Règlement sur la protection et la sécurité des données

Table des matières

1 Généralités

1.1 Validité

Les dispositions suivantes s'appliquent à tous les collaborateurs d'Allianz Suisse Société d'Assurances SA, d'Allianz Suisse Société d'Assurances sur la Vie SA et de leurs filiales (en particulier, CAP Compagnie d'Assurance de Protection Juridique S.A., Société de conseil en prévoyance SA, Quality1 AG, AMOS IT Suisse AG et Allianz Suisse Immobilier SA) ainsi que des agences générales d'Allianz Suisse.

1.2 Bases

Le présent règlement repose sur les dispositions de la loi fédérale sur la protection des données (LPD) ainsi que sur la directive «Allianz Standard for Data Protection and Privacy» (ASDP) du groupe Allianz.

Toute réglementation supplémentaire valable dans les différents domaines spécialisés est expressément réservée.

1.3 Champ d'application

La protection des données vise à protéger la personnalité et les droits fondamentaux des personnes qui font l'objet d'un traitement de données.

Tout collaborateur est tenu de se conformer aux principes et aux règles de la protection des données dans l'exercice de ses activités. Les cadres doivent faire respecter ces dispositions dans leur domaine de compétence et procéder à des contrôles réguliers.

Les règles s'appliquent au traitement tant automatisé que manuel des données relatives aux personnes physiques et aux personnes morales, que ces données soient sur papier ou enregistrées sur un support électronique.

Les dispositions relatives au traitement confidentiel des données personnelles et des autres données et informations professionnelles restent valables même après la fin des rapports de travail.

1.4 Niveaux de confidentialité

Données publiques («public»):
Données destinées au grand public et accessibles à tout un chacun.

Données à usage interne («internal»):
Données qui servent exclusivement à un usage interne au sein du groupe Allianz Suisse ou des sociétés concernées et qui ne sont ni destinées au grand public ni accessibles à tout un chacun.

Les données sans mention explicite sont considérées comme «internes».

Données confidentielles («confidential»):
Données auxquelles a accès un cercle restreint de personnes en ayant besoin pour leur travail.

Données strictement confidentielles («strictly confidential»):
Données qui pourraient avoir de lourdes conséquences pour Allianz Suisse si des personnes non autorisées en avaient connaissance. Seuls des personnes ou des cercles de personnes clairement désignés peuvent y avoir accès.

1.5 Classification des données

Le «data owner» compétent assigne un niveau de confidentialité à toutes les données d'Allianz Suisse. Celui-ci vaut également pour toutes les copies des données concernées, indépendamment du type de support et de traitement. Par «data owner», on entend généralement le

cadre responsable du service dans lequel les données ont été saisies ou collectées pour la première fois. Selon le principe maximum, les ensembles de données composés de plusieurs éléments sont affectés au niveau de l'élément ayant la classification la plus élevée. La classification des différentes données est publiée et accessible à tous les collaborateurs.

1.6 Données personnelles

Les données personnelles sont toutes les informations qui se rapportent à une personne physique ou morale identifiée ou identifiable.

En vertu de la LPD, les données sensibles englobent les données personnelles sur les opinions ou activités religieuses, philosophiques, politiques ou syndicales, la santé, la sphère intime ou l'appartenance à une race, des mesures d'aide sociale ainsi que des poursuites ou sanctions pénales et administratives.

Un profil de la personnalité est un assemblage de données qui permet d'apprécier les caractéristiques essentielles de la personnalité d'une personne physique.

Ces deux catégories de données doivent impérativement être classées comme confidentielles, traitées de manière très restrictive et bénéficier d'une protection stricte.

1.7 Principe de nécessité («need to know»)

Chaque collaborateur doit posséder les droits d'accès nécessaires à son travail quotidien. Le principe «need to know» est formulé comme suit: «Autant que nécessaire, le moins possible».

2 Dispositions concernant la gestion des données

2.1 Collecte de données personnelles

- Les données personnelles ne doivent être collectées que dans un but légitime lié à l'activité.

