



Política de privacidad de INAI

Iglesia Nueva Apostólica Internacional (INAI)

Válida a partir de
01 de enero de 2021



Índice

Prólogo / Introducción	2
Aspectos generales.....	3
Organización de la protección de datos.....	6
Derechos de los interesados	7
Transferencia y transmisión de datos al extranjero	7
Registro de las actividades de tratamiento y de los ficheros de INAI	8
Seguridad de los datos personales	9
Formación del personal administrativo	10
Consecuencias de infracciones.....	10
Disposiciones finales.....	10
Anexo: Definiciones.....	12

Fuentes

INAI, Directriz para Redes Sociales de la Iglesia Nueva Apostólica, edición de diciembre de 2017

Iglesia Nueva Apostólica Alemania Occidental, Política de privacidad, última actualización: 20 de abril de 2018

Iglesia Nueva Apostólica Sur de Alemania, Política de privacidad, última actualización: 24 de mayo de 2018

Iglesia Nueva Apostólica Suiza, Política de privacidad INA Suiza, última actualización: 1 de marzo de 2019

Iglesia Nueva Apostólica Austria, Política de privacidad INA Austria, última actualización: 1 de marzo de 2019



Prólogo / Introducción

Estimados Apóstoles, estimados colaboradores, estimados colaboradores en proyectos:

El 25 de mayo de 2018 entró en vigor el [Reglamento General de Protección de Datos \(RGPD\)](#). En primer lugar se aplica en los estados de la UE y del EEE. En algunos casos también es de aplicación en estados terceros como Suiza. INAI, en calidad de asociación de derecho suizo, está sujeta ante todo a la legislación suiza y, por consiguiente, a la [Ley de Protección de Datos suiza \(DSG, por sus siglas en alemán\)](#). En los últimos años, dicha ley se ha revisado completamente. El 25 de septiembre de 2020, el Parlamento aprobó el nuevo texto legislativo. Su contenido se basa fundamentalmente en el RGPD y está previsto que entre en vigor en el año 2022. A causa de ello, así como de los estrechos vínculos de INAI con Europa y de la creciente aceptación del RGPD a nivel mundial, la presente Política de privacidad se inspira en el RGPD.

Los contenidos del RGPD no son totalmente nuevos. Ya en el pasado las leyes de protección de datos de los estados miembros de la UE y del EEE, así como de Suiza, preveían de manera bastante concreta la clase de datos que se podían recopilar y tratar y las condiciones y fines del tratamiento. El RGPD refuerza estas normas y obliga a los responsables (las personas/organizaciones que recopilan/tratan datos) también a documentar de manera transparente y claramente legible los datos obtenidos. Todo ello se basa en el principio de minimización de datos, es decir, de recopilar solamente aquellos datos que realmente se necesitan para conseguir los fines legítimos y de suprimirlos en cuanto sea posible. Todos aquellos que recopilen y traten datos tienen que reflexionar sobre su propia actuación y sus procesos de trabajo, adaptándolos en caso necesario, ya que no existe un modelo de validez general que se pueda implementar tal cual.

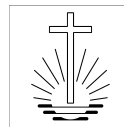
Los rápidos cambios en el comportamiento de comunicación de nuestra sociedad se ven influenciados enormemente por las innovaciones tecnológicas, de manera que la protección de datos a menudo pasa a un segundo plano. En calidad de Iglesia queremos asegurarnos de que los derechos de privacidad no se vean mermados por el simple hecho de disponer de medios más simples y cómodos, por lo que nos proponemos actuar de manera responsable también en este ámbito.

Cordialmente,

Su

Erich Senn
Administrador NACI

Frank Stegmaier
CFO



Aspectos generales

Art. 1º. Aspectos generales

(1) Para la protección de datos personales, la Iglesia Nueva Apostólica Internacional (en lo sucesivo denominada «INAI» o «el responsable») se basa en los estándares de protección de datos de la Unión Europea (UE), especialmente en lo que a los datos de los miembros de INAI y a los colaboradores de la Administración INAI (personal administrativo) se refiere.

