Direttive per la protezione dei dati CNA Svizzera

Data: del 1° marzo 2019 (stato al 1° settembre 2023)

Contenuto

Preambolo

Dal 25 maggio 2018 è in vigore il regolamento generale sulla protezione dei dati europeo Regolamento generale sulla protezione dei dati (RGPD). Esso è applicabile principalmente negli Stati dell'Unione Europea e dello Spazio Economico Europeo. In taluni casi trova applicazione anche per Stati terzi come la Svizzera. La CNA Svizzera, quale associazione secondo il diritto svizzero, soggiace in prima linea al diritto svizzero e di conseguenza alla legge svizzera sulla protezione dei dati (LPD). Questa legge è stata interamente rivista con effetto a decorrere dal 1° settembre 2023. Dal punto di vista del contenuto, integra in gran parte il RGPD. Pertanto, data la stretta connessione della CNA Svizzera con l'Europa e la sempre più ampia accettazione a livello mondiale nonché la diffusione dei contenuti del RGPD, le attuali direttive per la protezione dei dati traggono ispirazione dal RGPD. Le importanti peculiarità svizzere sono conseguentemente integrate.

Il RGPD e la LPD non costituiscono di per sé una novità assoluta. In effetti, già la precedente LPD stabiliva in maniera relativamente concreta a quali condizioni si potessero rilevare e trattare quali dati e a quali scopi. Il RGPD, come pure l'attuale LPD, hanno acuito queste regole e obbligano i responsabili (ogni persona fisica e/o organizzazione che rileva e tratta i dati) a una documentazione maggiormente trasparente e comprensibile dei dati raccolti. Il principio più importante è la minimizzazione dei dati, ossia raccogliere soltanto quei dati che sono necessari per una finalità lecita e ricancellarli il prima possibile. Quindi, per tutti coloro che raccolgono e trattano i dati significa occuparsi approfonditamente con le proprie azioni e i propri processi di lavoro, eventualmente adattandoli alla nuova situazione. In effetti, non esistono modelli universalmente validi che possano essere implementati senza alcun intervento.

§ 1 Significato, finalità, accessibilità

(1) Le presenti direttive per la protezione dei dati costituiscono la base vincolante per una protezione giuridicamente conforme e sostenibile dei dati riferiti alla persona («dati personali») della Chiesa Neo-Apostolica Svizzera (di seguito denominata «CNA Svizzera» o «la responsabile». Esse rappresentano il fondamento per tutti i documenti di attuazione come p.es. «Le istruzioni per ministri».

(2) Le Direttive per la protezione dei dati devono essere in ogni momento facilmente accessibili per tutti i ministri, i funzionari e tutto il personale dell'Amministrazione della CNA Svizzera. Pertanto, esse vengono pubblicate sia su cna-interno sia sul sito web della CNA Svizzera.

§ 2 Ambito d'applicazione

(1) Le presenti direttive per la protezione dei dati sono applicabili nell'area della CNA Svizzera. Per le comunità ecclesiali nel comprensorio della CNA Svizzera sono particolarmente rilevanti le istruzioni sulla «Protezione dei dati nella vita quotidiana della comunità».

(2) Le presenti direttive valgono personalmente per tutte le persone che sono in un rapporto di servizio onorifico, a tempo parziale o a tempo pieno, o in un rapporto d'altro genere con la CNA Svizzera (per es. l'incarico quale conducente di comunità) oppure con i suoi organismi o le sue istituzioni. Valgono anche per tutti i ministri e le ministre della Chiesa Neo-Apostolica (in merito vedi anche Catechismo, cap. 7.1 Il ministero e i servizi). Altresì sono valevoli per le persone che sono in un qualsiasi rapporto d'incarico e di servizio con la CNA Svizzera.

(3) Le prescrizioni e i divieti delle presenti direttive per la protezione dei dati si applicano a ogni genere di trattamento di dati personali, sia esso elettronico, cartaceo o verbale. Si applicano inoltre a tutti i tipi di

persone interessate (p.es. una sorella o un fratello, un ministro o una ministra, un collaboratore o una collaboratrice dell'Amministrazione della CNA Svizzera, ecc.).

