Reglement Datenschutz und Datensicherheit

Inhaltsverzeichnis

1 Allgemeines

1.1 Geltungsbereich

Die nachfolgenden Bestimmungen gelten für alle Mitarbeitenden der Allianz Suisse Versicherungs-Gesellschaft AG, der Allianz Suisse Lebensversicherungs-Gesellschaft AG sowie deren Tochtergesellschaften (insbesondere CAP Rechtsschutz-Versicherungsgesellschaft AG, Gesellschaft für Vorsorgeberatung AG, Quality1 AG, AMOS IT Suisse AG und Allianz Suisse Immobilien AG) und der Generalagenturen der Allianz Suisse.

1.2 Grundlagen

Das vorliegende Reglement basiert auf den Bestimmungen des Bundesgesetzes über den Datenschutz (DSG) sowie der vom Allianz Konzern herausgegebenen Policy "Allianz Standard for Data Protection and Privacy" (ASDP).

Weitergehende Regelungen, die in den einzelnen Fachbereichen gelten, bleiben ausdrücklich vorbehalten.

1.3 Anwendungsbereich

Der Datenschutz bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, deren Daten bearbeitet werden.

Alle Mitarbeitenden sind gehalten, bei ihrer Tätigkeit die Grundsätze und Regeln des Datenschutzes einzuhalten. Die Führungskräfte sind verpflichtet, die Einhaltung der datenschutzrechtlichen Bestimmungen in ihrem Zuständigkeitsbereich durchzusetzen und regelmässig zu kontrollieren.

Die Regelungen gelten sowohl für das automatische als auch für das manuelle Bearbeiten von Daten natürlicher und juristischer Personen, unabhängig davon, ob es sich um auf Papier oder elektronisch gespeicherte Daten handelt.

Die Bestimmungen bezüglich vertraulicher Behandlung von personenbezogenen und anderen geschäftlichen Daten und Informationen gelten über die Beendigung des Arbeitsverhältnisses hinaus.

1.4 Vertraulichkeitsstufen

Öffentliche Daten (public):
Daten, die für die Öffentlichkeit bestimmt und zugänglich sind.

Daten für den internen Gebrauch (internal):
Daten, die nur für den internen Gebrauch innerhalb der Allianz Suisse Gruppe oder innerhalb der betroffenen Gesellschaften und nicht für die Öffentlichkeit bestimmt oder zugänglich sind.

Nicht explizit gekennzeichnete Daten gelten als „intern“.

Vertrauliche Daten (confidential):
Daten, auf welche nur ein eingeschränkter Personenkreis Zugriff hat, welcher diese Daten zur Durchführung seiner Aufgaben benötigt.

Streng vertrauliche Daten (strictly confidential):
Daten, deren Kenntnis durch Unbefugte schwerwiegende Konsequenzen für die Allianz Suisse haben könnte. Diese Daten dürfen nur sehr restriktiv und namentlich bezeichneten Personen bzw. Personenkreisen zugänglich gemacht werden.

1.5 Datenklassifizierung

Sämtliche Daten bei der Allianz Suisse werden durch die zuständigen Information-Owner einer Vertraulichkeitsstufe zugeordnet. Die Klassifizierungsstufe gilt auch für sämtliche Kopien der

betreffenden Daten, unabhängig vom Speichermedium und der Art der Bearbeitung. Als Information-Owner gilt in der Regel die verantwortliche Führungskraft desjenigen Geschäftsbereichs, in welchem eine Datensammlung erstmalig erzeugt oder erhoben wird. Datensammlungen die aus verschiedenen Datenelementen zusammengesetzt sind, erhalten nach dem Maximumprinzip die Stufe des höchst klassifizierten Datenelements. Die Klassifizierung der einzelnen Daten wird publiziert und ist allen Mitarbeitenden zugänglich.

1.6 Personendaten

Personendaten sind alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person beziehen.

Besonders schützenswerte Personendaten umfassen gemäss DSG religiöse, weltanschauliche, politische oder gewerkschaftliche Ansichten oder Tätigkeiten, Daten betreffend die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, Massnahmen der sozialen Hilfe sowie administrative oder strafrechtliche Verfolgungen und Sanktionen.