(2) Hoy día, INAI supone que una protección de datos conforme a la normativa de la UE en su gran mayoría cumple con las disposiciones de la nueva Ley de protección de datos suiza (nDSG, por sus siglas en alemán), aprobada el 25 de septiembre de 2020 por el Parlamento suizo.

Art. 2º. Objeto

(1) La presente Política de privacidad de INAI (en lo sucesivo «Política de privacidad INAI» o «Política de privacidad») constituye la base vinculante para el tratamiento legal de *datos personales* por INAI.

(2) Esta Política de privacidad debe preservar y proteger los derechos y las libertades fundamentales de los interesados, especialmente su derecho a la protección de datos personales.

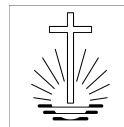
(3) Además, debe garantizar la libre circulación de estos datos.

Art. 3º. Ámbito de aplicación

(1) Esta Política de privacidad es de aplicación para el tratamiento de datos personales por INAI en calidad de asociación de derecho suizo con sede permanente en Zúrich (Suiza) y de unidad administrativa central.

(2) Está destinada personalmente a todo el personal administrativo. Esta Política de privacidad también es de aplicación para los Apóstoles, para los colaboradores en proyectos, así como para todas las personas que cumplan algún encargo o mantengan una relación de servicios con INAI.

(3) Las obligaciones y las prohibiciones de esta Política de privacidad son de obligado cumplimiento en cualquier tratamiento de datos personales, sea de forma electrónica, en soporte de papel u oral.



Art. 4º. Tratamiento y recopilación de datos

(1) Bajo *tratamiento de datos* se entiende cualquier manejo de datos personales, desde su recopilación hasta su archivo y supresión.

(2) En el tratamiento de datos personales se deben observar siempre los principios del RGPD (véase el art. 5º. RGPD): Licitud, lealtad, transparencia, limitación de la finalidad, minimización de datos, exactitud de los datos personales, limitación del plazo de conservación («derecho al olvido»), integridad, confidencialidad y disponibilidad («seguridad de los datos» / «seguridad de la información») y responsabilidad proactiva.

(3) En principio son las Iglesias regionales las que recopilan datos personales de los interesados.

(4) Datos principales de los miembros de la Iglesia: Algunas personas que trabajan en la administración tienen acceso a los datos principales de los miembros de las Iglesias regionales. Se requiere este acceso para tareas administrativas como la asistencia espiritual de las Iglesias por los Apóstoles o la pertenencia a grupos de proyecto de miembros de la Iglesia que colaboren en proyectos de INAI.

(5) Expedientes de Apóstoles: Los datos relacionados con la ordenación de un Apóstol son datos muy personales del interesado y, por consiguiente, se consideran datos sensibles. En su caso es la Iglesia regional en cuestión la que proporciona estos datos en vistas a la ordenación. Además, INAI dispone de información sobre los datos principales del Apóstol y sus ámbitos de trabajo geográficos.

(6) Expedientes del personal administrativo. En ellos a menudo se recopilan datos sobre la situación laboral, la pertenencia a partidos políticos, las aficiones, el número de hijos, la formación, etc., de la persona en cuestión. Estos datos también tienen carácter sensible.

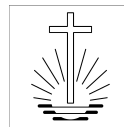
Art. 5º. Limitación de la finalidad, minimización de datos, consentimiento

(1) La recopilación, el tratamiento, el uso y la transmisión de datos personales solamente es admisible en caso de que sean necesarios para el cumplimiento de la misión de la Iglesia o que el interesado haya dado su consentimiento (limitación de la finalidad). Se requiere una operación de tratamiento de datos cuando el objetivo de la Iglesia no se pueda conseguir de otra manera o su consecución exija un esfuerzo mucho mayor.