§ 3 Definizione dei termini

(1) *Dato personale (CH: dati personali)*[1] è qualsiasi informazione riguardante una persona fisica (persona interessata) o identificabile. I dati dei fedeli fanno pure parte dei dati riferiti alla persona tanto quanto i dati personali e i dati dei ministri e delle ministri e delle persone con funzioni. Per esempio, il nome di un interlocutore permette di trarre conclusioni in riguardo a una persona fisica nello stesso modo come il suo indirizzo e-mail. È sufficiente che la rispettiva informazione sia collegata al nome della persona interessata o che, indipendentemente da ciò, possa essere dedotta dal contesto. Allo stesso modo, una persona può essere identificabile anche se l'informazione deve essere inizialmente collegata a una conoscenza aggiuntiva quale, p. es., la data di nascita, il numero personale o l'indirizzo IP. La provenienza delle informazioni non è rilevante per stabilire un riferimento alla persona. Anche fotografie, riprese video e audio possono rappresentare dei dati personali.

(2) *Categorie particolari di dati personali (CH: dati personali degni di particolare protezione)* sono informazioni dalle quali possono risultare l'origine razziale o etnica, le opinioni politiche, le convinzioni religiose o ideologiche, nonché un'eventuale appartenenza a sindacati, come pure dati genetici o biometrici che identificano chiaramente una persona fisica, dati riguardanti lo stato di salute o la vita sessuale, rispettivamente l'orientamento sessuale di una persona fisica e dati su misure dell'assistenza sociale o dati sui procedimenti o sanzioni amministrativi e penali.

(3) *Trattamento* è qualsiasi operazione o insieme di operazioni, compiute con o senza l'ausilio di processi automatizzati e applicate a dati personali, segnatamente la raccolta, la registrazione, l'organizzazione, la strutturazione, la conservazione, l'adattamento o la modificazione, l'estrazione, la consultazione, l'utilizzazione, la comunicazione mediante trasmissione, diffusione o qualsiasi altra forma di messa a disposizione, il raffronto o l'interconnessione, la limitazione, la cancellazione o la distruzione.

(4) *Limitazione di trattamento* è il contrassegno dei dati personali conservati con l'obiettivo di limitarne il trattamento in futuro.

(5) *Profilazione* o *Profilazione* a rischio elevato: dato che la CNA Svizzera, in quanto organizzazione responsabile, si astiene da qualsiasi tipo di profilazione, entrambi i termini non saranno spiegati ulteriormente in questa sede.

(6) *Anominizzazione / Pseudonimizzazione:* i dati personali si ritengono *anominizzati* quando non è più possibile identificare la persona a cui si riferiscono. L'«*anominizzazione*» è il processo mediante il quale si impedisce che i dati siano collegati a una persona specifica o che tale collegamento sia possibile solo tramite misure straordinarie. Nella *«pseudonimizzazione»*, invece, tutti i dati identificabili sono sostituiti con un identificativo neutro (pseudonimo). La pseudonimizzazione è reversibile (purché esista e sia accessibile una tabella di corrispondenza che consenta di collegare i dati pseudonimizzati alla persona originale). L'anonimizzazione, invece, è definitiva. Soltanto i dati completamente anonimizzati non valgono più come dati personali e pertanto non soggiacciono più alla legge sulla protezione dei dati.

[1] in inglese: «personal data» o «personal information».

(7) Il *titolare* è la persona fisica o giuridica (nel caso specifico, il titolare è unicamente la CNA Svizzera), l'autorità pubblica, il servizio o altro organismo che, singolarmente o insieme ad altri, determina le finalità e i mezzi del trattamento di dati personali.

(8) *Responsabile del trattamento* è la persona fisica o giuridica (per es. la ditta incaricata della manutenzione tecnologica dell'Amministrazione dati membri/ADM nel portale della CNA[2]), l'autorità pubblica, il servizio o altro organismo che tratta i dati personali per conto del titolare del trattamento.

(9) *Destinatario* è la persona fisica o giuridica, l'autorità pubblica, il servizio o un altro organismo che riceve comunicazione di dati personali, che si tratti o meno di terzi.

(10) *Terzo* è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che non sia l'interessato, il titolare del trattamento, il responsabile del trattamento e le persone autorizzate al trattamento dei dati personali sotto l'autorità diretta del titolare o del responsabile.

