1. Gouvernance

Règlement concernant la protection des données du Groupe Assura

Table des matières

1. But et champ d'application

1.1 But

1.1.1 Le but du présent règlement est de définir la politique générale de protection et de sécurité des données du Groupe Assura.

1.1.2 Il fixe les principes et les règles applicables que doivent suivre les sociétés du Groupe Assura telles que définies par le règlement d'organisation du groupe Assura et leurs collaborateurs lorsqu'ils traitent des données des prospects, des assurés, des postulants, des collaborateurs des sociétés du Groupe Assura, des tiers (tels que fournisseurs et intermédiaires d'assurances) et des sous-traitants.

1.1.3 Les principes et les règles énoncés ci-dessous doivent permettre en particulier la mise en œuvre des exigences légales (notamment celles figurant dans la Loi fédérale sur la protection des données (LPD) en ce qui concerne le traitement des données personnelles, de ses ordonnances d'application (OPDo et OCPD) et les exigences règlementaires des autorités de surveillance.

1.2 Champ d'application

1.2.1 Le présent règlement s'applique à toutes les sociétés du Groupe Assura telles que définies par le règlement d'organisation du Groupe Assura.

1.2.2 Selon la LPD, une distinction est à opérer entre les personnes privées (physiques et morales) telles que Figeas SA, Assura SA ou les intermédiaires d'assurance et les organes fédéraux tel qu'Assura-Basis SA, dans la mesure où certaines règles spécifiques leurs sont applicables.

1.2.3 Toutes les données traitées dans le cadre de l'exercice des fonctions respectives des collaborateurs, de la Direction générale et du Conseil d'administration sont concernées.

1.2.4 Le règlement s'applique aussi aux données traitées à l'étranger du moment qu'elles déploient des effets en Suisse.

1.2.5 L'émission du présent règlement, ainsi que ses modifications ultérieures, sont de la compétence du Conseil d'administration du Groupe Assura.

1.2.6 Lorsque le masculin est utilisé dans le présent règlement pour désigner des personnes, il s'agit d'un masculin générique désignant indifféremment les personnes des deux sexes.

2. Définitions

Dans le présent règlement, on entend par :

2.1 Communication

Le fait de transmettre des données personnelles ou de les rendre accessibles, y compris à l'étranger (Etats ou organismes internationaux).

2.2 Consentement

2.2.1 Toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte concluant, que des données à caractère personnel la concernant fassent l'objet d'un traitement.

2.2.2 Le consentement doit être exprès, c'est-à-dire résulter d'une manifestation explicite et claire de son accord lorsqu'il s'agit d'un traitement de données sensibles ou d'un profilage effectué par un organe fédéral.

2.3 Décision individuelle automatisée

Une décision prise exclusivement sur la base d'un traitement de données personnelles automatisé, sans intervention humaine, et qui a des effets juridiques pour la personne ou l'affecte de manière significative.

2.4 Données

2.4.1 Toutes les informations concernant le Groupe Assura ou ses sociétés, les assurés, les prospects, les collaborateurs du Groupe Assura, les fournisseurs et les partenaires externes (notamment les intermédiaires d'assurance).

2.4.2 Par données concernant le Groupe Assura ou ses sociétés, on entend les informations portant sur leur organisation, leurs procédures et processus, et leurs décisions.

2.5 Données personnelles

Toute information se rapportant à une personne physique identifiée ou identifiable, notamment à un assuré, à un prospect, à un collaborateur du Groupe Assura, à un fournisseur ou à un partenaire externe (notamment les intermédiaires d'assurance).

2.6 Données personnelles sensibles

Toutes les données personnelles portant sur la santé, la sphère intime, l'origine ethnique, raciale, les opinions ou activités religieuses, politiques, philosophiques, syndicales, ainsi que les mesures d'aide sociale, les données sur les poursuites, sanctions pénales ou administratives, et les données génétiques et biométriques.

2.7 Organe fédéral

L'autorité fédérale, le service fédéral ou la personne chargée d'une tâche publique de la Confédération. Assura-Basis SA est un organe fédéral au sens de la LPD.

2.8 Personne concernée

2.8.1 La personne physique ou morale dont les données font l'objet d'un traitement.

2.8.2 Au sens de la LPD, il s'agit uniquement de la personne physique.

2.9 Personne privée

La personne privée, physique ou morale, qui traite de données personnelles dans le cadre d'une relation privée. Assura SA, au même titre que Figeas SA, est une personne privée au sens de la LPD.

2.10 Préposé fédéral à la protection des données et à la transparence (PFPDT)

La personne physique qui est chargée de surveiller la bonne application des dispositions fédérales de protection des données. Il s'agit de l'autorité de surveillance en matière de protection des données.

2.11 Profilage

2.11.1 Toute forme de traitement automatisé de données personnelles consistant à utiliser ces données 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.

2.11.2 Si le profilage conduit à une compilation de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique, celui-ci doit être qualifié de profilage à risque élevé.