(2) La recopilación, el tratamiento y el uso de datos personales deberán limitarse a lo imprescindible para conseguir la finalidad (minimización de datos).

(3) La publicación de datos personales, por ejemplo a través de Internet, solamente es admisible con el consentimiento explícito. El consentimiento es válido si es una manifestación de voluntad libre, específica, informada e inequívoca del interesado, ya sea mediante una declaración o una clara acción afirmativa.

(4) No requieren un consentimiento particular las informaciones sobre acontecimientos de ministerio, viajes y actividades de Apóstoles que sean de interés para los miembros de la Iglesia en el mundo.



Art. 6º. Secreto de datos, secreto de la asistencia espiritual y discreción en el ministerio

(1) Las personas que trabajan para INAI no pueden recopilar, tratar o usar datos personales sin la autorización correspondiente. Antes de iniciar su actividad deben comprometerse a un trato confidencial de los datos personales (firma de una declaración de confidencialidad).

(2) Los registros («notas personales») elaborados en el ejercicio de la actividad profesional en INAI no deben ser accesibles a terceros, sin perjuicio de las disposiciones especiales sobre la protección del secreto de la asistencia espiritual. Lo mismo se aplica a las demás obligaciones de confidencialidad para preservar las obligaciones legales de secreto y confidencialidad y los secretos profesionales especiales que no se basan en disposiciones legales.

(3) Estas obligaciones de confidencialidad son de duración indefinida. También se aplican a informaciones intercambiadas o accesibles con anterioridad a la eventual firma de una declaración de confidencialidad. Son irrevocables y siguen en vigor incluso después de finalizar la colaboración o la relación contractual o el cumplimiento de la prestación convenida, así como después de finalizar la relación laboral, el encargo o los servicios acordados.

Art. 7º. Conservación, archivo y supresión

(1) Como norma general, los datos personales que ya no sean necesarios ni requieran su archivo deben ser suprimidos o destruidos permanentemente (por ej. con una destructora de documentos).

(2) Los datos personales deben ser suprimidos siempre y cuando no sea admisible su conservación, se haya revocado el consentimiento para su conservación o ya no sean necesarios para los fines de su recopilación.

(3) Para documentar la afiliación, recibir sacramentos y realizar ordenaciones en la Iglesia, así como para dar encargos y hacer nombramientos se requieren datos personales de miembros de la Iglesia. Por consiguiente, la revocación del consentimiento para la conservación o una retirada de la Iglesia no conlleva automáticamente la supresión de los datos. Simplemente se limita el acceso a estos datos personales para poder informar al interesado y entregarle documentos.

(4) Otras excepciones de la obligación de supresión son:

- los datos personales convertidos en anónimos;
- las obligaciones legales de conservación;
- datos personales que deban ser conservados a efectos de prueba o seguridad o para salvaguardar los intereses dignos de protección del interesado.

(5) Se deben regular los detalles en un concepto de supresión y archivo (incluyendo las copias de seguridad).



Organización de la protección de datos

Art. 8º. Delegado de protección de datos¹

(1) INAI nombra a un Delegado de protección de datos. Puede contactar con el Delegado de protección de datos dirigiéndose a:

Neuapostolische Kirche International
Delegado de protección de datos
Ueberlandstrasse 243
8051 Zúrich / Suiza

privacy@nak.org

(2) El Delegado de protección de datos vela por el cumplimiento del Reglamento General de Protección de Datos (RGPD), así como de otras normas legales, incluyendo las disposiciones de estas y otras directrices sobre protección de datos de INAI. El Delegado de protección de datos asesora e informa a la Dirección de administración sobre las obligaciones existentes en materia de protección de datos y es responsable de la comunicación con las autoridades de protección de datos. Controla de manera aleatoria, en función de los riesgos y con cierta regularidad, la conformidad de ciertos procesos con los requisitos de protección de datos.

(3) El Delegado de protección de datos ejerce su función sin órdenes en base a sus conocimientos específicos. Presenta sus informes directamente a la Dirección de administración.