(11) Un *consenso* dell'interessato (CH: consenso della persona interessata) è qualsiasi manifestazione di volontà libera, specifica, informata e inequivocabile dell'interessato, con il quale lo stesso manifesta il proprio assenso, mediante dichiarazione o azione positiva inequivocabile, che i dati personali che lo riguardano siano oggetto di trattamento.

§ 4 Organizzazione della protezione dei dati

(1) La CNA Svizzera ha designato una persona incaricata per la protezione dei dati (*CH: Consulente per la protezione dei dati*)[3]. Essa è raggiungibile medianti i seguenti dati di contatto:

Chiesa Neo-Apostolica Svizzera
Incaricato per la protezione dei dati
Ueberlandstrasse 243
8051 Zurigo
Svizzera

E-mail: privacy@nak.ch

(2) L'incaricato per la protezione dei dati sorveglia il rispetto della Legge federale sulla protezione dei dati (LPD) e del Regolamento europeo per la protezione dei dati (RGPD), nonché di altre disposizioni legali, comprese le prescrizioni di queste e altre direttive della CNA Svizzera in merito alla protezione dei dati. L'incaricato per la protezione dei dati consiglia e informa il direttore dell'Amministrazione dell'AaApd Svizzera [4] per quanto riguarda i doveri vigenti in materia di protezione dei dati ed è responsabile della comunicazione con l'Incaricato federale della protezione dei dati e della trasparenza (IFPDT). Egli controllerà i processi selezionati in modo campionario, orientato al rischio e a intervalli di tempo adeguati per verificarne la conformità alle disposizioni sulla protezione dei dati.

(3) L'incaricato per la protezione dei dati svolge i suoi compiti in modo indipendente e utilizzando la sua competenza professionale. Riferisce direttamente al direttore dell'Amministrazione dell'AaApd Svizzera.

[2] ADM = Amministrazione dati membri (l'ADM è parte del portale della CNA).
[3] Per semplicità, in questo contesto, verrà utilizzata esclusivamente la forma maschile, in conformità con la denominazione nella RGPD (Regolamento Generale sulla Protezione dei Dati).
[4] AaApd Svizzera = Area di attività dell'apostolo di distretto della Svizzera

(4) Il direttore dell'Amministrazione dell'AaApd Svizzera e i collaboratori e le collaboratrici dell'Amministrazione della CNA Svizzera devono sostenere l'incaricato per la protezione dei dati nell'adempimento dei suoi compiti.

§ 5 Utilizzo di dati personali

(1) Nel trattamento di dati personali occorre osservare i principi della Legge sulla protezione dei dati: liceità, principio della buona fede e della proporzionalità, trasparenza, pertinenza alla finalità, minimizzazione dei dati, esattezza dei dati personali, limitazione della conservazione («diritto all'oblìo»), integrità, riservatezza e disponibilità («sicurezza dell'informazione» o «sicurezza dei dati») e responsabilizzazione.

(2) In linea di principio il trattamento di dati personali può avvenire nel seguente modo (lista esemplificativa):

- la persona interessata o i titolari della responsabilità genitoriale o della tutela hanno acconsentito al trattamento dei dati,
- i dati sono necessari per preparare o adempiere a un contratto con la persona interessata (p. es. un contratto di adesione, un contratto di lavoro o un contratto di servizio),
- una legge statale ha imposto un obbligo in tal senso (p.es obblighi di conservazione previsti dalla legge),
- esiste un interesse ecclesiastico o di altra natura e gli interessi, le libertà fondamentali o i diritti fondamentali delle persone interessate non prevalgono (p. es., l'interesse nell'archiviare documenti di importanza storica per la chiesa o l'interesse nell'informare i membri o nell'utilizzare l'indirizzo postale di ex membri di una comunità ecclesiale per inviti a un evento di anniversario),
- interessi vitali della persona interessata o di terzi lo richiedono (p.es la divulgazione di dati di contatto nel contesto di un'emergenza medica).

(3) In deroga al paragrafo (2) tutti i ministri possono prendere degli appunti («note personali») ai fini del loro mandato di cura pastorale. Tuttavia, ciò deve essere limitato ai membri della Chiesa di cui si occupano personalmente nell'ambito del loro mandato pastorale. Il contenuto di queste note deve avere un collegamento diretto con l'attività pastorale. Tali note non devono essere accessibili a nessuno. In merito, i ministri interessati devono adottare misure tecniche o organizzative adeguate per proteggere questi dati.