2.12 Responsable du traitement

La personne privée (physique ou morale) ou l'organe fédéral qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des données, c'est-à-dire l'objectif et la manière de le réaliser.

2.13 Sous-traitant

Le prestataire qui traite des données personnelles pour le compte et selon les instructions du responsable du traitement.

2.14 Traitement de données

Toute opération relative à des données quels que soient les moyens et procédés utilisés, notamment la collecte, l'enregistrement, la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la destruction de ce type de données.

2.15 Violation de la sécurité des données

Toute violation de la sécurité entraînant de manière accidentelle ou illicite la perte de données, leur modification, leur effacement ou leur destruction, leur divulgation ou un accès non autorisé à ces données.

3. Rôles et responsabilités en matière de protection des données

3.1 Direction générale

3.1.1 La Direction générale du Groupe Assura est responsable de la mise en œuvre d'une organisation interne conforme à la règlementation en matière de protection des données.

3.1.2 Elle est conseillée par le Conseiller à la protection des données.

3.2 Conseiller à la protection des données

Le Conseiller à la protection des données remplit notamment les tâches suivantes :

a) Définit les exigences minimales de protection des données en fonction de leur nature et des finalités poursuivies par le traitement ;

b) Soutient les services opérationnels dans la mise en œuvre des mesures liées à la protection et à la sécurité des données personnelles ;

c) S'assure de la conformité du traitement des données avec les exigences légales et règlementaires en matière de protection des données, y compris dans les contrats et les projets d'entreprise ;

d) Contribue à la gestion et à la remédiation des incidents de sécurité impliquant des données personnelles ;

e) Tient un registre des activités de traitement de données personnelles tel que défini par la loi sur la protection des données pour Assura SA, Assura-Basis SA et Figeas SA. Concernant Assura-Basis SA, il le communique au Préposé fédéral à la protection des données ;

f) Veille à ce que les demandes en lien avec un traitement de données personnelles (ex. droit d'accès, droit à l'oubli, droit à la portabilité, etc.) soient correctement traitées et fassent l'objet d'une réponse dans le délai imparti par la loi ;

g) Participe à la formation des collaborateurs en matière de protection des données ;
h) Est l'interlocuteur principal du Préposé fédéral à la protection des données et des personnes concernées par le traitement ;
i) Rapporte régulièrement à la Direction générale sur l'état de conformité des sociétés du Groupe Assura et présente un suivi des plans de mesures mis en place en cas de non-conformité constatée ;
j) Veille à ce que le présent règlement soit régulièrement actualisé et respecté au sein du Groupe Assura.

3.3 Chief information security officer (CISO)

3.3.1 Le CISO est l'interlocuteur privilégié de la Direction générale et des collaborateurs du Groupe Assura ainsi que vis-à-vis des partenaires pour ce qui concerne notamment la définition des politiques et des standards visant à garantir la sécurité de l'information et des systèmes d'information.

3.3.2 Ses tâches sont définies de manière plus détaillée dans une directive.

3.4 Collaborateurs

Tous les collaborateurs sont responsables de traiter les données conformément aux règles et principes définis dans le présent règlement.

3.5 Propriétaire des données

Au sein du Groupe Assura, chaque donnée y compris les données personnelles doit avoir un propriétaire. Le propriétaire de la donnée est la personne responsable de son traitement. Il lui appartient de lui conférer le bon niveau de classification tel que défini au chapitre 7 ci-dessous et de sa mise à jour si nécessaire.

3.6 Département Clients & Marché

Le département Client & Marché est propriétaire des données traitées dans le cadre de la prospection de nouveaux clients en vue de la souscription de contrats d'assurances ainsi que des données en lien avec les intermédiaires d'assurances.

3.7 Département Prestations

3.7.1 Responsabilité générale

3.7.1.1 Le département des Prestations est propriétaire des données traitées dans le cadre de la souscription de contrats d'assurances, de la relation avec les assurés et en lien avec le remboursement des prestations (échanges avec les fournisseurs de soins, garanties, traitement des factures, décomptes de prestations, etc.).

3.7.1.2 Des dispositions particulières s'appliquent concernant le traitement des données des collaborateurs assurés auprès des sociétés d'assurance du Groupe Assura.

3.7.2 Service clientèle

Le service clientèle est responsable d'assurer la protection des données des assurés qu'il traite, lors de l'affiliation, du suivi de la relation contractuelle et du départ de l'assuré.

3.7.3 Service du médecin-conseil et médecin-conseil

3.7.3.1 Le service du médecin-conseil est responsable de la protection des données médicales des assurés traitées au sein des services médicaux (notamment des questionnaires de santé, des rapports d'expertise et des rapports médicaux).

3.7.3.2 Le médecin-conseil veille au respect des mesures de protection et de sécurité supplémentaires mises en place eu égard à la sensibilité de ces données.

