de Données à caractère personnel)	C	A-R	I	I
Surveiller l'efficacité des mesures de sécurité	I	A-R	I	I
Créer et conserver la documentation en tant que preuve de conformité	A-R	C	C	C
Traiter les demandes des personnes concernées	A-R	R	C	C
Coopérer avec l'autorité de contrôle à sa demande	A-R	C	C	C
Gérer la collecte de données	C	C	A-R	R
Démontrer la conformité avec les règles de protection des données	A-R	C	C	C
Traiter les incidents de protection des données et les notifications de violation de données	C	R	A-R	C
Traiter les questions de protection des données au quotidien	A-R	C	C	C

9. SENSIBILISATION ET FORMATION DU PERSONNEL

ARTEX ASSURANCES a l'obligation de s'assurer que l'intégralité de ses collaborateurs est bien informée et/ou formée conformément aux principes de la présente Politique ainsi qu'aux exigences en matière de protection des Données à caractère personnel.

À cette fin, ARTEX ASSURANCES doit assurer une sensibilisation générale à tous ses collaborateurs, et des formations plus spécifiques aux Services qui ont vocation à traiter des Données à caractère personnel au quotidien ou qui sont plus intimement impliqués dans les aspects critiques des Données à caractère personnel.

R13 ARTEX ASSURANCES doit former l'intégralité de ses collaborateurs aux principes de la protection des Données à caractère personnel.