(4) Il cambiamento della destinazione e finalità su cui si basava originariamente l'uso dei dati è ammissibile – oltre a un consenso esplicito della persona interessata– soltanto se la finalità del trattamento successivo è compatibile con la finalità originaria (per es., nel passaggio da un livello d'insegnamento a un altro). In questo contesto, è particolarmente importante considerare le aspettative ragionevoli della persona interessata riguardo a tale ulteriore trattamento da parte della CNA Svizzera, il tipo dei dati utilizzati, le conseguenze per la persona interessata e le possibilità di cifratura o pseudonimizzazione.

(5) La persona interessata deve essere completamente informata durante la raccolta dei suoi dati personali riguardo al trattamento dei suoi dati. L'informazione deve includere la finalità del trattamento, l'identità del titolare del trattamento, i destinatari dei suoi dati personali, nonché qualsiasi altra informazione ai sensi dell'Art. 19 della Legge svizzera sulla protezione dei dati (basato sulla base giuridica del RGPD: Art. 13 del RGPD), al fine di garantire un trattamento equo e trasparente. Le informazioni devono essere scritte in forma comprensibile e facilmente accessibile e nel linguaggio più semplice possibile.

(6) I dati personali devono essere oggettivamente esatti e, se necessario, aggiornati. L'estensione del trattamento dei dati dovrebbe essere pertinente alla necessità e rilevante in riguardo alle finalità predefinite. L'Amministrazione della CNA deve prevedere in merito gli adeguati processi. È autorizzata a farlo dal Presidente della Chiesa. Allo stesso modo, le banche dati sono da controllare regolarmente relativamente alla loro esattezza, necessità e attualità.

§ 6 Categorie particolari di dati personali

(1) Per principio, le categorie particolari di dati personali possono essere raccolte, trattate o utilizzate soltanto con il consenso della persona interessata o, eccezionalmente, sulla base di un'esplicita autorizzazione legale. Inoltre, devono essere adottate misure tecniche e organizzative aggiuntive (come la cifratura durante il trasporto, l'assegnazione minima di diritti) per proteggere tali dati.

§ 7 Trasferimento di dati

(1) Il trasferimento a terzi di dati personali è ammesso soltanto in base a un'autorizzazione legale oppure con il consenso della persona interessata.

(2) Se il destinatario dei dati personali si trova fuori dell'Unione Europea o dello spazio economico europeo, occorrono misure particolari per il rispetto dei diritti e degli interessi delle persone interessate. Il trasferimento di dati deve essere evitato se il livello di protezione dei dati presso il destinatario non è adeguato o se non può essere garantito tramite adeguate misure di protezione, come un accordo contrattuale (in particolare, le clausole contrattuali standard dell'UE).

§ 8 Fornitori di servizi esterni

(1) Se i fornitori di servizi esterni (p. es. fornitori di servizi IT, fornitori di servizi di archiviazione o distruzione di documenti) devono ottenere l'accesso a dati personali, l'incaricato per la protezione dei dati deve esserne informato preventivamente.

(2) I fornitori di servizi esterni che potrebbero accedere a dati personali devono essere selezionati con attenzione prima di assegnare loro l'incarico. La scelta deve essere documentata e considerare soprattutto i seguenti aspetti:

- idoneità professionale del fornitore di servizi esterni per l'utilizzo concreto dei dati,
- misure di sicurezza tecniche e organizzative,
- esperienza dell'offerente sul mercato,
- altri aspetti che permettono di presumere l'affidabilità del fornitore di servizio esterno (documentazioni sulla protezione dei dati, disponibilità alla cooperazione, tempi di reazione, ecc.).

(3) Se un fornitore di servizi esterno deve raccogliere, elaborare o utilizzare i dati personali per conto della Chiesa, è necessario stipulare un accordo sul trattamento dei dati («DPA[5]»). Questo accordo deve disciplinare gli aspetti legati alla protezione dei dati e alla sicurezza informatica. Inoltre, tutti i fornitori di servizi esterni saranno vincolati per iscritto alla riservatezza.

(4) I fornitori di servizi esterni devono essere soggetti a revisioni periodiche riguardo alle misure tecniche e organizzative concordate contrattualmente («TOM»). Il risultato è da documentare.

