Regolamento sulla protezione e la sicurezza dei dati

Inhaltsverzeichnis

1 Disposizioni generali

1.1 Ambito di applicazione

Le seguenti disposizioni valgono per tutti i dipendenti di Allianz Suisse Società di Assicurazioni SA, Allianz Suisse Società di Assicurazioni sulla Vita SA e delle sue affiliate (in particolare CAP Compagnia d'Assicurazione di Protezione giuridica SA, Società di Consulenza Previdenziale SA, Quality1 SA, AMOS IT Suisse SA e Allianz Suisse Immobiliare SA) nonché delle agenzie generali di Allianz Suisse.

1.2 Basi

Il presente regolamento si basa sulle disposizioni della Legge federale sulla protezione dei dati (LPD) e su quelle della direttiva del Gruppo Allianz "Allianz Standard for Data Protection and Privacy" (ASDP).

Sono fatte espressamente salve ulteriori disposizioni valide nei singoli reparti tecnici.

1.3 Ambito di applicazione

Scopo della protezione dei dati è proteggere la personalità e i diritti fondamentali delle persone i cui dati sono oggetto di trattamento.

Tutti i dipendenti sono tenuti a rispettare, nell'esercizio della propria attività, i principi e le norme in materia di protezione dei dati. I dirigenti sono tenuti a far rispettare le disposizioni in materia di protezione dei dati e a controllarne regolarmente l'osservanza nel loro ambito di responsabilità.

Le disposizioni valgono per il trattamento sia automatico che manuale dei dati di persone fisiche e giuridiche, a prescindere dal fatto che si tratti di dati memorizzati su supporto elettronico o cartaceo.

Le disposizioni riguardanti il trattamento riservato dei dati personali e commerciali devono essere rispettate anche dopo la cessazione del rapporto di lavoro.

1.4 Livelli di riservatezza

Dati pubblici (public)
Dati destinati e accessibili al pubblico.

Dati per uso interno (internal)
Dati destinati soltanto all'uso interno del Gruppo Allianz Suisse o delle società interessate e non destinati o accessibili al pubblico.

I dati privi di un'etichettatura specifica sono considerati "interni".

Dati confidenziali (confidential)
Dati a cui può accedere soltanto una ristretta cerchia di persone per l'espletamento delle proprie funzioni.

Dati strettamente confidenziali (strictly confidential)
Dati che, se resi accessibili a soggetti non autorizzati, potrebbero comportare gravi conseguenze per Allianz Suisse. Questi dati possono essere resi disponibili soltanto secondo criteri molto restrittivi a cerchie di persone o persone indicate per nome.

1.5 Classificazione dei dati

Gli Information owner competenti assegnano a tutti i dati disponibili in Allianz Suisse uno dei livelli di riservatezza indicati. Il livello di riservatezza assegnato vale anche per tutte le copie dei dati interessati indipendentemente dal supporto di memorizzazione e dal tipo di trattamento.

Di norma l'Information owner è il responsabile dell'unità nella quale la raccolta di dati è stata creata per la prima volta. Alle raccolte di dati composte da documenti di diverso tipo viene assegnato, secondo il principio di massimizzazione, il livello del documento con la classificazione più elevata. La classificazione dei singoli dati viene pubblicata ed è accessibile a tutti i dipendenti.

1.6 Dati personali

Sono considerati dati personali tutte le informazioni riferite a una persona fisica o giuridica identificata o identificabile.

La LPD definisce particolarmente sensibili (degni di particolare protezione) i dati concernenti le opinioni o attività religiose, filosofiche, politiche o sindacali, la salute, la sfera intima o l'appartenenza a una razza, le misure d'assistenza sociale nonché i procedimenti o le sanzioni amministrativi e penali.

I profili della personalità sono compilazioni di dati che permettono di valutare caratteristiche essenziali della personalità di una persona fisica.

Dati particolarmente sensibili e profili della personalità devono essere classificati obbligatoriamente come confidenziali, trattati secondo criteri particolarmente restrittivi e protetti con la massima riservatezza.

1.7 Principio di necessità (need-to-know)

A ciascun dipendente devono essere garantiti esclusivamente i diritti di accesso necessari per l'espletamento delle sue funzioni.

2 Disposizioni relative alla gestione dei dati

2.1 Raccolta di dati personali

- La rilevazione di dati personali è consentita solo per finalità legittime e 5inerenti al lavoro.