3.7.4 Responsabilité dans le cadre des SwissDRG

Les collaborateurs des cellules DRG font partie d'une entité particulière, soumise à certification en matière de protection des données. Ils sont responsables des minimal clinical dataset (MCD, diagnostics principaux et secondaires ainsi que les traitements) dont le traitement est réglé dans une instruction spécifique.

3.8 Département Finances

Le département des Finances est propriétaire de toutes les données financières des sociétés du Groupe Assura, ainsi que des données financières des assurés traitées notamment dans le cadre de l'encaissement des primes, du remboursement des prestations (comptes clients, paiements, correspondance et renseignements notamment dans le cadre de la procédure de poursuite, actes de défaut de biens) et des données liées à l'attribution de subsides.

3.9 Département Développement et Marketing

Le département Développement & Marketing est propriétaire des données qu'il traite à des fins statistiques ou de reporting, de campagne de marketing ou d'enquête clients pour l'ensemble du Groupe Assura.

3.10 Secteur Ressources humaines

Le Secteur Ressources humaines est propriétaire des données personnelles des collaborateurs, sous réserve des données qui relèvent de leur statut d'assuré auprès des sociétés d'assurance du Groupe Assura (p.ex. traitement des polices et des prestations) qui sont traitées par des collaborateurs dédiés au Département des prestations.

3.11 Département Informatique

Le département Informatique est propriétaire des données de configuration, de code source et des secrets permettant les accès aux infrastructures IT. Il est en outre responsable de la mise en œuvre des mesures techniques et organisationnelles concernant la sécurité des données électroniques traitées par les différents systèmes d'information utilisés par le Groupe Assura, ses collaborateurs et partenaires (accès, internet, emails, etc..).

3.12 Préposé fédéral à la protection des données et à la transparence (PFPDT)

3.12.1 <u>Compétences du PFPDT</u>

3.12.1.1 Le PFPDT doit d'office ou sur dénonciation ouvrir une enquête contre un organe fédéral ou une personne privée dès que des indices font penser que des traitements de données pourraient être contraires à des dispositions légales de protection des données. Le PFPDT pourra y renoncer lorsque la violation est de peu d'importance ou lorsque le responsable du traitement a pris les mesures adéquates pour rétablir une situation conforme au droit.

3.12.1.2 Si une procédure d'enquête est ouverte, le responsable du traitement est tenu de collaborer avec le PFPDT en lui fournissant les informations nécessaires à son enquête.

3.12.1.3 Si le responsable du traitement ne respecte pas son devoir de collaborer et que le PFPDT constate une violation de la protection des données, il peut ordonner diverses mesures administratives à l'encontre du responsable du traitement, tel que la modification, la cessation, la suspension de toute ou partie du traitement ou la destruction ou la suppression de toute ou partie des données. Il peut en outre demander que des mesures soient prises en matière de sécurité ou que les personnes concernées soient informées.

3.12.1.4 Le PFPDT n'a pas la compétence en revanche de prononcer des amendes ou de sanctionner pénalement le responsable du traitement.

3.12.2 Sanctions

3.12.2.1 Pour les personnes privées

Sur plainte, les autorités pénales peuvent infliger une amende d'un montant de CHF 250'000.-- au plus à l'encontre de la personne physique qui se rendrait coupable, par omission ou intentionnellement, de violation du devoir d'informer, de renseigner, de collaborer, du devoir de diligence et de discrétion, ainsi qu'en cas d'insoumission à une injonction du PFPDT.

3.12.2.2 Pour les organes fédéraux

Est passible de la même amende que celle mentionnée à l'art. 3.12.2.1 ci-dessus, la personne physique au sein de l'organe fédéral qui révèle intentionnellement des données personnelles dont il a connaissance dans le cadre de ses activités et en violation de son devoir de discrétion. L'obligation de garder le secret perdure après la fin des rapports de travail.

3.12.2.3 Si l'identification de la personne punissable au sein de l'entreprise nécessite des mesures d'enquête disproportionnées, l'entreprise elle-même est sanctionnée d'une amende de CH 50'000.-- maximum.

4. Obligations du responsable du traitement

4.1 Principes généraux

4.1.1 Licéité / légalité

4.1.1.1 Pour les personnes privées

Tout traitement de données personnelles doit être licite, c'est-à-dire ne pas contrevenir à une disposition impérative de la loi qui vise la protection de la personnalité de la personne physique. A défaut, un motif justificatif (p. ex. le consentement) est nécessaire pour effectuer le traitement.

4.1.1.2 Pour les organes fédéraux

Tout traitement de données personnelles doit se fonder sur une base légale. En l'absence de loi autorisant un tel traitement, un motif justificatif (p. ex. le consentement) est nécessaire.

4.1.2 Proportionnalité

4.1.2.1 Seules les données personnelles aptes et objectivement nécessaires à atteindre les finalités du traitement peuvent être traitées.

4.1.2.2 Le traitement doit être effectué en respectant un rapport raisonnable entre le but visé et les moyens utilisés, tout en préservant le plus possible les droits des personnes concernées. Il convient d'examiner systématiquement s'il existe un moyen moins intrusif pour atteindre le but recherché.