§ 9 Conservazione, archiviazione e cancellazione

(1) Vale il principio: dati personali che non sono più necessari e non sono degni di archiviazione devono essere cancellati, rispettivamente distrutti definitivamente (per esempio nel distruggidocumenti).

(2) I dati personali devono essere cancellati quando la loro conservazione è illegittima, il consenso per la conservazione è stato revocato o non sono più necessari per le finalità per cui sono stati raccolti.

(3) Eccezioni sono:

- dati personali resi anonimi
- obblighi legali di conservazione dei documenti
- dati personali che sono stati raccolti nell'ambito di un atto sacro irrevocabile e non ripetibile, come il Battesimo o il Suggello, oppure che occorrono per eventuali futuri atti ecclesiastici, come per es. il matrimonio o il funerale (per es. certificato di Battesimo, certificato di Suggello)
- dati personali che devono essere conservati per scopi di prova o di sicurezza, oppure per la tutela degli interessi legittimi della persona fisica
- legittimo interesse della Chiesa nell'archiviazione di documenti di importanza storica per la chiesa.

(4) I dettagli devono essere regolati in un concetto di cancellazione e archiviazione (compresa la sicurezza dei dati).

[5] DPA: Data Processing Agreement

§ 10 Minimizzazione, Privacy by Design/Privacy by Default

(1) L'uso di dati personali deve essere orientato all'obiettivo di raccogliere, trattare o utilizzare il minor numero possibile di dati da parte di una persona interessata (principio della «minimizzazione dei dati»). In particolare, i dati personali devono essere anonimizzati o pseudonimizzati, nella misura in cui ciò sia possibile in base alla finalità dell'utilizzo. Per esempio, nell'ambito di un'analisi statistica dei dati, non sarà necessario conoscere e utilizzare il nome completo di una persona interessata. Piuttosto, questa informazione potrà essere sostituita con un dato scelto a caso, il quale può anch'esso garantire la differenziabilità delle informazioni esaminate.

(2) Considerazioni analoghe valgono per la scelta e la messa in opera di sistemi di gestione di dati (per es. l'ADM nel portale della CNA). La protezione dei dati deve essere integrata fin dall'inizio nelle specifiche e nell'architettura dei sistemi di elaborazione dati al fine di agevolare il rispetto dei princìpi di protezione della sfera privata (privacy) e della protezione dei dati, in particolare il principio di minimizzazione dei dati.

§ 11 Diritti delle persone interessate

(1) L'esercizio dei diritti sottostanti, come per es. la condivisione di informazioni, deve riferirsi alla persona esatta. Pertanto, **l'autorizzazione del richiedente e la sua identità devono essere accertati in anticipo e al di là di ogni dubbio**.

(2) La persona interessata ha il **diritto d'accesso** in merito a tutti i dati personali che sono memorizzati e/o trattati nei suoi riguardi.

(3) In linea di principio, le informazioni vengono comunicate per iscritto, a meno che la persona interessata non abbia presentato la richiesta d'accesso in forma elettronica. Le informazioni devono essere comunicate entro 30 giorni dal ricevimento della richiesta di informazioni. La CNA Svizzera comunica alla persona interessata in particolare le seguenti informazioni (cfr. Art. 25 cpv. 2 LPD): tutti i dati esistenti che la riguardano, incluse le informazioni disponibili sulla provenienza dei dati; le finalità ed eventualmente le basi legali del trattamento nonché le categorie dei dati personali trattati, coloro che si occupano del trattamento dei dati ed eventuali destinatari dei dati.

(4) Le persone interessate hanno **diritto di rettifica** dei propri dati personali qualora risultino inesatti. Nel contempo possono richiedere il completamento di dati personali incompleti.

(5) La persona interessata ha il **diritto alla cancellazione** dei propri dati personali alle seguenti condizioni:

- la conoscenza dei dati personali non è più necessaria per soddisfare lo scopo per cui sono stati memorizzati,
- la persona interessata ha revocato il consenso e non sussiste altro fondamento giuridico per il trattamento,
- il loro trattamento è illecito,
- la persona interessata si oppone o invoca un diritto di opposizione basato su una situazione personale particolare - da motivare,
- si tratta di dati personali particolari la cui esattezza non può essere comprovata oppure
- esiste un altro obbligo legale per la cancellazione dei dati.