Persönlichkeitsprofile sind Zusammenstellungen von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlauben.

Beide Datenkategorien sind zwingend als vertraulich klassifiziert und müssen besonders restriktiv bearbeitet und streng geschützt werden.

1.7 Notwendigkeitsprinzip (need-to-know)

Jedem/jeder Mitarbeitenden sind lediglich diejenigen Zugriffsrechte zu gewähren, die zur Erfüllung seiner/ihrer Aufgaben notwendig sind. Das Notwendigkeitsprinzip besagt: „Soviel wie nötig, so wenig wie möglich“.

2 Bestimmungen bezüglich Umgang mit Daten

2.1 Beschaffung von Personendaten

- Personendaten dürfen nur für legitime, geschäftsbezogene Zwecke erhoben werden.

- Personendaten dürfen nur erhoben werden, wenn die betroffene Person davon Kenntnis hat und damit einverstanden ist, oder die Erhebung anderweitig gesetzlich erlaubt oder vorgeschrieben ist. Es ist nicht zulässig, personenbezogene Daten aus Drittquellen (z.B. Internet oder Datenbroker) ohne Kenntnis und Einverständnis der Betroffenen zu beschaffen, wenn dies nicht in einem unmittelbaren Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrages steht und es hierfür keinen anderen hinreichenden Rechtfertigungsgrund gibt (siehe Ziffer 3).

- Wird auf die Einwilligung abgestellt, so muss diese freiwillig und nach angemessener Information erfolgen; die betroffene Person kann ihre Einwilligung zurückziehen.

- Die Datenbeschaffung und deren Zweck muss für die betroffene Person transparent sein; Ausnahmen sind nur zulässig, soweit das Gesetz dies vorsieht oder erlaubt (siehe Ziffer 3). Der Zweck muss der betroffenen Person kommuniziert werden oder er muss aus den Umständen erkennbar sein.

- Die erhobenen oder generierten Daten müssen im Hinblick auf den damit verfolgten Zweck grundsätzlich korrekt und vollständig sein. Fehlerhafte Daten müssen berichtigt oder, falls dies nicht möglich ist, vernichtet werden, sofern dem keine Aufbewahrungspflicht oder sonst ein überwiegendes Interesse entgegensteht. In einem solchen Fall ist die Fehlerhaftigkeit nach Möglichkeit zu vermerken.

- Entsteht durch die Datenerhebung eine neue Datensammlung, so ist diese dem internen Datenschutzbeauftragten zu melden. Ausserdem ist die Datensammlung einem Information Owner zuzuordnen und von diesem nach Vertraulichkeit zu klassifizieren (siehe Ziffer 1.4).

- Erhebungsformulare und Webseiten, die der Datenerhebung dienen, müssen eine Datenschutzklausel beinhalten, die in angemessener Weise über den Erhebungszweck und die Bearbeitung der Daten informiert. Die Datenschutzklausel muss mit dem internen Datenschutzbeauftragten abgestimmt werden.

2.2 Datenbearbeitung

- Personendaten dürfen grundsätzlich nur zu den Zwecken bearbeitet werden, zu denen sie beschafft wurden. Die Bearbeitung muss rechtmässig, nach Treu und Glauben und verhältnismässig erfolgen.

- Daten dürfen gemäss dem Notwendigkeitsprinzip (siehe Ziffer 1.7) nur denjenigen Mitarbeitenden zugänglich gemacht werden, welche diese für ihre Arbeit benötigen. Sie sind gegen unbefugtes Bearbeiten zu schützen.

- Vertrauliche oder personenbezogene Unterlagen müssen bei Abwesenheit vom Arbeitsplatz unter Verschluss gehalten werden.

- Vertrauliche und streng vertrauliche Dokumente rsp. die Datenträger, die solche Daten enthalten, sind grundsätzlich entsprechend zu kennzeichnen.

- Personenbezogene Auskünfte dürfen nur der betroffenen Person erteilt werden und erfolgen regelmässig schriftlich. In einem ersten Schritt muss dafür die Identität der betroffenen Person sichergestellt werden. Umfassende Auskunftsbegehren über sämtliche Daten einer betroffenen Person sind unverzüglich dem internen Datenschutzbeauftragten weiterzuleiten.