4.1.3 Conservation des données personnelles

Les données personnelles doivent être détruites ou anonymisées dès qu'elles ne sont plus nécessaires au regard des finalités du traitement, à moins qu'une base légale n'exige leur conservation.

4.1.4 Bonne foi et transparence

4.1.4.1 Tout traitement de données personnelles doit se faire de bonne foi, c'est-à-dire conformément au but communiqué aux personnes concernées lors de la récolte ou qui ressort de la loi ou des circonstances. Aucun traitement de données ne doit avoir lieu à l'insu ou contre la volonté de la personne.

4.1.4.2 Tant la collecte que les finalités du traitement doivent être reconnaissables par la personne concernée.

4.1.5 Finalité

4.1.5.1 Tout traitement de données personnelles doit respecter le but communiqué lors de leur collecte.

4.1.5.2 Tout autre nouveau traitement doit rester compatible avec les finalités initialement communiquées à la personne concernée.

4.1.6 Exactitude

Les données personnelles traitées doivent être exactes et aussi actuelles que les circonstances le permettent. Sous réserve d'obligations légales contraires, le responsable du traitement prend des mesures appropriées permettant de rectifier, effacer ou détruire les données inexactes ou incomplètes. A cette fin, tous les collaborateurs signalent les inexactitudes constatées dans le cadre de leurs activités.

4.1.7 Sécurité des données personnelles

Les données personnelles traitées par le Groupe Assura doivent être protégées par des mesures organisationnelles et techniques appropriées en fonction du risque encouru (niveau de classification) contre toute violation de la sécurité des données interne ou externe.

Ces mesures doivent garantir la confidentialité, la disponibilité, l'intégrité et la traçabilité des données traitées.

4.2 Devoir d'information

4.2.1 Lors de la collecte de données personnelles auprès de la personne concernée ou auprès de tiers, le responsable du traitement communique à la personne concernée les informations

nécessaires pour qu'elle puisse faire valoir ses droits mentionnés au Chapitre 6 ci-dessous et pour que la transparence des traitements soit garantie. Il lui communique au moins :

a) L'identité et les coordonnées du responsable de traitement ;
b) La finalité du traitement ;
c) Le cas échéant, les destinataires ou les catégories de destinataires auxquels les données personnelles sont transmises ;
d) Le cas échéant, le nom de l'Etat tiers dans lequel les données personnelles sont communiquées et les garanties y relatives.

4.2.2 Lorsque les données personnelles sont collectées auprès de tiers, la personne concernée est informée dans le mois qui suit la réception de ces données, à moins que la personne ait donné préalablement son consentement à la collecte ou si une base légale justifie cette dernière. En cas de communication à des tiers dans l'échéance de ce délai, la personne concernée doit être informée au plus tard lors de cette communication.

4.2.3 Le responsable du traitement est délié, peut restreindre ou différer la communication d'informations dans certaines situations prévues par la LPD, comme par exemple si la personne dispose déjà des informations, si le traitement est prévu par la loi ou si les intérêts prépondérants d'un tiers l'exigent.

4.2.4 Le devoir d'information est en particulier mis en œuvre par la publication de la notice en matière de traitement des données sur le site internet du Groupe Assura, ainsi que par la publication du registre de traitement par l'organe fédéral.

4.3 Décision individuelle automatisée

4.3.1 Une décision individuelle automatisée est une décision prise à l'égard d'une personne, par le biais d'algorithmes appliqués à ses données personnelles, sans qu'aucun être humain n'intervienne dans le processus.

4.3.2 La personne concernée qui fait l'objet d'une telle décision doit en être informée préalablement et doit pouvoir faire valoir son point de vue. Cas échéant, elle peut demander que la décision individuelle automatisée soit revue par une personne physique.

4.3.3 Cette obligation ne s'applique pas si la décision est prise en relation avec la conclusion ou l'exécution d'un contrat et que la demande de la personne est pleinement satisfaite ou si la personne concernée a expressément consenti à la prise de ce type de décision.

4.4 Communication de données à l'étranger

4.4.1 Principe

Les données personnelles peuvent être communiquées à l'étranger dans un pays dont la législation présente un niveau adéquat selon la liste établie par le Conseil fédéral, par exemple dans un pays de l'Union européenne.

4.4.2 Garanties complémentaires

Si la législation du pays en question ne présente pas un niveau adéquat, le responsable du traitement doit prendre des mesures supplémentaires pour assurer un niveau de protection approprié, par exemple par l'adoption de clauses contractuelles types approuvées par le PFPDT ou si la personne en question a donné expressément son consentement. Dans ces cas, le conseiller à la protection des données doit être préalablement consulté et son accord obtenu avant toute communication de données dans un pays ne présentant pas un niveau adéquat de protection.