- La rilevazione di dati personali è consentita solo a condizione che la persona interessata ne sia a conoscenza e vi acconsenta oppure se è altrimenti autorizzata o prescritta per legge. Non è consentito acquisire dati personali da fonti terze (ad es. Internet o broker di dati) all'insaputa e senza autorizzazione degli interessati se tale operazione non è direttamente connessa alla stipula o alla gestione di un contratto e non sussiste nessun'altra motivazione sufficiente (v. punto 3).

- Il rilascio di un eventuale consenso deve essere facoltativo e la persona interessata deve aver ricevuto informazioni adeguate al riguardo; quest'ultima ha la facoltà di revocarlo.

- La raccolta dei dati e la sua finalità devono essere trasparenti per la persona interessata; sono consentite eccezioni solo se previste od autorizzate dalla legge (v. punto 3). La finalità della raccolta deve essere comunicata alla persona interessata o essere riconoscibile dalle circostanze.

- I dati raccolti o generati devono essere sempre corretti e completi in linea con la finalità perseguita. I dati errati devono essere rettificati o, se ciò non è possibile, distrutti, a condizione che essi non siano soggetti a obbligo di conservazione e che la loro distruzione non sia in contrasto con un interesse preponderante. In tal caso l'inesattezza dei dati deve essere contrassegnata ove possibile.

- Se la rilevazione di dati dà origine a una nuova raccolta di dati, questa deve essere notificata al responsabile della protezione dati interno. La nuova raccolta di dati deve essere inoltre assegnata a un Information owner che provvederà a classificarla secondo il grado di riservatezza (v. punto 1.4)

- I moduli per la rilevazione di dati e i siti Internet che servono a raccogliere dati devono contenere una clausola sulla protezione dei dati con le opportune informazioni circa lo scopo della rilevazione e il trattamento dei dati. La clausola sulla protezione dei dati va concordata con il responsabile della protezione dati interno.

2.2 Trattamento dei dati

- Di regola, i dati personali devono essere trattati esclusivamente per le finalità indicate all'atto della loro acquisizione. Il trattamento dei dati deve avvenire in maniera conforme alla legge, nel rispetto del principio della buona fede e di quello della proporzionalità.

- Conformemente al principio di necessità (v. punto 1.7), i dati devono essere resi accessibili solo ai dipendenti che ne hanno bisogno per motivi di lavoro. Essi devono essere protetti dall'accesso non autorizzato.

- I documenti di carattere riservato o contenenti dati personali devono essere custoditi sotto chiave quando si è assenti dalla propria postazione di lavoro.

- I documenti confidenziali e strettamente confidenziali ovvero i supporti che contengono dati di questo genere devono essere sempre opportunamente contrassegnati.

- Le informazioni personali possono essere comunicate solo alla persona interessata e di norma per scritto, dopo averne accertato l'identità. Le richieste di informazioni più generali che riguardano tutti i dati di una persona interessata devono essere inoltrate immediatamente al responsabile della protezione dati interno.

- Il trattamento di dati da parte di terzi e la trasmissione di dati a soggetti terzi sono consentiti solo dopo che il responsabile della protezione dati interno e/o l'Ufficio legale/Compliance abbiano verificato il rispetto delle disposizioni della LPD. A tal fine è di norma indispensabile stilare una clausola di riservatezza.

- È vietato memorizzare dati commerciali su memorie dati private o pubblicamente accessibili (p. es. Public Cloud, social media o spazi di archiviazione Internet come iCloud, Google Drive o Dropbox). L'utilizzo di altri servizi Cloud esterni è consentito solo con l'espressa autorizzazione del responsabile della protezione dati interno.

- La trasmissione di dati confidenziali tramite reti pubbliche deve avvenire di norma in modalità cifrata (è possibile cifrare il collegamento di rete oppure i dati stessi).

- Nella comunicazione orale di informazioni personali o confidenziali è necessario assicurarsi che queste non possano essere ascoltate da soggetti non autorizzati (vale in particolare per le conversazioni telefoniche in pubblico).

- La trasmissione di dati personali al di fuori della Svizzera richiede di regola la previa autorizzazione del responsabile della protezione dati interno, tranne se i dati sono inviati alla persona interessata stessa o se il processo di trasmissione è già stato autorizzato nel caso concreto. Lo stesso vale anche per l'inoltro di dati personali al Gruppo Allianz a Monaco e alle società del Gruppo Allianz.

- L'inoltro di dati confidenziali ovvero e-mail confidenziali è consentito di regola solo con il consenso dell'Information owner.