- Die Bearbeitung von Daten durch Dritte und die Weitergabe von Daten an Drittparteien ist nur erlaubt, nachdem dies durch den internen Datenschutzbeauftragten und/oder Legal & Compliance auf die Vorgaben des DSG geprüft wurde. Regelmässig ist dafür eine Vertraulichkeitsvereinbarung erforderlich.

- Das Abspeichern von geschäftsbezogenen Daten auf öffentlich zugänglichen oder privaten Datenspeichern (z.B. Public Clouds, Social Media oder Internet-Speicher wie iCloud, Google Drive oder Dropbox) ist verboten. Die Nutzung von anderen externen Cloud-Diensten ist nur mit der ausdrücklichen Genehmigung des internen Datenschutzbeauftragten erlaubt.

- Die Übertragung von vertraulichen Daten über öffentliche Netzwerke muss grundsätzlich verschlüsselt erfolgen. Dabei können entweder die Netzverbindung oder die Daten selbst verschlüsselt werden.

- Bei Gesprächen über vertrauliche oder personenbezogene Informationen ist darauf zu achten, dass keine unbefugten Personen mithören können. Dies ist insbesondere bei telefonischen Unterredungen in der Öffentlichkeit zu beachten.

- Bei grenzüberschreitender Weitergabe von personenbezogenen Daten muss vorgängig grundsätzlich die Genehmigung durch den internen Datenschutzbeauftragten eingeholt werden, ausser, die Daten werden an die betroffene Person selbst gesandt oder der Prozess der Weitergabe ist im konkreten Fall bereits freigegeben worden. Dies gilt auch für die Weiterleitung von Personendaten an den Allianz Konzern in München bzw. an Allianz-Konzerngesellschaften.

- Die Weitergabe von vertraulichen Daten rsp. Weiterleitung von vertraulichen e-Mails ist grundsätzlich nur mit dem Einverständnis des Information-Owners gestattet.

- Namentlich Daten betreffend die berufliche Vorsorge (BVG, Kollektivversicherung) und der obligatorischen Unfallversicherung sowie Schadendaten der Rechtsschutzversicherung unterliegen einer spezialgesetzlichen Schweigepflicht und müssen deshalb vertraulich behandelt werden. Die Verletzung spezialgesetzlicher Schweigepflichten kann strafrechtliche Konsequenzen haben.

2.3 Datenentsorgung

- Daten dürfen grundsätzlich nur solange aufbewahrt werden, wie es der Bearbeitungszweck oder die gesetzlich oder reglementarisch vorgeschriebenen Aufbewahrungsfristen erfordern.

- Sämtliche Unterlagen, Dokumente, Aktennotizen, e-Mail-Ausdrucke, Screenshots etc. in Papierform müssen ausnahmslos über die eigens zu diesem Zweck bereitgestellten, verschlossenen Container (Reisswolf) entsorgt oder in einem Schredder vernichtet werden. Die offenen Papierabfallbehälter dürfen nur für die Entsorgung von Zeitungen, Karton, Verpackungsmaterial, Werbung, Kataloge und nicht mit Absendern von Privatpersonen versehenen Briefumschlägen benutzt werden.

  Im Zweifelsfall ist Papierabfall über die verschlossenen Container zu entsorgen.

- Elektronisch auf überschreibbaren Datenträgern (Festplatten, Speichersticks) abgespeicherte Daten sind vor der Entsorgung des Datenträgers sicher über ein sog. Wipingverfahren (überschreiben der Daten) oder physischer Zerstörung zu löschen, so dass diese nicht mehr rekonstruierbar sind.

- Nicht überschreibbare Datenträger wie z.B. CD, DVD oder andere optische Datenspeicher, müssen vor der Entsorgung physisch zerstört werden (z.B. zerschneiden).

3 Ausnahmen

Soweit die vorstehenden Bestimmungen zum Umgang mit Daten Ausnahmen zulassen, sind diese entweder dem internen Datenschutzbeauftragten oder Legal & Compliance zu unterbreiten. Eine Ausnahmegenehmigung ist nicht erforderlich, wenn die fragliche Datenbearbeitung durch ein anderes Reglement auch im Hinblick auf den Datenschutz ausdrücklich erlaubt wird. Im Zweifel sind die vorstehenden Stellen zu konsultieren.

