SUPRA

# Règlement concernant le traitement des données personnelles

Entrée en vigueur au 1er septembre 2014

# Table des matières

## Préambule

SUPRA-1846 SA (ci-après Supra) est une société d'assurances active dans l'assurance obligatoire des soins, conformément à la Loi fédérale sur l'assurance-maladie obligatoire (LAMal). Le présent règlement régit la pratique en matière de protection des données dans le domaine des assurances sociales.

## 1. Fondements juridiques, champ d'application et définitions

Ce règlement repose sur la Loi fédérale sur la protection des données (LPD) et son ordonnance, plus précisément sur l'art. 21 OLPD.

Il vaut pour tous les organes et collaborateurs de Supra, pour les sociétés liées à celle-ci, ainsi que pour les auxiliaires, partenaires commerciaux ou tiers qui, sur mandat, ont accès électroniquement ou physiquement à des données personnelles.

En matière de protection des données, on entend par :

a) données personnelles : toutes les informations qui se rapportent à une personne identifiée ou identifiable ;
b) personne concernée : la personne physique ou morale au sujet de laquelle des données sont traitées ;
c) données sensibles : notamment les données personnelles sur la santé, les mesures d'aides sociales, les poursuites ou sanctions pénales et administratives ;
d) traitement : toute opération relative à des données personnelles – quels que soient les moyens et procédés utilisés – notamment la collecte, la conservation, l'exploitation, la modification, la communication, l'archivage ou la destruction de données ;
e) communication : le fait de rendre des données personnelles accessibles, par exemple en autorisant leur consultation, en les transmettant ou en les diffusant.

## 2. Départements concernés par la protection des données

Sont concernés par le respect des dispositions en matière de protection des données notamment les services suivants :

### 2.1. Service clients / Portefeuille (GPO)

Assure la protection des données de base (p. ex. propositions d'assurance, polices, mutations).

### 2.2. Prestations (SIN)

Assure la protection des données en relation avec les données inhérentes aux prestations (p. ex. décomptes de prestations, échanges de données avec les fournisseurs de prestations). La manière de procéder avec les données médicales est réglementée séparément.

### 2.3. Informatique (INF)

Assure la sécurité des données sur le plan du traitement électronique des données, en particulier pour les autorisations d'accès (également pour les polices

des collaborateurs), ainsi qu'au niveau d'Internet, de la transmission d'e-mails et de l'échange de données avec des partenaires externes.

**2.4. Finances et recouvrement (FIN et CTX)**
Assure la protection des données liées à l'encaissement (p. ex. comptes clients, paiements, correspondance et renseignements dans le cadre de la procédure de poursuite).

**2.5. Ressources humaines (RH)**
Assure la protection des données se rapportant au personnel.

**2.6. Archivage (ARC)**
Assure la protection des données en rapport avec la sauvegarde et la destruction physique et électronique des données.

**2.7. Service technique (INT)**
Assure la protection des données par rapport à l'accès aux bâtiments de l'entreprise.

**2.8. Médecin-conseil**
Dans le domaine de l'assurance obligatoire, il dirige le service du médecin-conseil (SMC) qui lui est rattaché, comprenant secrétariat et personnes auxiliaires et assure la protection des données médicales.

**2.9. Marketing**
Assure la protection des données dans le cadre des actions publicitaires.

## 3. Mise en pratique et respect du règlement

**3.1. Collaborateurs**
Tous les collaborateurs doivent veiller, dans leur domaine d'activité, à l'application et au respect de la protection des données et du présent règlement, ainsi qu'à l'observation, en tout temps, du devoir de confidentialité relevant tant de la loi que du contrat de travail.

**3.2. Cadres**
Tous les cadres répondent de l'exigence imposée à leurs collaborateurs de comprendre, de mettre en pratique et de respecter les exigences de la protection des données, ceci dans leur domaine de compétences et de responsabilités. Ils s'assurent, en particulier, que :

a) les autorisations d'accès de leurs collaborateurs soient définies conformément à leurs tâches;
b) leurs collaborateurs connaissent le contenu et la signification de la protection des données;
c) le respect de la protection des données dans leur domaine de compétences soit périodiquement contrôlé.

### 3.3. Conseiller à la protection des données

Le conseiller surveille, de façon autonome, le respect des prescriptions en matière de protection des données à l'intérieur de l'entreprise et remplit notamment les tâches suivantes:

a) il vérifie que l'ensemble des contrats et des projets qui incluent le traitement de données soient conformes à la réglementation légale ;
b) il tient un répertoire des fichiers de données ;
c) il veille à ce que le présent règlement soit régulièrement actualisé et respecté au sein de l'entreprise ;
d) il veille à ce que les demandes de renseignements au sens de l'art. 8 LPD soient suivies, dans le délai imparti, de réponses correctes du point de vue du contenu ;
e) il est l'interlocuteur du Préposé fédéral à la protection des données ;
f) il aide les services opérationnels dans la planification et la mise en pratique des mesures liées à la protection et à la sécurité des données ;
g) il transmet à la direction opérationnelle des informations sur son activité et, là où il y a lieu, lui recommande des mesures correctives et coordonne la mise en œuvre de celles-ci.