- Les données personnelles ne doivent être collectées que si la personne concernée en est informée et donne son accord ou si la collecte est autorisée d'une autre manière ou prescrite par la loi. Leur obtention auprès de sources tierces (p. ex. Internet ou fournisseurs de données) sans information ni consentement des personnes concernées est illicite si elle n'est pas directement liée à la conclusion ou au traitement d'un contrat et s'il n'existe aucun autre motif légitime suffisant (cf. ch. 3).

- Si l'on s'appuie sur le consentement, celui-ci doit être donné volontairement et après une information adéquate. La personne concernée peut le retirer.

- La collecte de données et son but doivent être transparents pour la personne concernée. Des exceptions sont permises uniquement si la loi les prévoit ou les autorise (cf. ch. 3). Le but de la collecte doit être communiqué à la personne concernée ou être identifiable au vu des circonstances.

- Les données collectées ou générées doivent être correctes et exhaustives par rapport au but poursuivi. Celles qui sont erronées seront corrigées ou, si cela n'est pas possible, supprimées, à moins qu'elles ne soient soumises à une obligation de conservation ou qu'il n'existe un intérêt supérieur. Dans ce cas, le caractère erroné devra être mentionné dans la mesure du possible.

- Si les données collectées constituent une nouvelle base de données, celle-ci doit être annoncée au conseiller interne en protection des données. De plus, les données seront affec-

tées à un «data owner», qui les classera en fonction de leur confidentialité (cf. ch. 1.4).

- Les formulaires et les pages Internet servant à collecter des données doivent comporter une clause de protection des données, qui informe de manière appropriée sur le but de la collecte et le traitement des données. Cette clause doit être validée par le conseiller interne en protection des données.

2.2 Traitement des données

- En principe, les données personnelles ne doivent être traitées que dans le but pour lequel elles ont été collectées. Le traitement doit être licite et effectué conformément aux principes de la bonne foi et de la proportionnalité.

- En vertu du principe «need to know» (cf. ch. 1.7), les données personnelles ne doivent être accessibles qu'aux collaborateurs en ayant besoin pour leur travail. Elles doivent être protégées contre tout traitement non autorisé.

- Les documents confidentiels ou personnels doivent être conservés sous clé lorsqu'un collaborateur s'absente de son poste de travail.

- Les documents confidentiels et strictement confidentiels et les supports de données qui comprennent des données correspondantes doivent être désignés comme tels.

- Les renseignements personnels ne doivent être fournis qu'à la personne concernée. Ils sont généralement donnés par écrit, mais l'identité de la personne concernée doit d'abord être vérifiée. Les demandes de renseignements détaillés concernant toutes les données d'une personne concernée seront transmises sans délai au conseiller interne en protection des données.

- Le traitement de données par des tiers et la remise de données à des tiers ne sont autorisés qu'après un examen des dispositions de la LPD par le conseiller interne en protection des données et/ou par Droit et Compliance. En général, une convention de confidentialité est nécessaire en la matière.

- L'enregistrement de données professionnelles sur des supports de données librement accessibles ou privés (p. ex. «public clouds», réseaux sociaux ou supports Internet tels qu'iCloud, Google Drive ou Dropbox) est interdit. L'utilisation d'autres services externes de «cloud» requiert l'accord exprès du conseiller interne en protection des données.

- Les données confidentielles transmises par l'intermédiaire de réseaux publics doivent être cryptées. À cet égard, il est possible de crypter la connexion réseau ou les données proprement dites.

- Lors d'entretiens concernant des informations confidentielles ou personnelles, il faut s'assurer qu'aucune personne non autorisée ne peut entendre. Il convient notamment d'en tenir compte lors de conversations téléphoniques tenues en public.

- En principe, tout transfert transfrontalier de données personnelles requiert l'accord préalable du conseiller interne en protection des données, sauf si celles-ci sont envoyées à la personne concernée ou si le processus de transfert a déjà été validé dans un cas concret. Cela s'applique également à la transmission de données personnelles au groupe Allianz à Munich ou à ses filiales.

- En principe, le transfert de données confidentielles ou la transmission de courriels confidentiels ne sont autorisés qu'avec l'accord du «data owner».

- Les données concernant la prévoyance professionnelle (LPP, assurance collective) et l'assurance-accidents obligatoire ainsi que les données de sinistres de l'assurance de protection juridique sont soumises à un devoir de discrétion défini dans des lois spéciales; elles doivent donc être traitées de manière confidentielle. Toute violation de ce devoir de discrétion peut entraîner des sanctions pénales.