Qualora sussista l'obbligo di cancellazione e i dati personali siano stati precedentemente resi pubblici, è necessario informare altri responsabili del trattamento dei dati riguardo alla richiesta di cancellazione da parte della persona interessata in relazione a tutte le copie dei suoi dati come pure a tutti i link riferiti a tali dati.

(6) La persona interessata può esigere una **limitazione del trattamento** dei propri dati, se

- l'esattezza dei suoi dati personali è contestata (p. es., nome registrato in modo errato dopo il matrimonio). Tuttavia, questa limitazione del trattamento si applica solo fino a quando l'unità organizzativa di competenza (p.es. l'Amministrazione della CNA Svizzera o la comunità ecclesiale a cui appartiene la persona interessata) non ne abbia chiarito l'esattezza oppure
- il trattamento è illecito, ma la persona interessata rifiuta la cancellazione dei dati oppure
- la CNA Svizzera non necessita più dei dati personali per le finalità del trattamento, ma la persona interessata li richiede per far valere, esercitare o difendere i propri diritti legali, oppure
- la persona interessata ha presentato opposizione al trattamento a causa di una situazione particolare e l'unità organizzativa competente (p. es., l'Amministrazione della CNA Svizzera o la comunità ecclesiale a cui la persona interessata appartiene) è ancora intenta a esaminare l'opposizione.

(7) **Altri diritti sanciti dalla legge sono**: diritto a una menzione che indichi il carattere contestato dei dati personali; diritto di revoca e opposizione; diritto di divulgazione e trasferimento dei dati.

(8) La persona deve essere informata entro un mese su tutte le misure adottate in risposta alla sua richiesta.

(9) L'incaricato per la protezione dei dati è a disposizione come consulente per garantire i diritti delle persone interessate.

§ 12 Richieste di informazioni da parte di terzi su persone interessate

(1) In linea di principio, la CNA Svizzera non divulga alcun dato personale a terzi. Qualora un ente dovesse richiedere informazioni su persone interessate, per esempio un'autorità o un'istituzione sociale, la divulgazione di informazioni è consentita solo se

- la parte richiedente informazioni può dimostrare un interesse legittimo a tale scopo e
- esiste una norma di legge che obbliga a fornire le informazioni, nonché
- l'identità del richiedente o della parte richiedente è chiaramente stabilita.

§ 13 Registro delle attività di trattamento

(1) La CNA Svizzera mantiene un registro di tutte le operazioni di trattamento dati e delle persone responsabili di tali operazioni di trattamento. L'incaricato per la protezione dei dati può essere coinvolto per fornire consulenza su informazioni richieste dalla legge.

(2) Su richiesta, la CNA Svizzera mette il registro a disposizione dell'autorità competente per la protezione dei dati. Ne è responsabile l'incaricato per la protezione dei dati in accordo con il direttore amministrativo dell'ara di attività del distretto apostolico Svizzera.

§ 14 Formazione

(1) Le persone che hanno accesso costante o regolare a dati personali della CNA Svizzera, che raccolgono tali dati o sviluppano sistemi per il trattamento di questi dati, devono essere adeguatamente istruite sulle norme legali in materia di protezione dei dati. L'incaricato per la protezione dei dati decide, d'intesa con il direttore amministrativo dell'AaApd Svizzera, la forma e la frequenza dei relativi corsi di formazione.

§ 15 Segreto dei dati, segreto pastorale e segreto ministeriale

(1) Alle persone che lavorano per l'Amministrazione della CNA Svizzera è vietato raccogliere, trattare o utilizzare dati personali in modo non autorizzato. Prima di iniziare la loro attività, sono tenute a trattare i dati personali in modo confidenziale (sottoscrivendo una dichiarazione di riservatezza).

(2) Le persone con obblighi di riservatezza particolari (p. es., i responsabili ADM) sono inoltre tenute a impegnarsi per iscritto in tal senso.

(3) Le annotazioni («note personali») redatti nell'esercizio di un mandato pastorale ecclesiastico non devono essere accessibili a terze persone. Le particolari norme sulla protezione del segreto pastorale rimangono intatte. Lo stesso vale per tutti gli altri obblighi di segretezza al fine di rispettare gli obblighi legali di segretezza e riservatezza, o segreti professionali o speciali segreti ministeriali che non si basano su disposizioni di legge.