## 4. Principes applicables au traitement des données

### 4.1. Bases légales et autorisation préalable

Dans le domaine des assurances sociales, les données personnelles sont traitées en conformité avec les dispositions de la LAMal, en particulier avec l'art. 42 al. 3 et 4, les art. 84 et 84a LAMal. En dehors de ce contexte, le traitement nécessite l'autorisation préalable de la personne concernée.

### 4.2. Finalité du traitement

Supra traite les données personnelles de ses clients uniquement à des fins d'exécution et de bon déroulement de l'assurance obligatoire des soins. Toute autre utilisation des données nécessite l'autorisation de la personne concernée.

Le traitement a lieu aussi bien sous forme physique qu'électronique et il est protégé contre l'accès de tiers non autorisés.

### 4.3. Principe de la proportionnalité

Lors du traitement des données personnelles, le principe de la proportionnalité doit être respecté. Ceci implique en particulier, dans le cadre de la fourniture des prestations, que seules peuvent être traitées les données personnelles nécessaires à la réalisation des tâches.

Le principe de proportionnalité vaut également pour la transmission interne des données.

### 4.4. Autorisations d'accès

Les collaborateurs n'ont accès qu'aux données personnelles indispensables à l'accomplissement de leurs tâches. Les autorisations d'accès sont attribuées sur la base de la fonction exercée et font régulièrement l'objet de vérifications (cf. chiffre 3.2 lit. a).

Le service informatique gère une liste des autorisations d'accès et met en œuvre les accès conformément aux autorisations accordées.

L'accès aux polices des collaborateurs et de leur famille fait l'objet de protections particulières. Seuls les collaborateurs appartenant à un cercle défini de façon restrictive se verront attribuer l'autorisation d'accès, ceci non sans s'être préalablement aussi engagés par écrit à respecter le devoir de discrétion à l'égard des autres collaborateurs. Un tel droit d'accès est à refuser à toute autre personne.

### 4.5. Communication interne de données

En interne, les dossiers doivent être exclusivement transmis sous pli fermé, dans les enveloppes prévues à cet effet. Il convient, dans de tels cas également, d'observer le principe de la proportionnalité.

Supra peut charger des tiers de l'exécution et du déroulement des opérations d'assurance ou de parties d'entre elles. A cet égard, il importe de respecter les conditions de l'art. 10a LPD. Plus précisément, les tiers appelés à collaborer doivent garantir une protection des données, dont la portée correspond pour le moins à celle de Supra.

### 4.6. Communication externe de données

La transmission externe de données n'est fondamentalement admise que dans la mesure où existe une base légale à ce propos (art. 30 et 32 al. 2 LPGA, art. 82 et 84a LAMal). Une communication allant au-delà nécessite l'accord préalable de la personne concernée ou l'injonction d'une autorité.

### 4.7. Consultation du dossier

L'étendue et la forme de cette consultation reposent avant tout sur l'art. 47 LPGA et les art. 8 ss. OPGA (ordonnance sur la partie générale du droit des assurances sociales). Une personne a en principe le droit illimité de consulter les documents la concernant. Elle peut habiliter une tierce personne à les consulter.

Le conseiller à la protection des données examine le bien-fondé des requêtes formulées en vue de la consultation des documents, au sens de l'art. 8 LPD. Au cas où de telles demandes concernent ou englobent des renseignements médicaux, il transmet une copie de la requête au médecin-conseil. Ce dernier s'assure que les documents soumis au secret médical soient directement transmis à la personne ayant émis la requête ou à l'organe explicitement désigné par elle.

## 5. Mesures servant à garantir la protection des données

### 5.1. Informations aux collaborateurs, plus particulièrement lors de l'entrée en service

Les principes de la protection des données sont portés à la connaissance de tout collaborateur dès son entrée en service. Celui-ci s'engage par écrit à respecter strictement le devoir de confidentialité stipulé par la loi ainsi que le devoir de discrétion relevant du droit du travail.

Les auxiliaires du médecin-conseil doivent en outre signer un document spécial, qui régit les droits et les obligations en rapport avec le service du médecin-conseil.

Les principes de la protection des données sont rendus accessibles à chaque collaborateur sur Intranet.

Selon les besoins, la direction opérationnelle met à disposition d'autres instruments nécessaires et appropriés pour la formation et l'information des collaborateurs. Elle informe en particulier des nouveautés et changements en matière de protection des données.