- I dati concernenti la previdenza professionale (LPP, assicurazione collettiva) e l'assicurazione infortuni obbligatoria nonché i dati relativi a sinistri dell'assicurazione di protezione giuridica sono soggetti per legge a un obbligo di riservatezza specifico e vanno pertanto trattati in modo confidenziale. La violazione degli obblighi di riservatezza previsti da norme specifiche può avere conseguenze penali.

2.3 Eliminazione dei dati

- I dati devono essere custoditi di regola solo per il periodo necessario alle finalità di trattamento e secondo i termini prescritti dalla legge o dai regolamenti.

- Tutti i documenti, gli appunti, le e-mail stampate, gli screenshot, ecc. in formato cartaceo vanno smaltiti senza alcuna eccezione utilizzando gli appositi container chiusi (Reisswolf) oppure distrutti mediante un distruggi documenti. I normali contenitori aperti per rifiuti cartacei possono essere utilizzati esclusivamente per lo smaltimento di giornali, cartone, materiale d'imballaggio, pubblicità, cataloghi e buste su cui non siano indicati mittenti privati.

  In caso di dubbi vanno utilizzati i container chiusi.

- Prima di smaltire un supporto dati elettronico sovrascrivibile (disco fisso, memory stick), i dati memorizzati devono essere cancellati in modo sicuro per impedirne il recupero mediante un processo di wiping (sovrascrizione dei dati) o tramite la distruzione fisica del supporto.

- I supporti dati che non possono essere sovrascritti come CD, DVD o altri supporti ottici, devono essere distrutti fisicamente (ad es. tagliati) prima di essere smaltiti.

3 Eccezioni

Eventuali eccezioni consentite sulla base delle disposizioni di cui sopra relative alla gestione dei dati devono essere sottoposte al responsabile protezione dati interno o all'Ufficio legale/Compliance, tranne il caso in cui il trattamento dei dati in questione sia esplicitamente autorizzato da un altro regolamento anche per quanto riguarda la protezione dei dati. In caso di dubbio devono essere consultate le due istanze menzionate.

4 Violazioni delle disposizioni sulla protezione dei dati

Tutte le violazioni della Legge sulla protezione dei dati o delle disposizioni del presente regolamento, in particolare perdite e rivelazioni di dati involontarie, devono essere immediatamente segnalate al responsabile della protezione dati interno.

Il rispetto delle disposizioni in materia di protezione dei dati viene controllato regolarmente dal responsabile della protezione dati interno ed eventualmente da altre persone. La mancata osservanza delle disposizioni può comportare per i singoli collaboratori sanzioni disciplinari o avere persino conseguenze penali.

5 Disposizioni sulla gestione dei dati in base alla loro classificazione

La tabella seguente riporta in sintesi le regole principali per gestire i dati a seconda del loro livello di riservatezza.

	Dati pubblici	Dati interni	Dati confidenziali	Dati strettamente confidenziali
Esempi di dati per livello di riservatezza	• Documenti pubblicitari, opuscoli • Descrizioni di prodotti • Relazioni di esercizio • Statuti • Comunicati stampa • Schede informative	• Dati di base dei clienti (nome, indirizzo, data di nascita, ecc.) • Proposte e polizze assicurative • Direttive e regolamenti • Organigrammi • Job description • Dati relativi a progetti	• Dati sulla salute, referti medici • Dati retributivi • Dati personali • Dati relativi ad esecuzioni • Verbali del comitato direttivo e del consiglio di amministrazione • Contratti con broker e partner convenzionati	• Dati relativi a pianificazione e strategia aziendali • Password
Etichettatura documenti	"Public" sul frontespizio, se opportuno	I dati non etichettati sono considerati "interni".	"Confidential" sul frontespizio o a piè di pagina Deve essere indicato l'Information owner/l'autore.	"Strictly confidential" sul frontespizio o a piè di pagina Deve essere indicato l'Information owner/l'autore.
Destinatari	Chiunque	Tutto il personale del Gruppo Allianz Suisse secondo il principio di necessità	Cerchia di persone limitata in base al principio di necessità	Cerchia di persone limitata; i nomi devono essere indicati nel documento
Invio postale	Nessun requisito particolare	**Posta interna:** nessun requisito particolare **Posta per l'esterno**: in busta chiusa	**Posta interna e per l'esterno:** in busta chiusa con annotazione "personale"	Consentito solo previo consenso dell'Information owner **Posta interna:** in busta chiusa con annotazione "strettamente confidenziale" Se possibile il documento va recapitato personalmente. **Posta per l'esterno:** in busta chiusa con annotazione "personale"
Trasmissione via fax	Nessun requisito particolare	Nessun requisito particolare	Deve essere ricevuto personalmente dal destinatario.	Non ammessa