4 Verstösse gegen Datenschutz-Bestimmungen

Sämtliche Verstösse gegen das Datenschutzgesetz oder die Bestimmungen dieses Reglements, insbesondere ungewollte Verluste und Preisgaben von Daten, müssen dem internen Datenschutzbeauftragten umgehend gemeldet werden.

Die Einhaltung der datenschutzrechtlichen Bestimmung wird regelmässig durch den internen Datenschutzbeauftragten und ggf. weiteren Personen kontrolliert. Die Nichtbeachtung dieser Bestimmungen kann für die einzelnen Mitarbeitenden arbeitsrechtliche oder gar strafrechtliche Konsequenzen zur Folge haben.

5 Regelungen zum Umgang mit Daten nach Klassifizierungsstufen

Die wichtigsten, alltäglichen Regelungen bezüglich Umgang mit Daten für die verschiedenen Vertraulichkeitsstufen sind in der folgenden Übersichtstabelle zusammengefasst:

	Öffentliche Daten	**Interne Daten**	**Vertrauliche Daten**	**Streng vertrauliche Daten**
Beispiele von Daten pro Klassifizierungsstufe	• Werbeprospekte, Broschüren • Produktbeschreibungen • Geschäftsberichte • Statuten • Pressemitteilungen • Merkblätter	• Kunden-Basisdaten (Name, Adresse, Geburtsdatum etc.) • Versicherungsanträge /-Policen • Weisungen und Reglemente • Organigramme • Stellenbeschreibungen • Projektdaten	• Gesundheitsdaten, Arztberichte • Lohndaten • Personaldaten • Betreibungsdaten • Protokolle der Geschäftsleitung und des Verwaltungsrates • Verträge mit Maklern und Kooperationspartnern	• Informationen bez. Unternehmensplanung und Strategie • Passwörter
Kennzeichnung Dokumente	„public“ auf Deckblatt, wo sinnvoll	Daten ohne Kennzeichnung gelten als intern	„confidential“ auf Deckblatt oder in Fusszeile Information-Owner rsp. Verfasser muss ersichtlich sein	„strictly confidential“ auf Deckblatt oder in Fusszeile Information-Owner rsp. Verfasser muss ersichtlich sein
Empfängerkreis	Jedermann	Alle Mitarbeiter der Allianz Suisse Gruppe nach Notwendigkeitsprinzip	Eingeschränkter Personenkreis nach Notwendigkeitsprinzip	Eingeschränkter Personenkreis; muss im Dokument namentlich aufgeführt sein.
Postversand	Keine speziellen Auflagen	**Intern:** keine speziellen Auflagen **Extern:** in verschlossenem Couvert	**Intern und Extern: i**n verschlossenem Couvert mit Vermerk „persönlich“	Nur mit Einverständnis des Information-Owners erlaubt. **Intern:** In verschlossenem Couvert mit Vermerk „streng vertraulich“. Wenn möglich persönlich bringen. **Extern**: In verschlossenem Couvert mit Vermerk „persönlich“.
Fax	Keine speziellen Auflagen	Keine speziellen Auflagen	Persönlicher Empfang durch Adressat muss sichergestellt sein	Nicht erlaubt