4.5 Registre des activités de traitement

4.5.1 Assura-Basis SA, Assura SA, Figeas SA, ainsi que leurs sous-traitants (pour les données traitées pour leur compte) doivent tenir chacun un registre de toutes les activités de traitement. Le registre doit contenir au minimum les indications suivantes :

a) L'identité du responsable de traitement ;
b) La finalité du traitement ;
c) Une description des catégories de personnes concernées et des données traitées ;
d) Les catégories de destinataires ;
e) Le délai de conservation des données ou les critères utilisés pour le déterminer ;
f) Une description générale des mesures de sécurité des données ;
g) En cas de communication des données à l'étranger, le nom de l'Etat concerné et, cas échéant, les garanties prévues.

4.5.2 Le registre du traitement doit faire l'objet à minima d'une mise à jour annuelle, lors de tout nouveau traitement, ou lorsqu'une modification s'avère nécessaire.

4.5.3 Assura-Basis SA, en tant qu'organe fédéral, doit le déclarer au PFPDT qui le publie sur sa plateforme. Assura SA et Figeas SA doivent le tenir à disposition du PFPDT en cas de demande.

4.6 Analyse d'impact

4.6.1 Principe

4.6.1.1 Pour tout nouveau traitement de données personnelles entrainant un risque élevé pour les personnes concernées selon notamment la nature des données traitées, l'étendue, la finalité du traitement ou l'utilisation de nouvelles technologies, une analyse d'impact doit être effectuée par le responsable du traitement. Cette analyse d'impact doit être réalisée au minimum quatre mois avant la mise en œuvre du traitement envisagé pour tenir compte du délai indiqué au chiffre 4.6.1.4 ci-dessous.

4.6.1.2 Pour tout nouveau traitement, le conseiller à la protection des données doit être préalablement consulté pour déterminer si une analyse d'impact est nécessaire.

4.6.1.3 L'analyse d'impact doit être conservée au minimum deux ans après la fin du traitement.

4.6.1.4 Pour les organes fédéraux

Dès qu'un nouveau traitement de données est prévu par un organe fédéral, une analyse d'impact doit impérativement être réalisée si les conditions mentionnées à l'art. 4.6.1.1 ci-dessus sont remplies.

Si l'analyse d'impact révèle que, malgré les mesures prévues, il subsiste un risque élevé pour la personnalité ou les droits fondamentaux de la personne concernée, le PFPDT doit être consulté pour détermination dans un délai de trois mois.

4.6.1.5 Pour les personnes privées

Le responsable du traitement privé est délié de son obligation d'établir une analyse d'impact s'il est tenu d'effectuer le traitement envisagé en vertu d'une obligation légale. Il peut également y renoncer dans certains cas, notamment s'il recourt à un système, un produit ou un service certifié.

Si une analyse d'impact est nécessaire, il peut être renoncé à soumettre cette analyse au PFPDT si le conseiller à la protection des données est consulté.

4.6.2 Contenu minimal

L'analyse d'impact doit contenir au minimum :

a) Une description du traitement envisagé ;

b) Une évaluation des risques pour la personnalité ou les droits fondamentaux de la personne concernée ;
c) Les mesures prévues pour protéger sa personnalité et ses droits fondamentaux.

4.7 Privacy by design/by default

4.7.1 Protection des données dès la conception (privacy by design)

Pour tout nouveau projet de création de produits ou de services impliquant un traitement de données personnelles, le responsable du traitement est tenu de mettre en place, dès la conception du projet, les mesures techniques et organisationnelles adéquates afin que le traitement respecte les principes énumérés à l'art. 4.1 ci-dessus.

4.7.2 Protection des données par défaut (privacy by default)

Lorsque plusieurs options sont offertes pour le traitement des données personnelles dans le cadre d'un service, d'un logiciel ou d'un appareil et que la personne a la possibilité de régler elle-même ces options, le responsable du traitement garantit que le traitement doit se limiter à ce qui est strictement nécessaire au but poursuivi par le traitement de données, à moins que la personne concernée ait donné son consentement pour un traitement plus élargi. A cette fin, le responsable du traitement doit notamment prévoir les préréglages appropriés.

4.8 Formations

Le responsable du traitement doit s'assurer que les collaborateurs du Groupe Assura sont régulièrement formés en matière de protection des données.

5. Sous-traitance

5.1 Principe

5.1.1 Le responsable du traitement peut sous-traiter le traitement de données à un tiers (à une autre société du Groupe Assura ou à un prestataire externe) pour autant que les conditions suivantes soient remplies :
   a) La sous-traitance est prévue dans un contrat écrit ou par la loi ;
   b) Seuls les traitements que le responsable du traitement serait en droit d'effectuer lui-même sont sous-traités ;
   c) Aucune obligation légale ou contractuelle de garder le secret ne l'interdit.

5.1.2 Le responsable du traitement reste dans tous les cas responsable de la protection et de la sécurité des données dont le traitement est confié à un tiers.