(4) Questi obblighi di riservatezza sono illimitati nel tempo. Essi si applicano anche alle informazioni scambiate o rese accessibili prima dell'eventuale sottoscrizione di una dichiarazione di riservatezza. Sono irrevocabili e rimangono in vigore anche dopo la cessazione della collaborazione, del rapporto contrattuale o dell'adempimento dei servizi concordati, nonché dopo la conclusione di un rapporto di lavoro o incarico/mandato.

§ 16 Reclami

(1) Ogni persona interessata ha il diritto di presentare un reclamo in merito al trattamento dei propri dati qualora ritenga che i propri diritti siano stati violati.

(2) L'organo competente per i suddetti reclami è l'incaricato per la protezione dei dati, in quanto autorità interna, indipendente e libera da direttive.

§ 17 Audit

(1) Al fine di garantire un elevato livello di protezione dei dati, i processi rilevanti possono essere sottoposti a audit regolari da parte di enti interni o da parte di auditor esterni. Nel caso si stabilisca un potenziale di miglioramento occorre adottare misure correttive immediate.

(2) Le conoscenze rilevate nell'audit sono da documentare. La documentazione deve essere consegnata all'incaricato per la protezione dei dati, al direttore amministrativo dell'AaApd Svizzera e ai responsabili specialistici del processo corrispondente.

(3) Un audit è considerato completato con successo quando tutte le misure documentate nel rapporto sono state attuate. Se necessario, vengono condotti audit di follow-up, in cui le raccomandazioni dell'audit iniziale vengono sottoposte a verifica per quanto riguarda la loro implementazione.

§ 18 Inchieste interne

(1) Le misure volte a chiarire i fatti e evitare o scoprire reati o gravi violazioni dei doveri devono essere eseguite nel rigoroso rispetto delle norme di legge in materia di protezione dei dati. In particolare, la raccolta e l'utilizzo dei dati associati a tale scopo investigativo devono essere necessari, appropriati e proporzionati, tenendo in debito conto gli interessi legittimi della persona interessata.

(2) La persona interessata sarà informata quanto prima delle misure adottate nei suoi confronti.

(3) In tutte le forme di indagine interna, l'incaricato per la protezione dei dati deve essere preventivamente coinvolto nella selezione e nella progettazione delle misure.

§ 19 Disponibilità, confidenzialità, integrità e tracciabilità dei dati

(1) In base al tipo, all'entità, alle circostanze e alle finalità del trattamento, nonché alla probabilità dell'evento, per ogni procedura (p. es. lo sviluppo di una nuova banca dati contenente dati personali dei membri della chiesa) deve essere effettuata un'analisi documentata delle necessità di protezione e una valutazione dei rischi per le persone interessate.

(2) Per garantire la disponibilità, la confidenzialità, l'integrità e la tracciabilità dei dati (sicurezza delle informazioni o sicurezza dei dati), viene elaborato un concetto di sicurezza generale in base alla valutazione delle necessità di protezione e all'analisi dei rischi, vincolante per tutte le procedure. In partico-

lare, si deve tenere conto dello stato dell'arte, degli strumenti e delle misure di cifratura e di protezione dei dati. Il concetto di sicurezza deve essere regolarmente rivisto, esaminato e valutato in relazione all'efficacia delle misure tecniche e organizzative ivi previste.

(3) Affinché i sistemi di trattamento dei dati siano protetti da utilizzi non autorizzati, è necessario assicurare che le persone non autorizzate non possano accedervi. Le porte degli spazio non occupati devono essere chiuse a chiave, mentre è fondamentale implementare e attivare misure efficaci per controllare l'accesso ai dispositivi. L'accesso al sistema deve rimanere bloccato in assenza di persone autorizzate, garantendo così un elevato livello di sicurezza.

(4) Le password consentono l'accesso ai sistemi e ai dati personali in essi memorizzati. Rappresentano un'identificazione personale dell'utente e non sono trasferibili. Assicurarsi che le password siano sempre tenute sotto chiave. Le password devono avere una lunghezza minima di otto caratteri e devono essere composte da una combinazione di caratteri (lettere maiuscole, lettere minuscole, numeri e caratteri speciali). Le password non devono comparire in un dizionario né essere costituite da termini facilmente intuibili, in particolare non devono includere parole correlate alla CNA Svizzera.