2.3 Destruction des données

- Les données seront conservées aussi longtemps que cela est nécessaire au but du traitement et que la loi ou les règlements le prescrivent.

- Les documents, notes, impressions de courriels, captures d'écran, etc. sous forme papier doivent obligatoirement être éliminés dans les conteneurs fermés mis à disposition à cet effet ou détruits au moyen d'un broyeur de documents. Les corbeilles à papier ouvertes sont réservées à l'élimination des journaux, du carton, des emballages, de la publicité, des catalogues et des enveloppes ne mentionnant pas le nom de personnes privées.

  En cas de doute, il convient d'utiliser les conteneurs fermés.

- Les données électroniques enregistrées sur des supports de données réinscriptibles (disques durs, clés USB) doivent être effacées à l'aide d'un procédé de «wiping» (écrasement des données) ou détruites physiquement avant l'élimination de leur support afin qu'elles ne puissent plus être reconstituées.

- Les supports de données qui ne peuvent pas être écrasés (p. ex. CD, DVD ou d'autres supports de données optiques) doivent être détruits physiquement (p. ex. découpage) avant leur élimination.

3 Exceptions

Dans la mesure où les dispositions précédentes concernant le traitement des données prévoient des exceptions, celles-ci doivent être soumises au conseiller interne en protection des données ou à Droit et Compliance. Une approbation de l'exception n'est pas requise si le traitement des données concerné est expressément autorisé par un autre règlement relatif à la protection des données. En cas de doute, l'instance supérieure sera consultée.

4 Violation des dispositions sur la protection des données

Toute infraction à la loi sur la protection des données ou aux dispositions du présent règlement, en particulier les pertes et divulgations involontaires de données, doit être immédiatement notifiée au conseiller interne en protection des données.

Le respect des dispositions légales relatives à la protection des données est contrôlé régulièrement par le conseiller interne en protection des données et, au besoin, par d'autres personnes. Le non-respect de ces dispositions peut entraîner des sanctions en matière de droit du travail, voire des sanctions pénales pour les collaborateurs concernés.

5 Règles concernant la gestion des données selon leur niveau de classification

Le tableau suivant récapitule les principales règles applicables à la gestion quotidienne des données en fonction de leur niveau de classification:

	Données publiques	Données internes	Données confidentielles	Données strictement confidentielles
Exemples de données par niveau de classification	• Prospectus publicitaires, brochures • Descriptifs de produits • Rapports de gestion • Statuts • Communiqués de presse • Mémentos	• Données de base des clients (nom, adresse, date de naissance, etc.) • Propositions d'assurance, polices • Directives et règlements • Organigrammes • Descriptions de poste • Données de projets	• Données de santé, rapports médicaux • Données salariales • Données personnelles • Données de poursuite • Procès-verbaux des séances du Directoire et du Conseil d'administration • Contrats avec des courtiers et des partenaires de coopération	• Informations sur les projets et la stratégie de l'entreprise • Mots de passe
Désignation des documents	Mention «public» sur la page de couverture si cela peut être utile	Les données sans mention sont considérées comme internes	Mention «confidentiel» sur la page de couverture ou en pied de page Indication du «data owner» ou de l'auteur	Mention «strictement confidentiel» sur la page de couverture ou en pied de page Indication du «data owner» ou de l'auteur
Cercle des destinataires	Tout un chacun	Tous les collaborateurs du groupe Allianz Suisse selon le principe «need to know»	Cercle restreint de personnes selon le principe «need to know»	Cercle restreint de personnes; doit être indiqué nommément dans le document
Envoi par la poste	Aucune obligation particulière	**Interne:** aucune obligation particulière **Externe:** sous enveloppe cachetée	**Interne et externe:** sous enveloppe cachetée avec la mention «personnel»	Autorisé uniquement avec le consentement du «data owner» **Interne:** sous enveloppe cachetée avec la mention «strictement confidentiel». Si possible, remise en mains propres **Externe:** sous enveloppe cachetée avec la mention «personnel»

