A + A Assureurs Associés SA
Etude, placement et gérance de portefeuilles d'assurances
Place St-Gervais 1 I CP 1213 I CH-1211 Genève 1
t +41 22 716 19 19 I f +41 22 731 85 21
info@synerisk.ch I www.synerisk.ch

Directive interne sur la protection des données pour A + A Assureurs Associés SA

A. Préface

A + A Assureurs Associés SA (ci-après également "employeur"), il est important de traiter les données personnelles conformément à la loi.

La direction est responsable du traitement légal des données personnelles, applique elle-même les présentes directives et s'assure que les collaborateurs traitent les données de manière conforme.

Sébastien Beck a été désigné comme responsable interne de la protection des données et agit en tant que personne de contact interne pour les demandes relatives à la protection des données.

Sébastien Beck
Sebastien.beck@synerisk.ch
Tél. +41 22 716 19 19

B. Protection des données

1. Que sont les données personnelles ?

Toutes les informations qui permettent d'identifier une personne physique précise sont des données personnelles (par exemple, le nom, l'adresse, la date de naissance, le numéro IBAN, le numéro de police, le numéro de sécurité sociale, les données relatives à la santé, les sanctions pénales, mais aussi, dans certaines circonstances, l'ID de l'appareil et d'autres données d'identification de l'appareil).

2. Qu'est-ce que le traitement des données personnelles ?

Toute manipulation de données personnelles, notamment la collecte, l'enregistrement, la conservation, l'utilisation, la modification, la communication, l'archivage, l'effacement ou la destruction de données, constitue un traitement de données personnelles.

3. Quand le traitement de données personnelles par des collaborateurs est-il autorisé ?

Les données personnelles ne peuvent être traitées par les collaborateurs que si le traitement est en rapport avec l'exécution de leurs obligations contractuelles. Tout autre traitement de données par les collaborateurs est interdit.

Les autorisations système des collaborateurs sont définies sur la base de leurs fonctions et mises en œuvre par des mesures techniques et organisationnelles. Une limitation ou une extension des autorisations pour certains collaborateurs est possible à tout moment.

4. Comment les données personnelles sont-elles stockées et protégées ?

L'employeur prend des mesures techniques et organisationnelles pour protéger les données. Les données sont ainsi protégées contre la destruction, l'accès non autorisé, les traitements de données contraires à la loi et la perte. Les mesures prises sont contrôlées au moins une fois par an et adaptées si nécessaire.

Dès que le but du traitement est atteint, les données personnelles sont détruites ou rendues anonymes conformément aux directives internes de suppression. La personne responsable de la destruction physique est Sébastien Beck, Administrateur et la personne responsable de la destruction électronique est Sébastien Beck, Administrateur.

Les données qui doivent être conservées plus longtemps en raison d'obligations de conservation légales ou autres sont exclues de la suppression.

Les documents commerciaux doivent être conservés pendant 10 ans conformément à l'art. 958f al. 1 CO. Les documents fiscaux généraux doivent être conservés pendant 10 ans conformément à l'art. 70 al. 2 en relation avec la LTVA. L'art. 42 al. 6 LTVA doit être conservé pendant 10 ans. Les documents qui servent à des fins de preuve ou qui sont nécessaires pour d'autres raisons objectives doivent être conservés plus longtemps.

5. Quelles données personnelles sont traitées ?

Les collaborateurs ne doivent collecter et traiter que les données personnelles nécessaires à la réalisation des objectifs (minimisation des données).

Certains traitements de données, comme celui de l'archivage, sont nécessaires pour que l'employeur puisse remplir ses obligations légales ou contractuelles.

6. Quels autres éléments les collaborateurs doivent-ils prendre en compte lors du traitement de données personnelles ?

Si le mandat existe avec une entreprise cliente, la prise de contact directe des collaborateurs du client n'est autorisée que si elle est nécessaire à l'exécution du contrat d'assurance ou à la clarification du sinistre.

Si des collaborateurs de l'entreprise cliente sont contactés directement à d'autres fins, par exemple pour négocier d'autres assurances, il faut s'assurer que ces personnes ont donné leur consentement à la prise de contact.

7. Comment les collaborateurs traitent-ils les demandes des personnes concernées ?

En vertu de la nouvelle loi suisse sur la protection des données, les personnes concernées peuvent exiger le renseignement, la remise, la transmission, la rectification ou la suppression de leurs données personnelles. Elles peuvent en outre s'opposer à des traitements illicites ou révoquer leur consentement (p. ex. opt-in pour une newsletter).

Tous les courriers, appels téléphoniques, courriels ou autres contenant de telles demandes seront immédiatement transmis à Sébastien Beck, Administrateur. Il est chargé de coordonner les demandes et d'y répondre. Il ne sera répondu à aucune demande par téléphone.