5.2 Modalités

5.2.1 <u>Obligations du responsable de traitement</u>

5.2.1.1 Le responsable du traitement choisit le sous-traitant qui présente des garanties suffisantes en matière de protection des droits des personnes concernées (par ex. sur la base d'une certification) ;

5.2.1.2 Afin d'assurer la protection et la sécurité des données traitées dans le cadre de la mission attribuée au sous-traitant, le responsable du traitement lui soumet ses instructions ad hoc ;

5.2.1.3 Le responsable du traitement doit s'assurer par des contrôles réguliers, à minima une fois par an, que le sous-traitant traite les données conformément à ses instructions et au contrat.

5.2.1.4 En cas de sous-traitance d'une fonction essentielle, respectivement importante, des exigences supplémentaires sont prévues dans une directive idoine.

5.2.2 Obligations du sous-traitant

5.2.2.1 Le sous-traitant choisi par le responsable du traitement doit pouvoir garantir en tout temps que le traitement des données qui lui est confié est conforme aux exigences requises en matière de sécurité et de protection des données.

5.2.2.2 Le sous-traitant ne peut traiter les données que sur la base des instructions reçues du responsable du traitement et pour le compte de ce dernier.

5.2.2.3 Le sous-traitant est tenu d'établir un registre de traitement des données personnelles qu'il traite pour le responsable du traitement conformément à l'art. 4.5.1 ci-dessus.

5.2.2.4 Le sous-traitant ne peut lui-même déléguer un traitement de données à un tiers qu'avec l'autorisation préalable du responsable du traitement.

6. Les droits des personnes concernées par un traitement de données opéré par le Groupe Assura

6.1 Droit d'accès

6.1.1 Chaque personne peut par écrit, ou par voie électronique, demander au responsable de traitement à avoir accès à l'ensemble des données traitées par le Groupe Assura la concernant. Les renseignements sont communiqués en principe par écrit, une consultation sur place est toutefois possible selon entente avec le responsable du traitement.

6.1.2 L'exercice de ce droit peut être exercé en tout temps, sans besoin de motivation particulière et gratuitement à moins que la communication des renseignements occasionne des efforts disproportionnés, auquel cas une participation adéquate aux coûts pourra être demandée.

6.1.3 Le responsable du traitement peut refuser, restreindre ou différer la communication des renseignements dans certains cas prévus par loi, notamment si les intérêts prépondérants d'un tiers l'exigent ou si la demande d'accès est manifestement infondée ou procédurière.

6.1.4 Les renseignements doivent être communiqués dans un délai de 30 jours à compter de la réception de la demande. Si ce délai ne peut pas être respecté, le responsable de traitement informe la personne concernée dans ce même délai en lui indiquant dans quel délai les informations seront fournies. En cas de refus, de restriction ou de report, il communique dans les mêmes délais en indiquant les motifs.

6.2 Droit en cas de décision individuelle automatisée

La personne concernée par une décision automatisée selon l'art. 4.3.1 ci-dessus peut exercer son droit à la revue de la décision par une personne physique.

6.3 Droit de portabilité

6.3.1 Toute personne concernée par un traitement de données peut demander à ce que les données personnelles qu'il a lui-même communiquées au responsable de traitement lui soit remise sous un format électronique couramment utilisé.

6.3.2 Ce droit s'applique uniquement si :

a) Les données sont traitées de manière automatisée ;
b) Il ne porte pas atteinte à des tiers ;
c) Les données sont traitées sur la base du consentement.

6.3.3 Après vérification de la légitimité de la demande par le conseiller à la protection des données, les informations lui sont communiquées dans un format structuré couramment utilisé et lisible par un ordinateur, pour autant que cela soit techniquement possible.

6.3.4 L'exercice du droit à la portabilité peut être refusé pour les motifs invoqués à l'art. 6.1.3 ci-dessus.

6.4 Droit d'opposition

6.4.1 Toute personne concernée par un traitement de données peut sur la base d'un intérêt digne de protection rendu vraisemblable s'opposer expressément à ce que des données personnelles déterminées soient traitées par le responsable du traitement.

6.4.2 Ce droit d'opposition peut être rejeté si :

a) Le traitement de données repose sur une base légale ;
b) Des intérêts privés ou publics prépondérants supérieurs aux intérêts de la personne concernée l'exigent.

6.5 Droit à l'oubli

Toute personne concernée par un traitement de données peut demander au responsable de traitement à ce que ses données personnelles soient supprimées ou anonymisées dès que l'utilisation de ses données n'est plus nécessaire au but poursuivi, si elles sont inexactes ou si le traitement repose sur le consentement de la personne et que cette dernière décide de le retirer.
Les mêmes limites que celles prévues à l'art. 6.4.2 ci-dessus s'appliquent à l'exercice de ce droit.

6.6 Droit de rectification

Toute personne concernée par un traitement de données peut demander au responsable du traitement en cas de données erronées ou incomplètes, à ce que ses données soient rectifiées pour être mises à jour, sauf si la modification est interdite par une loi.
Si l'inexactitude d'une donnée personnelle ne peut être établie, la personne concernée peut demander au responsable de traitement d'ajouter à la donnée concernée la mention de son caractère litigieux.