(5) L'accesso ai dati personali dovrebbe essere consentito solo alle persone che, nell'esercizio dei loro compiti, hanno bisogno di conoscere tali dati (principio del «need-to-know»). Le autorizzazioni di accesso devono essere definite e documentate in modo preciso e completo.

(6) I trasferimenti di dati attraverso reti pubbliche devono essere possibilmente cifrati. La cifratura diventa obbligatoria se il livello di protezione dei dati personali lo richiede.

(7) Gli interventi di manutenzione sui sistemi o sulle apparecchiature di telecomunicazione da parte di fornitori di servizi esterni devono essere supervisionati. Inoltre, è necessario garantire che i fornitori di servizi non possano accedere ai dati personali in modo non autorizzato. L'accesso remoto per la manutenzione deve essere concesso solo in casi specifici e seguire il principio dell'attribuzione dei diritti minimi. Le attività di manutenzione da remoto devono essere possibilmente registrate o protocollate.

§ 20 Valutazione d'impatto sulla protezione dei dati

(1) La CNA Svizzera elabora preventivamente una valutazione d'impatto sulla protezione dei dati per il trattamento dei dati che potrebbe comportare un elevato rischio per la personalità o i diritti fondamentali della persona interessata.

(2) L'incaricato per la protezione dei dati fornisce consulenza alla CNA Svizzera sull'esecuzione di una valutazione d'impatto sulla protezione dei dati e sulla determinazione dei casi in cui il trattamento dei dati può comportare un rischio elevato per le persone interessate.

§ 21 Violazione della protezione dei dati («data breach»)

(1) Qualora i dati della CNA Svizzera o di una comunità ecclesiale dovessero essere divulgati illegalmente a terzi, è necessario informare immediatamente il direttore amministrativo dell'AaApd Svizzera. Quest'ultimo coinvolge immediatamente l'incaricato per la protezione dei dati nell'ambito dell'indagine dei fatti.

(2) La notifica deve includere tutte le informazioni rilevanti per chiarire la situazione, in particolare il destinatario, le persone interessate e il tipo e l'entità dei dati trasmessi.

(3) L'adempimento di un eventuale obbligo di notifica all'IFPDT viene effettuato esclusivamente dall'incaricato per la protezione dei dati, previa consultazione con il direttore amministrativo dell'AaApd Svizzera. Le persone interessate devono essere informate dalla direzione della CNA Svizzera e l'incaricato per la protezione dei dati deve essere consultato a titolo consultivo.

§ 22 Conseguenze delle violazioni

(1) Una violazione negligente o addirittura intenzionale di queste direttive può comportare provvedimenti ai sensi del diritto del lavoro, compreso il licenziamento immediato o con preavviso. Anche sanzioni penali e conseguenze civili come il risarcimento danni possono essere prese in considerazione.

§ 23 Obbligo di responsabilità e tracciabilità

(1) La conformità alle disposizioni di queste direttive sulla protezione dei dati deve essere dimostrabile in ogni momento. In questo contesto, occorre prestare particolare attenzione alla tracciabilità e alla trasparenza delle misure adottate, per esempio attraverso la relativa documentazione.

§ 24 Attuazione delle direttive

(1) In considerazione dell'ulteriore sviluppo della legge sulla protezione dei dati e delle evoluzioni tecnologiche o organizzative, le attuali direttive sulla protezione dei dati saranno sottoposte a revisioni periodiche per valutare la necessità di aggiornamenti o integrazioni.

(2) Le modifiche a queste direttive sulla protezione dei dati diventano efficaci senza richiedere procedure formali. I ministri e le ministri e le persone con funzioni di responsabilità come tutto il personale dell'Amministrazione della CNA Svizzera sono da informare tempestivamente e in modo appropriato sulle modifiche delle disposizioni.

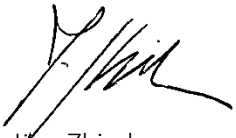
§ 25 Disposizioni finali ed entrata in vigore

(1) Le presenti direttive sulla protezione dei dati sostituiscono le direttive sulla protezione dei dati attualmente in vigore, datate 1° marzo 2019.

(2) Le modifiche entreranno in vigore il 1° settembre 2023.

Zurigo, 6 giugno 2023

Per la Chiesa Neo-Apostolica Svizzera:



Jürg Zbinden
Presidente della Chiesa

Reto Keller
Direttore dell'Amministrazione