Les demandes ne sont acceptées que si la personne concernée a fourni une preuve d'identité appropriée et s'il n'existe aucun motif légal de report, de restriction ou d'exclusion.

La réponse aux demandes n'entraîne en principe pas de frais pour les personnes concernées. Pour les demandes particulièrement volumineuses, une participation aux frais pouvant aller jusqu'à 300 CHF peut être demandée.

8. Quelles sont les obligations de déclaration des collaborateurs ?

Un incident de sécurité informatique peut se produire, par exemple, lorsqu'un collaborateur clique sur une URL dans un e-mail suspect, ouvre une pièce jointe suspecte, exécute des macros dans des documents, lorsque des données sont cryptées, que des données d'accès sont perdues ou transmises, ou que des données personnelles sont communiquées à des personnes non autorisées (par exemple, envoi d'un e-mail à plusieurs destinataires qui ne se connaissent pas sans utiliser la fonction Bcc ; communication de données personnelles par téléphone sans vérification de l'identité de l'appelant).

Les employés signalent immédiatement toute suspicion ou connaissance d'un incident de sécurité informatique à Sébastien Beck, Administrateur. La perte d'équipements utilisés à des fins professionnelles ou de documents physiques doit également être signalée sans délai.

Si des données personnelles sont concernées, la personne responsable en réfère immédiatement à la direction, qui décide ensuite de la communication interne et externe et d'une éventuelle notification au Préposé fédéral à la protection des données et, le cas échéant, à d'autres autorités de surveillance.

9. Quelles sanctions peuvent être imposées aux collaborateurs ?

Tous les collaborateurs veillent à ce que toutes les données et informations dont ils prennent connaissance dans le cadre de leur relation de travail soient traitées de manière confidentielle. Si les collaborateurs ne respectent pas leur devoir de confidentialité, l'employeur et/ou la personne concernée par la violation peut demander des comptes au collaborateur.

Les collaborateurs peuvent être punis en cas de violation intentionnelle de leurs obligations (violation du secret professionnel ou du secret d'affaires selon l'art. 62 de la loi suisse sur la protection des données ou l'art. 162 du code pénal suisse).

C. Sécurité de l'information

10. Comment les collaborateurs utilisent-ils les outils informatiques ?

L'employeur met à la disposition des collaborateurs des ordinateurs et d'autres infrastructures informatiques pour l'exécution des obligations contractuelles. Pour que la protection des données soit garantie, les collaborateurs doivent mettre en œuvre les mesures suivantes :

- Tous les appareils, réseaux et logiciels nécessaires à l'exécution des obligations contractuelles sont mis à la disposition des collaborateurs. Toute autre infrastructure non autorisée ne doit pas être utilisée à des fins professionnelles.
- Les appareils privés ne doivent pas être utilisés à des fins professionnelles et ceux-ci ne doivent pas être connectés aux appareils de réseau de l'employeur.
- Les paramètres de base des appareils, des réseaux ou des logiciels ne doivent pas être modifiés par les collaborateurs.
- Le réseau utilisé pour le bureau à distance ou à domicile (par exemple Handyhotsport) doit être protégé par un mot de passe fort. Les réseaux publics et non protégés par un mot de passe ne peuvent être utilisés que via un VPN.
- Le support pour l'infrastructure informatique est assuré par Sébastien Beck, Administrateur.
- Les collaborateurs ne doivent pas installer de logiciels supplémentaires sans consulter Sébastien Beck, Administrateur.

11. Comment les informations sont-elles protégées par les collaborateurs ?

11.1. Données de connexion

L'utilisation soigneuse des données de connexion représente une part importante de la sécurité des données. Les collaborateurs doivent respecter les règles suivantes :

- Les collaborateurs sont tenus de choisir des mots de passe uniques et forts. Les mots de passe et noms d'utilisateur utilisés dans le cadre professionnel ne doivent pas être utilisés à des fins privées et ne doivent pas être portés à la connaissance d'autres personnes.
- Les mots de passe ne doivent être utilisés que pour un accès spécifique.
- Aucun mot de passe ne doit être noté. Si l'employeur met à disposition des solutions de mots de passe, le collaborateur est tenu de les utiliser.

11.2. Stockage des données

Les données professionnelles ne peuvent être stockées que sur les systèmes de stockage de fichiers mis à disposition par l'employeur. Aucune donnée professionnelle ne doit être enregistrée sur des systèmes de stockage de fichiers privés ou sur des nuages. Si le courrier électronique, le calendrier ou d'autres applications sont synchronisés sur des appareils privés, ils doivent être exclus des éventuelles sauvegardes dans le nuage.