### 5.2. Informatique

En relation avec le système informatique, le département compétent veille à la maîtrise des points suivants:

a) organisation et sécurisation des droits d'accès attribués ;
b) contrôle des accès et des autorisations d'accès des collaborateurs par rapport aux systèmes informatiques ou aux données des assurés ;
c) mise en sécurité des données ("backup" et archivage) ;
d) assurer la protection des données lors de l'utilisation d'Internet comme canal de transactions ;
e) sécurité de l'ensemble du réseau (réseaux de confiance, encodage, protection sous forme de mots de passe, raccordement d'entreprises étrangères, accès à l'Internet) ;
f) si des données personnelles sensibles sont transmises via des réseaux externes de communication, les données personnelles en question doivent être encodées. En particulier, les e-mails et tout ce qui leur est annexé, contenant des données personnelles sensibles, sont à encoder ;
g) assurer une élimination appropriée et qualifiée des supports de données électroniques, quels qu'ils soient.

### 5.3. Service du médecin-conseil (SMC)

#### 5.3.1. Acquisition et traitement des données

S'il manque des données médicales décisives pour la prise de décisions, les fournisseurs de prestations concernés sont invités à les transmettre au médecin-conseil. A cet effet, Supra met à la disposition des prestataires une enveloppe-réponse adressée à l'attention du médecin-conseil.

Supra assure que le courrier adressé au médecin-conseil soit exclusivement ouvert et traité par le médecin-conseil ou ses auxiliaires.

Le médecin-conseil observe le principe de la proportionnalité en matière de communication des données médicales aux collaborateurs de Supra. Il ne transmet que les données indispensables au traitement du cas d'assurance.

#### 5.3.2. Organisation

Le médecin-conseil est responsable de l'accomplissement des activités spécifiques à son service. Pour mener à bien sa tâche, il est légitimé à faire appel à des auxiliaires. A cet égard, le médecin-conseil est responsable du choix, de l'instruction et de la surveillance de ces personnes.

Le médecin-conseil veille à ce que les données dont il dispose sous forme écrite ou électronique soient conservées de telle manière qu'elles ne soient accessibles qu'à lui-même et à ses auxiliaires.

Supra met à la disposition du médecin-conseil tous les moyens nécessaires, afin que le traitement et la conservation des données de son service soient conformes aux exigences de la protection des données. Parmi ceux-ci figurent notamment des mesures touchant les constructions, comme par exemple un système électronique de contrôle des accès aux locaux (badges), qui rend impossible aux personnes non autorisées l'accès aux locaux du SMC, et encore des installations de rangement qui puissent se fermer à clé.

### 5.4. Conservation et destruction des données personnelles

Dès que possible, les données personnelles seront conservées dans des endroits fermés à clé. On veillera à ne déposer sur son bureau que les documents indispensables à l'exécution de ses tâches.

Les données personnelles sur support papier ne doivent pas être déversées dans les ordures ordinaires ou mêlées telles quelles à la collecte du vieux papier. S'agissant de la destruction des documents, chaque bureau est équipé d'un container, dont le contenu est régulièrement vidé et détruit.

### 5.5. Réglementation des accès physiques

Supra fait en sorte qu'aucun tiers ne puisse s'introduire sans autorisation dans les locaux où les données sont conservées et/ou traitées.

A cette fin, les portes d'entrée et de sortie de l'ensemble des bâtiments doivent être sécurisées par un système électronique de contrôle des accès (badge). L'accès au(x) guichet(s) de la réception est autorisé aux clients et visiteurs durant les heures de bureau. Des personnes venant de l'extérieur n'ont en aucun cas le droit de se tenir, en dehors de toute surveillance, dans des locaux où les données sont conservées et/ou traitées.

## 6. Traitement des données dans la pratique

### 6.1. Renseignements donnés par téléphone

#### 6.1.1. Renseignements au sujet de l'interlocuteur lui-même (personne assurée)

A l'exception des informations concernant l'état de santé, il est possible de donner tous les renseignements généraux qui ressortent de la consultation du dossier à l'écran, pour autant que l'interlocuteur s'annonce comme étant l'assuré et qu'il puisse s'identifier par son numéro de police et sa date de naissance. Lorsqu'un renseignement médical est sollicité, il sera répondu à l'assuré que seule une demande écrite est valable et que la désignation d'un médecin en tant qu'intermédiaire pourra être requise, si ladite communication est susceptible d'entraîner une atteinte à la santé à la personne assurée (art. 47 al. 2 LPGA).

#### 6.1.2. Renseignements donnés à son interlocuteur au sujet de son enfant

Les principes décrits au point 6.1.1 s'appliquent lorsqu'un parent téléphone au sujet de son enfant âgé de moins de 18 ans et vivant dans le même ménage.