	Dati pubblici	Dati interni	Dati confidenziali	Dati strettamente confidenziali
Stampa	Nessun requisito particolare	Nessun requisito particolare	Le stampe vanno immediatamente rimosse dalla stampante.	Stampa solo previo consenso dell'Information owner; le stampe vanno immediatamente rimosse dalla stampante.
Invio per e-mail	Nessun requisito particolare	**Invio interno:** selezione degli indirizzi e-mail tramite la rubrica Allianz **Invio esterno:** cifratura necessaria per l'invio di dati personali a terzi[1]	- cifratura - etichettatura come "confidential" - inoltro di e-mail riservate solo previo consenso dell'Information owner	**Invio interno:** - cifratura - etichettatura come "strictly confidential" - inoltro di e-mail riservate solo previo consenso dell'Information owner **Invio esterno:** non consentito
Trasmissione via FTP	Nessun requisito particolare	Solo tramite un account specifico riservato al destinatario Necessaria cifratura (collegamento o dati)	Consentito solo previo consenso dell'Information owner Solo tramite un account specifico riservato al destinatario Necessaria cifratura (collegamento o dati)	Non consentita
Duplicati (es. copie)	Nessun requisito particolare	Nessun requisito particolare	Consentito solo previo consenso dell'Information owner	Consentito solo previo consenso dell'Information owner
Archiviazione elettronica	Nessun requisito particolare	Applicazione del principio di necessità La memorizzazione di dati su supporti mobili è consentita solo in modalità cifrata e previo consenso dell'Information owner.	Cifrare i dati sui supporti Allianz non mobili ogni volta che è possibile. La memorizzazione di dati su supporti mobili è consentita solo in modalità cifrata e previo consenso dell'Information owner. Etichettare i supporti dati come "confidential".	Cifratura obbligatoria Non è consentita la memorizzazione su supporti mobili (eccezione: notebook Allianz cifrati).

[1] Non sono soggette a cifratura obbligatoria:
- le e-mail dal cui contenuto risulti impossibile risalire a una persona fisica o giuridica determinata o determinabile (ad es. non sono riportati dati personali o i dati sono stati anonimizzati);
- le e-mail per le quali gli interessati abbiano espresso il proprio consenso a trasmettere dati per via diretta e senza cifratura.

	Dati pubblici	Dati interni	Dati confidenziali	Dati strettamente confidenziali
Archiviazione fisica	Nessun requisito particolare	Durante l'assenza dalla postazione di lavoro, custodire documenti e supporti dati sotto chiave.	Durante l'assenza dalla postazione di lavoro, custodire documenti e supporti dati sotto chiave. Custodire i documenti confidenziali all'interno di un raccoglitore in busta chiusa separata.	Custodire sempre sotto chiave i documenti non in uso.
Inoltro	Nessun requisito particolare	Inoltro interno secondo il principio di necessità Inoltro a soggetti esterni solo previo consenso dell'Information owner Informazioni alla persona interessata solo dopo accertamento dell'identità Richieste di informazioni e di consultazione come anche altre richieste che riguardano i dati di una persona interessata da parte della stessa sono trattate dal responsabile della protezione dati interno.	Inoltro solo previo consenso dell'Information owner Informazioni alla persona interessata solo dopo accertamento dell'identità Richieste di informazioni e di consultazione come anche altre richieste che riguardano i dati di una persona interessata da parte della stessa sono trattate dal responsabile della protezione dati interno.	Inoltro di norma direttamente a cura dell'Information owner o solo su suo incarico
Social media (Facebook, Twitter, blog, ecc.)	Nessun requisito particolare	Non sono consentiti il caricamento di dati (upload) e la comunicazione di informazioni interne.	Non sono consentiti il caricamento di dati (upload) e la comunicazione di informazioni confidenziali.	Non sono consentiti il caricamento di dati (upload) e la comunicazione di informazioni strettamente confidenziali.
Perdita/fuga di dati, dati compromettenti	Nessun requisito particolare	Segnalazione immediata all'Information owner e al responsabile della protezione dati interno	Segnalazione immediata all'Information owner e al responsabile della protezione dati interno	Segnalazione immediata all'Information owner e al responsabile della protezione dati interno

6 Entrata in vigore

Il presente "Regolamento sulla protezione e la sicurezza dei dati" entra in vigore il 1° gennaio 2016 e sostituisce la versione del 1° gennaio 2008.