(4) La Dirección de administración y el personal administrativo asisten al Delegado de protección de datos en el cumplimiento de sus funciones.

(5) En la presentación pública de la Iglesia a menudo se encuentran indicaciones sobre la protección de datos en las que deberá mencionarse a partir de ahora al Delegado de protección de datos.

Art. 9º. Coordinador de protección de datos

(1) Además, INAI se compromete a formar en materia de protección de datos a una persona que trabaje en la administración. Esta persona tiene el encargo de asegurar la aplicación de la protección de datos y de dar las instrucciones correspondientes dentro de la Iglesia.

¹ Por razones de simplificación, en lo sucesivo solamente se usará la forma masculina, de conformidad con el uso en el RGPD.



Derechos de los interesados

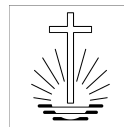
Art. 10º. Derechos de los interesados

- (1) La Dirección de administración informa a los interesados exhaustivamente sobre el tratamiento de sus datos, como mínimo una vez con motivo de su contratación u ordenación.
- (2) El ejercicio de los siguientes derechos, por ej. el de acceso, debe ir dirigido a la persona correcta, por lo que con anterioridad hay que verificar de manera fiable la autorización y la identidad del solicitante.
- (3) Derecho de acceso: a solicitud de los interesados hay que darles acceso a los datos conservados sobre su persona. Por regla general, el acceso se da por escrito, salvo que el interesado haya solicitado el acceso electrónico. Hay que dar acceso en un plazo de 30 días desde la recepción de la solicitud.
- (4) Derecho de rectificación o supresión: los interesados pueden solicitar que se complementen datos personales incompletos y que se supriman los datos que ya no sean necesarios. Con anterioridad a una eventual supresión de datos, hay que tener en cuenta que podría estar en conflicto con obligaciones legales u otras obligaciones de conservación, o con un interés de la Iglesia u otro interés legítimo.
- (5) El que crea que un organismo de la Iglesia, mediante la recopilación, el tratamiento o el uso de sus datos personales, ha vulnerado sus derechos puede dirigirse por escrito al Delegado de protección de datos o a la Dirección de administración.

Transferencia y transmisión de datos al extranjero

§ 11º. Transferencia y transmisión de datos

- (1) La transmisión de datos personales a terceros solamente es admisible con una autorización legal o por encargo o con el consentimiento del interesado.
- (2) La Dirección de administración se encuentra en Zúrich (Suiza) y trata los datos personales en Suiza. La protección de estos datos en el intercambio con las Iglesias regionales en la UE y en el EEE se garantiza mediante la decisión de adecuación de la Comisión de la UE, así como a través de la información adecuada y el consentimiento del interesado.
- (3) La eventual transferencia y transmisión de datos a una Iglesia regional o a organizaciones con sede fuera de la UE o el EEE, solamente se permite con el consentimiento expreso del interesado.



Art. 12º. Proveedores de servicios externos

(1) En el caso de que proveedores de servicios externos deban tener acceso a datos personales habrá que informar previamente al Delegado de protección de datos.

(2) Con anterioridad a la adjudicación de un contrato deberán seleccionarse minuciosamente a los proveedores de servicios que puedan tener acceso a datos personales. Deberá documentarse esta selección, teniendo en cuenta sobre todo los siguientes aspectos:

- competencia profesional del proveedor de servicios para el manejo correcto de los datos;
- medidas de seguridad técnico-organizativas;
- experiencia del proveedor de servicios en el mercado;
- otros aspectos que permitan anticipar la fiabilidad del proveedor de servicios (documentación de protección de datos, disponibilidad de cooperación, tiempos de reacción, etc.).

(3) En el caso de que un proveedor de servicios recopile, trate o use datos personales por encargo, deberán firmarse un acuerdo de tratamiento de datos por encargo, así como las correspondientes declaraciones de confidencialidad que regulen todos los aspectos de protección de datos y seguridad informática.