11.3. Communication

Les données personnelles et les informations commerciales considérées comme confidentielles doivent être communiquées en toute sécurité. Les collaborateurs doivent donc respecter les consignes suivantes :

- Si les assurances mettent à disposition des portails pour le téléchargement d'informations, ceux-ci doivent être utilisés par les collaborateurs.
- Si des données personnelles sensibles ou des informations confidentielles sont envoyées par e-mail, les e-mails sont cryptés de bout en bout ou la transmission s'effectue via un lien crypté ou une plateforme sécurisée.
- Si une transmission sécurisée n'est pas possible, une confirmation écrite est demandée au client, selon laquelle il accepte une transmission ordinaire des données (par exemple sous forme de pièce jointe à un e-mail).
- Si des informations sensibles ou confidentielles, notamment des mots de passe, sont envoyées par courrier, les documents sont envoyés en recommandé/courrier plus.
- Les collaborateurs qui téléphonent en dehors de leur lieu de travail s'assurent qu'aucun tiers non autorisé n'ait connaissance de données personnelles ou de secrets d'affaires.
- Lors d'appels vidéo, aucun tiers non impliqué ne doit être visible dans le champ de la caméra. Les enregistrements ne sont autorisés que s'ils ont été annoncés au préalable.
- Lorsqu'ils partagent leur écran, les collaborateurs doivent s'assurer que des tiers non autorisés n'ont pas accès aux données professionnelles.
- Les services de messagerie privée ne doivent pas être utilisés pour des communications professionnelles.

11.4. Politique de Clean Desk et de Clear Screen

Les collaborateurs suivent une politique de Clean Desk et de Clear Screen et s'engagent à respecter les consignes suivantes :

- Ils rangent tous les documents et dossiers à la fin de la journée ou en cas d'absence prolongée.
- Après les réunions, tous les documents et dossiers sont retirés de la salle de réunion. En outre, les informations figurant sur les tableaux blancs et les flipcharts sont retirées ou détruites.
- Les collaborateurs qui quittent leur poste de travail verrouillent tous les écrans ou se déconnectent. Cela vaut également pour les absences de courte durée comme les pauses café.

11.5. Restriction d'accès et d'entrée

Les collaborateurs ne doivent pas permettre à des tiers non autorisés d'accéder aux locaux non publics. Il est interdit aux personnes externes de se rendre dans les locaux non accessibles au public sans être accompagnées.

11.6. Comment la protection contre les logiciels malveillants est-elle assurée ?

Les logiciels malveillants représentent un risque élevé pour la sécurité des données. Les collaborateurs sont donc tenus de respecter les consignes suivantes :

- Les collaborateurs ne doivent pas désactiver ou contourner les logiciels installés.
- Les collaborateurs doivent installer sans délai toutes les mises à jour et actualisations officielles.
- Les pièces jointes et les documents provenant d'expéditeurs inconnus ne doivent pas être ouverts. Les collaborateurs sont tenus de signaler les e-mails suspects à Sébastien Beck, Administrateur.
- Les liens vers des sites web externes ne doivent être cliqués que s'ils sont sûrs.
- Aucun document ou logiciel ne doit être téléchargé à partir de sites web inconnus.
- Dans la mesure du possible, les collaborateurs ne peuvent visiter que des sites web certifiés SSL.
- Aucun courrier électronique privé ne doit être transféré vers des adresses électroniques professionnelles.

11.7. Quelles sont les directives que les collaborateurs doivent respecter lorsqu'ils utilisent Internet ?

L'utilisation d'Internet peut présenter un risque pour la sécurité des données. Les collaborateurs doivent donc respecter les règles suivantes :

- La navigation sur Internet et le téléchargement de documents ne sont autorisés qu'à des fins professionnelles.
- Il est interdit de visiter des sites web dont le contenu comprend : des propos ou des représentations pornographiques, sexistes, racistes ou faisant l'apologie de la violence ; des systèmes pyramidaux et boule de neige ; la promotion et le financement du terrorisme, les casinos en ligne ; tout autre contenu illégal ou contraire aux bonnes mœurs.
- Les informations commerciales ne doivent pas être téléchargées sur Internet, et notamment aucun contenu ne doit être saisi dans des outils de traduction gratuits ou des chatbots ou autres applications d'intelligence artificielle. Ces outils peuvent éventuellement réutiliser les informations saisies pour entraîner leurs modèles et systèmes d'intelligence artificielle.

D. Contact

Les questions ou remarques peuvent être adressées à l'adresse suivante :

Sébastien Beck
Sebastien.beck@synerisk.ch
Tél. +41 22 716 19 19

E. Effet

La présente directive entre en vigueur le 01.01.2024.