7. Principes de sécurité des données

En matière de sécurité des données, le Groupe Assura a établi une classification selon les quatre dimensions suivantes : la confidentialité, l'intégrité, la disponibilité et la traçabilité. Pour chaque dimension, quatre niveaux de criticité ont été établis. Pour chacun de ces niveaux, des mesures de sécurité spécifiques ont été déterminées.

7.1 Confidentialité

Le propriétaire de chaque donnée doit classifier les données qu'il traite selon un des quatre niveaux de confidentialité établit par le Groupe Assura, à savoir : « Public », « Interne », « Confidentiel » et « Secret ».

7.1.1 Données publiques (niveau 1)

Les données et documents classés « Public » ne contiennent aucune donnée personnelle et sont destinés à être distribués et consultés librement à l'extérieur du Groupe Assura, sans que cela ne porte préjudice au Groupe Assura (p. ex. le rapport de groupe, brochures marketing). Aucun mécanisme de protection n'est nécessaire à ce niveau.

7.1.2 Données internes (niveau 2)

7.1.2.1 Les données et documents classés « Interne » sont destinés à être utilisés uniquement à l'intérieur du Groupe Assura ou de manière limitative et ciblée à l'extérieur, cas échéant avec

l'accord du propriétaire des données ou du document (p. ex. organigramme, règlement, directive). Leur divulgation à l'extérieur du Groupe peut porter un préjudice limité au Groupe Assura ou aux personnes dont les données sont traitées. Des mécanismes organisationnels et techniques sont nécessaires pour en limiter l'accès.

7.1.2.2 Les données et documents internes ne peuvent pas contenir de données personnelles sensibles.

7.1.3 Données confidentielles (niveau 3)

7.1.3.1 Les données et documents classés « Confidentiel » sont destinés à être communiqués de manière contrôlée à l'intérieur du Groupe Assura (p. ex. les données personnelles des assurés ou des collaborateurs, les données financières, les projets d'entreprise). Leur divulgation à l'extérieur du Groupe peut porter un préjudice effectif au Groupe Assura ou aux personnes dont les données sont traitées. Le cercle des personnes ayant accès à ce type de données est connu, limité et respecte les principes découlant du présent règlement.

7.1.3.2 Les données et documents dont la classification n'est pas spécifiée sont à traiter comme confidentiels.

7.1.4 Données secrètes (niveau 4)

Les données et documents classés « Secret » sont destinés à être communiqués de manière très limitée à l'intérieur du Groupe Assura (par ex. les données médicales des assurés ou des collaborateurs, rentabilité des produits, projets de partenariat ou contrat stratégiques). Leur divulgation à l'extérieur du Groupe peut porter un préjudice important à l'entreprise. Ils ne peuvent être diffusés sans l'accord écrit de leur propriétaire. Le cercle des personnes ayant accès à ce type de données est très limité, connu et peut être fourni à tout moment.

7.2 Intégrité

L'intégrité permet d'assurer l'exactitude des données, soit que des données ou des documents n'ont pas été modifiés ou détruits de façon non autorisée. Le propriétaire de chaque donnée doit classifier les données qu'il traite selon un des quatre niveaux suivants d'intégrité établi par le Groupe Assura :

7.2.1 Pas de contrainte d'intégrité (niveau 1)

Les données et documents peuvent être modifiés ou supprimés sans que cela ne porte préjudice au Groupe Assura ou aux personnes dont les données sont traitées. Aucun mécanisme de correction n'est nécessaire à ce niveau.

7.2.2 Intégrité standard (niveau 2)

Les modifications ou suppressions de données et documents à ce niveau porte un préjudice limité au Groupe Assura ou aux personnes dont les données sont traitées (perte de temps dans le traitement, nécessité de reprendre le travail déjà réalisé). Des mécanismes organisationnels et techniques sont nécessaires pour limiter les impacts de ces modifications ou suppressions.

7.2.3 Intégrité renforcée (niveau 3)

Les modifications ou suppressions de données et documents à ce niveau porte un préjudice effectif au Groupe Assura ou aux personnes dont les données sont traitées (efforts significatifs pour corriger

les erreurs, impacts sur l'image, altération de la relation avec les clients et partenaires). Des mécanismes organisationnels et techniques sont nécessaires pour limiter les modifications ou suppressions.

7.2.4 Intégrité inaltérable (niveau 4)

Les modifications ou suppressions de données et documents à ce niveau portent un préjudice très important au Groupe Assura ou aux personnes dont les données sont traitées (efforts considérables pour corriger les erreurs, impacts fort sur l'image, altération durable de la relation avec les clients et partenaires, non-respect d'obligations légales). Des mécanismes organisationnels et techniques sont indispensables pour empêcher les modifications ou suppressions. Toute modification doit faire l'objet d'audit détaillés.