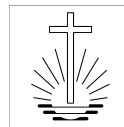
(4) Habrá que controlar periódicamente el cumplimiento de las medidas técnico-organizativas acordadas contractualmente con el proveedor de servicios. Se deberá documentar el resultado.

Registro de las actividades de tratamiento y de los ficheros de INAI

Art. 13º. Registro de las actividades de tratamiento

(1) INAI lleva un registro de todos los tratamientos bajo su competencia y de los responsables de estos tratamientos (véase el art. 30 del RGPD). El Delegado de protección de datos podrá dar asesoramiento sobre las informaciones requeridas legalmente (véase el documento separado «Registro de las actividades de tratamiento de INAI»).

(2) Bajo petición de la autoridad competente de protección de datos, INAI pondrá a su disposición el registro, siendo responsable de ello el Delegado de protección de datos de acuerdo con la Dirección de administración.



Art. 14º. Definición de «fichero»

(1) Un fichero es todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica. Ficheros son, por ejemplo, los expedientes de personal o los bancos de datos que contengan datos de miembros.

(2) Los miembros de INAI son los Apóstoles distribuidos por el mundo. Sus datos se recopilan lo más tarde cuando haya intención de llamarlos a este ministerio. INAI conserva estos datos en el banco de datos correspondiente del portal INA.

Seguridad de los datos personales

Art. 15º. Seguridad de los datos

(1) Los datos personales deben ser tratados de manera que garanticen una seguridad apropiada de los datos personales, incluyendo la protección de un tratamiento no autorizado o ilegítimo y de pérdida no intencionada, destrucción no intencionada o deterioro no intencionado, mediante la aplicación de medidas técnicas u organizativas apropiadas.

(2) El departamento informático aplica las medidas técnicas u organizativas necesarias para garantizar la seguridad de los datos personales conservados.

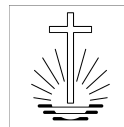
(3) De conformidad con sus funciones reflejadas en el contrato de empleo, el personal administrativo está obligado a manejar con atención los datos personales y los medios técnicos del empleador.

Art. 16º. Violación de la seguridad de datos («filtración de datos»)

(1) En el caso de que se hubieran divulgado de manera ilegítima datos de INAI a terceros habrá que informar inmediatamente a la Dirección de administración, que involucrará sin demora al Delegado de protección de datos para esclarecer los hechos.

(2) En dicha información se indicará todos los datos de interés para esclarecer los hechos, sobre todo el destinatario, los implicados, así como el tipo y el alcance de los datos transmitidos.

(3) Para el cumplimiento de un eventual deber de información hacia la autoridad de protección de datos será responsable exclusivamente el Delegado de protección de datos de acuerdo con la Dirección de administración. La Dirección de administración informará a los interesados, con asistencia y asesoramiento del Delegado de protección de datos.



Formación del personal administrativo

Art. 17º. Formación sobre protección de datos y seguridad

(1) Las personas que permanente o regularmente tengan acceso a datos personales de INAI, que los recopilen o que desarrollen sistemas para su tratamiento deberán recibir una formación apropiada sobre las normas de protección de datos. El Delegado de protección de datos decidirá, de acuerdo con la Dirección de administración, sobre la forma y la periodicidad de estas formaciones.

(2) Los ciberdelincuentes a menudo se aprovechan de cualidades humanas como la disposición para ayudar, la confianza, el miedo o el respeto a la autoridad. Por ello es importante que el personal administrativo también reciba formación sobre temas como la ciberseguridad.

Consecuencias de infracciones

Art. 18º. Consecuencias de infracciones

(1) Una infracción negligente o incluso deliberada de la presente Política de privacidad puede dar origen a medidas disciplinarias, llegando hasta el despido inmediato o dentro de los plazos estipulados. También podrían aplicarse sanciones penales y civiles como la reclamación de daños y perjuicios.