Lorsqu'un parent téléphone pour obtenir des renseignements au sujet d'un enfant assuré majeur, seuls des renseignements concernant l'adresse enregistrée, la couverture d'assurance, le montant et l'échéance des primes pourront être donnés. S'agissant des autres renseignements, ils ne seront donnés qu'à la condition de disposer d'une autorisation écrite préalable de l'assuré. A défaut, il convient d'indiquer à l'interlocuteur que l'information sera transmise directement à l'assuré soit par écrit, soit par téléphone si ce dernier fait la démarche lui-même.

**6.1.3. Fournisseur de prestations**

Seuls des renseignements sur la couverture d'assurance peuvent être communiqués au fournisseur de prestations, pour autant que cela soit dans l'intérêt de la personne assurée, en particulier dans le cas d'une admission en urgence à l'hôpital.

Par contre, aucune déclaration de prise en charge n'est accordée oralement. Une telle demande doit être déposée par écrit par le fournisseur de prestations et fera l'objet d'une réponse écrite.

**6.1.4. Tiers**

Conformément au devoir de confidentialité, aucun renseignement ne doit être fourni à des tiers. Ceci vaut aussi pour des informations comme l'adresse, les numéros de téléphone, l'existence ou l'inexistence d'un rapport d'assurance.

**6.2. Renseignements écrits**

**6.2.1. Principe**

Il y a lieu de donner des renseignements exhaustifs aux personnes assurées.

Des renseignements seront donnés à des tiers légitimés dans le cadre de l'entraide administrative, en réponse à une requête fondée par écrit, ceci dans le respect des dispositions légales (art. 32 LPGA, art. 84a LAMal) et sans que soit nécessaire l'accord préalable de la personne concernée. En dehors de ce contexte, il n'est pas accordé de renseignement écrit à un tiers ne disposant pas de l'accord préalable de la personne concernée.

**6.2.2. Personne assurée**

L'étendue du renseignement écrit est fonction de ce que veut la personne assurée. Si l'information requise concerne aussi les données en possession du médecin-conseil, ce dernier doit les lui transmettre par courrier séparé. Conformément à l'art. 47 al. 2 LPGA, il pourra être exigé de la personne assurée qu'elle désigne un médecin intermédiaire afin de lui transmettre les données médicales dont la communication directe à l'assuré pourrait lui porter préjudice (informations particulièrement sensibles, par exemple dans le contexte d'une maladie grave ou psychique).

**6.2.3. Entraide administrative et renseignements à des tiers bénéficiant d'une procuration**

L'entraide administrative a lieu dans les limites des dispositions légales (art. 32 LPGA, 84a LAMal). Il convient dans tous les cas d'observer le principe de la proportionnalité. La demande d'entraide administrative doit être motivée.

L'étendue des informations fournies à la personne habilitée résulte de la procuration donnée par la personne concernée. Les données sensibles, notamment les informations touchant à l'état de santé, ne sont transmises que si la procuration fait explicitement mention de cet aspect.

### 6.3. Renseignements par la voie électronique

#### 6.3.1. Trafic en ligne (service.net)

Dans le cadre de la plate-forme SUPRA*net*, la communication de renseignements a lieu selon les conditions stipulées dans le contrat en ligne SUPRA*net*. Les données sont déposées dans la boîte aux lettres électronique, qui est protégée par un numéro et un mot de passe, et à laquelle seules les personnes autorisées ont accès.

#### 6.3.2. E-mails

Pour répondre aux questions des personnes assurées via e-mails, il importe, dans tous les cas où cela est possible, de fournir des informations anonymes (p.ex. pas de nom et prénom sous rubrique "objet" du mail, mais seulement la police d'assurance), ceci afin que l'identité du destinataire ne puisse pas être découverte. Les données sensibles doivent être transmises exclusivement par courrier postal.

## 7. Sanctions

### 7.1. Sanctions pénales

Dans le cas d'une violation de la protection des données, les sanctions pénales (art. 35 LPD, 92 et 93 LAMal,) sont applicables.

Supra dénonce à l'autorité judiciaire compétente les infractions commises qui relèvent du droit pénal.

### 7.2. Sanctions relevant du droit du travail

Les infractions à l'encontre de la protection des données ou du devoir de confidentialité seront sanctionnées, en fonction de la gravité du cas, par un avertissement, une résiliation ordinaire, voire une résiliation avec effet immédiat du contrat de travail. Restent réservées les créances de droit civil ainsi que les actions intentées en vertu du droit pénal.

## 8. Entrée en vigueur

Ce règlement concernant le traitement des données personnelles entre en vigueur le 1er septembre 2014.