7.3 Disponibilité

Par disponibilité, on entend un accès en tout temps aux données nécessaires à la réalisation des activités par le biais des applicatifs dédiés. La stratégie de continuité des activités décrit notamment les processus-clés et les applicatifs qui les soutiennent. Une instruction ad hoc sur la gestion des risques définit quant à elle cinq niveaux de criticité en matière d'impact, à savoir sévère, majeur, modéré, mineur et insignifiant. Pour chacun de ces niveaux, une durée maximale admissible des défaillances est décrite ainsi que les mesures de remédiation.

7.4 Traçabilité

La traçabilité permet d'identifier tout accès non-autorisé et de déterminer l'origine d'un incident sur la base d'un enregistrement. Celui-ci permet d'établir notamment qui a accédé à la donnée, si un traitement a été réalisé et quand une éventuelle altération de la donnée est intervenue. Le propriétaire de chaque donnée doit classifier les données qu'il traite selon un des quatre niveaux suivants de traçabilité établi par le Groupe Assura :

7.4.1 Aucune traçabilité (niveau 1)

L'absence de trace concernant la donnée ou le traitement ne porte aucun préjudice à l'entreprise ou aux personnes dont les données sont traitées. Aucune mesure n'est nécessaire à ce niveau.

7.4.2 Traçabilité standard (niveau 2)

L'absence de trace à ce niveau porte un préjudice limité à l'activité et/ou à la conformité de l'entreprise. Les processus internes de l'entreprise et des contraintes réglementaires imposent de conserver une trace minimale de l'accès à la donnée ou de l'exécution du traitement (qui a accédé à la donnée, à quelle heure et à quel système d'information).

7.4.3 Traçabilité détaillée (niveau 3)

L'absence de trace à ce niveau porte un préjudice effectif à l'activité et/ou à la conformité de l'entreprise. Les processus internes de l'entreprise et les contraintes réglementaires imposent de conserver une trace détaillée de l'accès à la donnée ou de l'exécution du traitement (qui a accédé à la donnée, à quelle donnée, à quelle heure, à quel système d'information et la nature du traitement).

7.4.4 Traçabilité complète (niveau 4)

L'absence de trace à ce niveau porte un préjudice très important à l'activité et/ou à la conformité de l'entreprise. Les processus internes de l'entreprise et les contraintes réglementaires imposent de conserver une trace complète de l'accès à la donnée ou de l'exécution du traitement (qui a accédé à la donnée, à quelle donnée, à quelle heure, à quel système d'information et la nature du traitement et l'état de la donnée avant et après l'accès)

8. Mesures générales servant à garantir la protection des données

8.1 Mesures concernant les données physiques

Pour garantir la sécurité et la protection des données physiques au sein du Groupe Assura, les collaborateurs doivent respecter les principes suivants :

a) *Accès aux bâtiments :* seuls les collaborateurs disposant d'un badge sont autorisés à accéder aux locaux du Groupe Assura. Toute transmission du badge à un tiers est interdite ;
b) *Clear desk policy* : Les supports physiques contenant des données confidentielles sont à conserver dans des endroits (bureaux ou armoires) fermés à clef ;
c) *Courrier interne* : Les enveloppes contenant des données confidentielles ou secrètes doivent être fermées et contenir la mention « confidentiel » ;
d) *Destruction des documents* : Les documents papiers contenant des données confidentielles ou secrètes, ainsi que les documents internes contenant des données personnelles doivent être détruits par déchiqueteuse ;
e) *Distribution des documents* : La distribution des documents papiers au sein du Groupe Assura et à l'extérieur doit être ciblée, limitée et basées sur le principe de proportionnalité.
f) *Conservation des documents :* Les documents papiers doivent être stockés au sein du Groupe Assura et doivent être conservés et détruits selon la directive interne en la matière.

8.2 Mesures concernant les données au format électronique

La protection des données au format électronique au sein du Groupe Assura repose sur les principes suivants :

a) L'accès aux systèmes d'information du Groupe Assura impose une authentification et une autorisation systématique de chaque utilisateur (nom d'utilisateur et mot de passe nécessaires). Ceux-ci sont renouvelés régulièrement dans le temps, selon l'instruction ad hoc.
b) Les droits d'accès aux systèmes d'information sont attribués, sur la base des rôles métiers définis par les différents métiers. Les exceptions sont justifiées, suivies et régulièrement contrôlées par les managers et le responsable applicatif métier. Les droits d'accès sont revus annuellement.
c) Les données sont chiffrées au repos et lors de leur transit.
d) Une authentification forte peut être exigée pour les accès informatiques les plus sensibles.
e) Les données électroniques doivent être archivées et supprimées conformément à la directive interne en la matière.
f) Les données et informations sont détruites des matériels informatiques avant leur recyclage.
g) Des mesures et solutions techniques sont mises en place pour lutter contre la perte, le vol ou la fuite de données et pour lutter contre les cybermenaces.

9 Dispositions finales

Le présent règlement a été adopté par le Conseil d'administration le 5 juillet 2023 et entre en vigueur le 1er septembre 2023. Il remplace et annule le règlement concernant le traitement des données daté du 1er juillet 2016.