Disposiciones finales

Art. 19º. Responsabilidad proactiva

(1) Se debe poder demostrar en cualquier momento el cumplimiento de la presente Política de privacidad, velando sobre todo por la trazabilidad y transparencia de las medidas adoptadas, por ejemplo sobre la documentación pertinente.

Art. 20º. Modificaciones

(1) En virtud de la evolución del derecho de protección de datos, así como de los cambios tecnológicos u organizativos se determinará con regularidad la necesidad de adaptar o completar la presente Política de privacidad.

(2) Para la entrada en vigor de las modificaciones de la presente Política de privacidad no se requiere ninguna formalidad. Habrá que informar al personal administrativo inmediata y adecuadamente sobre las disposiciones modificadas.



Art. 21°. Cumplimiento y entrada en vigor

(1) La Dirección de administración está autorizada para adoptar medidas reglamentarias complementarias en forma de instrucciones de servicio.

(2) La presente Política de privacidad entra en vigor el 1 de enero de 2021 y sustituye cualquier política de privacidad anterior de INAI.

Zúrich, diciembre de 2020

Por la Iglesia Nueva Apostólica Internacional (INAI):

Erich Senn
Administrador INAI

Frank Stegmaier
CFO



Anexo: Definiciones

(1) *Datos personales*² son toda información sobre una persona física identificada o identificable (el interesado). Son datos personales tanto los datos sobre hermanos y hermanas como los datos sobre el personal y sobre los portadores de ministerio y los responsables. Por ejemplo, tanto el nombre como la dirección de correo electrónico de un interlocutor permiten extraer conclusiones sobre una persona física. Para ello basta que la información esté relacionada con el nombre del interesado o que pueda ser recreada independientemente del nombre. Igualmente es posible la identificación de una persona si primero hay que asociar la información a conocimientos adicionales, por ej. la fecha de nacimiento, el número de personal o la dirección IP. La generación de la información es irrelevante para su conexión con una persona. Fotografías, vídeos o grabaciones de sonido también pueden ser datos personales.

(2) *Categorías especiales de datos personales* son datos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física. Para la recopilación, el tratamiento o el uso de categorías especiales de datos personales por norma general se requiere el consentimiento del interesado; excepcionalmente es posible en base a una autorización legal explícita. Además, se requiere la adopción de medidas técnicas u organizativas adicionales (por ej. el cifrado en el transporte, concesión limitada de derechos) para la protección de categorías especiales de datos personales.

(3) El *tratamiento* es cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

(4) La *limitación del tratamiento* es el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro.

(5) La *elaboración de perfiles* es toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física. Sin embargo, INAI como organización responsable renuncia a la toma automática de decisiones o a la elaboración de perfiles.

(6) *Anonimización / seudonimización*: Los datos personales se consideran *anonimizados* cuando es imposible determinar la identidad de la persona. El término «anonimizar» se usa para cualquier operación que impida atribuir datos a una persona identificada o que lo permita solamente con un esfuerzo extraordinario. En la *seudonimización*, sin embargo, se sustituyen

² En inglés: «personal data» o «personal information».



todos los datos identificables por un conjunto de datos neutro (seudónimo). Mientras se puede revertir la seudonimización (en tanto exista y sea accesible una tabla de correspondencia que permita la reunión de las dos partes de datos), la anonimización es definitiva. Solamente los datos completamente anonimizados no se consideran datos de carácter personal.

(7) El *responsable del tratamiento* o *responsable* es la persona física o jurídica (en el presente caso el responsable es únicamente INAI), autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

(8) El *encargado del tratamiento* es la persona física o jurídica (por ej. la empresa encargada del mantenimiento tecnológico de la administración de miembros/MDV³), autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

(9) El *destinatario* es la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero.

(10) El *tercero* es la persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

(11) Un *consentimiento* del interesado es toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.

³ MDV (Mitgliederdatenverwaltung) son las siglas utilizadas para designar la administración de datos de miembros.