	Données publiques	Données internes	Données confidentielles	Données strictement confidentielles
Fax	Aucune obligation particulière	Aucune obligation particulière	La réception personnelle par le destinataire doit être garantie	Non autorisé
Impression	Aucune obligation particulière	Aucune obligation particulière	Aller chercher immédiatement les documents imprimés à l'imprimante	Impression uniquement avec l'accord du «data owner»; aller chercher immédiatement les documents imprimés à l'imprimante
Envoi par courriel	Aucune obligation particulière	**Envoi interne:** sélectionner les adresses e-mail dans le répertoire d'adresses d'Allianz **Envoi externe:** cryptage requis lors de l'envoi de données personnelles à des tiers[1]	- Cryptage - Mention «confidentiel» - Transmission des courriels confidentiels uniquement avec l'accord du «data owner»	**Envoi interne:** - Cryptage - Mention «strictement confidentiel» - Transmission des courriels strictement confidentiels uniquement avec l'accord du «data owner» **Envoi externe:** non autorisé
Transfert par FTP	Aucune obligation particulière	Uniquement via un compte dédié spécifiquement au destinataire Cryptage requis (connexion ou données)	Autorisé uniquement avec le consentement du «data owner» Uniquement via un compte dédié spécifiquement au destinataire Cryptage requis (connexion ou données)	Non autorisé
Duplicata (p. ex. copies)	Aucune obligation particulière	Aucune obligation particulière	Autorisé uniquement avec l'accord du «data owner»	Autorisé uniquement avec l'accord du «data owner»
Archivage physique	Aucune obligation particulière	Documents et supports de données conservés sous clé lorsque l'on s'absente du poste de travail	Documents et supports de données conservés sous clé lorsque l'on s'absente du poste de travail Documents confidentiels d'un dossier conservés dans une enveloppe séparée, fermée et clairement désignée	Documents toujours conservés sous clé lorsqu'ils ne sont pas utilisés

[1] Sont exclus de l'obligation de cryptage:
- les courriels qui ne se rapportent pas directement à une personne physique ou morale identifiée ou identifiable (p. ex. aucune donnée personnelle ou données personnelles rendues anonymes);
- les courriels concernant une personne qui a accepté que ses données soient envoyées directement et sans chiffrement.

	Données publiques	Données internes	Données confidentielles	Données strictement confidentielles
Archivage électronique	Aucune obligation particulière	Respect du principe «need to know» Enregistrement sur des supports de données portatifs autorisé uniquement avec un cryptage et l'accord du «data owner»	Sur des supports de données non portatifs d'Allianz, si possible avec cryptage Enregistrement sur des supports de données portatifs autorisé uniquement avec un cryptage et l'accord du «data owner» Support de données désigné comme confidentiel	Cryptage obligatoire Enregistrement interdit sur des supports de données portatifs (exception: ordinateurs portables cryptés d'Allianz)
Transmission	Aucune obligation particulière	Transmission interne selon le principe de nécessité À des tiers externes uniquement avec l'accord du «data owner» Renseignements à la personne concernée uniquement après vérification de son identité Les demandes de renseignements et de consultation et les autres demandes concernant les données d'une personne sont traitées par le conseiller interne en protection des données	Transmission uniquement avec l'accord du «data owner» Renseignements à la personne concernée uniquement après vérification de son identité Les demandes de renseignements et de consultation et les autres demandes concernant les données d'une personne sont traitées par le conseiller interne en protection des données	En général, autorisée par le «data owner» lui-même ou uniquement à sa demande
Réseaux sociaux (Facebook, Twitter, blogs, etc.)	Aucune obligation particulière	Interdiction de charger des données et de communiquer des informations internes	Interdiction de charger des données et de communiquer des informations confidentielles	Interdiction de charger des données et de communiquer des informations strictement confidentielles
Perte, fuite, compromission	Aucune obligation particulière	Notification immédiate au «data owner» et au conseiller interne en protection des données	Notification immédiate au «data owner» et au conseiller interne en protection des données	Notification immédiate au «data owner» et au conseiller interne en protection des données

6 Entrée en vigueur

Le présent règlement sur la protection et la sécurité des données entre en vigueur le 1er janvier 2016 et remplace la version du 1er janvier 2008.