	Öffentliche Daten	Interne Daten	Vertrauliche Daten	Streng vertrauliche Daten
Druck	Keine speziellen Auflagen	Keine speziellen Auflagen	Ausdrucke sofort vom Drucker entfernen	Ausdrucke nur mit Einverständnis des Information-Owners; sofort vom Drucker entfernen
Versand via e-Mail	Keine speziellen Auflagen	**Interner Versand**: E-Mail-Adressen über das Allianz-Adressverzeichnis anwählen **Externer Versand:** Verschlüsselung erforderlich beim Versand personenbezogener Daten an Dritte[1]	- verschlüsseln - als confidential bezeichnen - Weiterleitung vertraulicher e-Mails nur mit Einverständnis des Owners	**Interner Versand**: - verschlüsseln - als strictly confidential bzeichnen - Weiterleitung streng vertraulicher e-Mails nur mit Einverständnis des Owners **Externer Versand**: nicht erlaubt
FTP-Übermittlung	Keine speziellen Auflagen	Nur via dediziertes, für den Empfänger bestimmtes Account Verschlüsselung erforderlich (Verbindung oder Daten)	Nur mit Einverständnis des Information-Owners erlaubt. Nur via dediziertes, für den Empfänger bestimmtes Account Verschlüsselung erforderlich (Verbindung oder Daten)	Nicht erlaubt
Duplikate (z.B. Kopien)	Keine speziellen Auflagen	Keine speziellen Auflagen	Nur mit Einverständnis des Information-Owners zulässig	Nur mit Einverständnis des Information-Owners zulässig
Elektronische Ablage	Keine speziellen Auflagen	Need-to-know-Prinzip beachten. Speicherung auf mobilen Datenträgern ist nur verschlüsselt und mit Einverständnis des Information-Owners erlaubt .	Auf nicht mobilen Allianz Speichermedien wenn möglich verschlüsseln. Speicherung auf mobilen Datenträgern ist nur verschlüsselt und mit Einverständnis des Information-Owners erlaubt Datenträger als confidential kennzeichnen.	Zwingend verschlüsseln. Speicherung auf mobilen Datenträgern ist nicht erlaubt (Ausnahme: verschlüsselte Allianz Notebooks).

[1] Vom Verschlüsselungszwang ausgenommen sind:
- E-Mails aus deren Inhalt nicht auf eine bestimmte oder bestimmbare natürliche oder juristische Person geschlossen werden kann (z. B. Inhalt enthält keine oder anonymisierte Personendaten);
- E-Mails, bei denen die Betroffenen ihr Einverständnis erklärt haben, dass ihnen die Daten direkt und unverschlüsselt zugestellt werden dürfen.

	Öffentliche Daten	Interne Daten	Vertrauliche Daten	Streng vertrauliche Daten
Physische Ablage	Keine speziellen Auflagen	Unterlagen und Datenträger bei Abwesenheit vom Arbeitsplatz unter Verschluss halten	Unterlagen und Datenträger bei Abwesenheit vom Arbeitsplatz unter Verschluss halten. Vertrauliche Dokumente innerhalb eines Dossiers in separatem, verschlossenem und gekennzeichnetem Couvert	Unterlagen bei Nichtgebrauch stets unter Verschluss halten.
Weitergabe	Keine speziellen Auflagen	Interne Weitergabe gemäss Notwendigkeitsprinzip. An externe Parteien nur mit Einverständnis des Information-Owners. Auskünfte an die betroffene Person selbst nur nach Sicherstellung der Identität. Auskunfts- und Einsichtsbegehren sowie andere, die Daten einer Person betreffende Gesuche von ihr werden durch den internen Datenschutzbeauftragten bearbeitet.	Weitergabe grundsätzlich nur mit Einverständnis des Information-Owners. Auskünfte an die betroffene Person selbst nur nach Sicherstellung der Identität. Auskunfts- und Einsichtsbegehren sowie andere, die Daten einer Person betreffende Gesuche von ihr werden durch den internen Datenschutzbeauftragten bearbeitet.	In der Regel durch den Information-Owner selbst oder nur in dessen Auftrag erlaubt.
Social Media (Facebook, Twitter, Blogs etc)	Keine speziellen Auflagen	Datenupload und Mitteilung von internen Informationen nicht erlaubt	Datenupload und Mitteilung von vertraulichen Informationen nicht erlaubt	Datenupload und Mitteilung von streng vertraulichen Informationen nicht erlaubt
Verlust / Abfluss / Kompromittierung	Keine speziellen Auflagen	Unverzügliche Meldung an Information-Owner und internen Datenschutzbeauftragten	Unverzügliche Meldung an Information-Owner und internen Datenschutzbeauftragten	Unverzügliche Meldung an Information-Owner und internen Datenschutzbeauftragten

6 Inkrafttreten

Das vorliegende Reglement Datenschutz und Datensicherheit tritt am 1. Februar 2016 in Kraft und ersetzt die Version 1. Januar 2008.