Datenschutzrichtlinie NAK Österreich

Datum: Gültig ab 1. März 2019

Präambel

Die europäische Datenschutz-Grundverordnung (DSGVO) ist per se nichts komplett Neues. So war bis dato bereits im Datenschutzgesetz 2000 relativ konkret festgehalten, unter welchen Bedingungen welche Daten für welche Zwecke erhoben und verarbeitet werden dürfen. Die DSGVO und das Datenschutz-Anpassungsgesetz 2018 verschärfen diese Regelungen und verpflichten die Verantwortlichen (jene Person/Organisation, die Daten erhebt/verarbeitet) auch zu transparenterer und nachvollziehbarerer Dokumentation der erhobenen Daten. Der Grundsatz ist Datenminimierung, also nur jene Daten zu erheben, die zu einem berechtigten Zweck auch benötigt werden und diese sobald wie möglich auch wieder zu löschen. Für alle, die Daten erheben und verarbeiten, bedeutet dies, sich intensiv mit dem eigenen Tun und den eigenen Arbeitsprozessen auseinanderzusetzen und diese ggf. zu adaptieren. Denn es gibt keine allgemein gültigen Vorlagen, die ohne Zutun einfach implementiert werden können.

§ 1 Bedeutung, Ziel, Zugänglichkeit

(1) Diese Datenschutzrichtlinie ist die verbindliche Basis für einen rechtskonformen und nachhaltigen Schutz personenbezogener Daten («Personendaten») bei der Neuapostolischen Kirche in Österreich (im Folgenden «NAK Österreich» oder «der Verantwortliche» genannt). Sie ist die Grundlage für alle Umsetzungsdokumente wie z.B. Handlungshinweise für Seelsorger (Amtsträger).

(2) Mit dieser Datenschutzrichtlinie sollen die Grundrechte und Grundfreiheiten von betroffenen Personen, insbesondere ihr Recht auf Schutz personenbezogener Daten gewahrt und geschützt werden.

(3) Die Datenschutzrichtlinie muss für alle Amtsträger (Seelsorger), Funktionsträger und Beschäftigten der Administration NAK Österreich jederzeit leicht zugänglich sein.

§ 2 Geltungsbereich

(1) Diese Datenschutzrichtlinie findet Geltung für das Gebiet der NAK Österreich. Für die Kirchengemeinden im Gebiet der NAK Österreich gelten insbesondere die Handlungshinweise «Datenschutz im Gemeindealltag».

(2) Sie gilt persönlich für alle Personen, die in einem ehren-, neben-, oder vollamtlichen Dienst- oder anderen Verhältnis zur NAK Österreich (z.B. Beauftragung als Gemeindevorsteher) oder ihren Einrichtungen und Institutionen stehen sowie allen kirchlichen Amtsträger der Neuapostolischen Kirche (siehe dazu auch im Katechismus, Kap. 7.1 Das Amt und die Dienste). Ebenso gilt diese Richtlinie für Personen, die in irgendeinem Auftragsverhältnis zur NAK Österreich stehen.

(3) Die Gebote und Verbote dieser Datenschutzrichtlinie gelten für jeglichen Umgang mit personenbezogenen Daten, unabhängig ob dieser elektronisch oder in Papierform erfolgt. Ebenso beziehen sie alle Arten von *betroffenen Personen* (z.B. eine Schwester / ein Bruder, ein Amtsträger, ein Mitarbeitender der Kirchenverwaltung, usw.) in ihren Geltungsbereich ein.

§ 3 Begriffsbestimmungen

(1) *Personenbezogene Daten*[1] sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (betroffene Person). Daten der Geschwister gehören dabei ebenso

[1] In Englisch: «personal data» oder «personal information».

zu den personenbezogenen Daten wie Personaldaten und Daten der Amtsträger sowie von Funktionsträgerinnen und Funktionsträgern. Beispielsweise lässt der Name eines Ansprechpartners ebenso einen Rückschluss auf eine natürliche Person zu, wie seine E-Mail-Adresse. Es genügt, wenn die jeweilige Information mit dem Namen der betroffenen Person verbunden ist oder unabhängig hiervon aus dem Zusammenhang hergestellt werden kann. Ebenso kann eine Person bestimmbar sein, wenn die Information mit einem Zusatzwissen erst verknüpft werden muss, so z. B. beim Geburtsdatum, der Personalnummer oder der IP-Adresse. Das Zustandekommen der Information ist für einen Personenbezug unerheblich. Auch Fotos, Video- oder Tonaufnahmen können personenbezogene Daten darstellen.

(2) *Besondere Arten personenbezogener Daten* sind Informationen, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen sowie eine eventuelle Zugehörigkeit zu politischen Parteien oder Gewerkschaften hervorgehen kann sowie genetische Daten, biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben bzw. der sexuellen Orientierung einer natürlichen Person.

(3) *Verarbeitung* ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführter Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.

(4) *Einschränkung der Verarbeitung* ist die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken.

(5) *Profiling* bezeichnet jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.

(6) *Anonymisierung / Pseudonymisierung:* Personenbezogene Daten gelten dann als *anonymisiert*, wenn die Person nicht mehr bestimmbar ist. Unter «anonymisieren» versteht man jeglichen Vorgang, durch den die Zuordnung von Daten zu einer konkreten Person verhindert wird oder nur noch mit aussergewöhnlichem Aufwand möglich ist. Bei der *Pseudonymisierung* hingegen werden alle identifizierenden Daten durch einen neutralen Datensatz (Pseudonym) ersetzt. Die Pseudonymisierung lässt sich rückgängig machen (solange eine Korrespondenztabelle besteht und zugänglich ist, die eine Zusammenführung der beiden Datenteile ermöglicht). Die Anonymisierung indes ist endgültig. Nur vollkommen anonymisierte Daten gelten nicht mehr als Personendaten.

(7) *Verantwortlicher* ist die natürliche oder juristische Person (vorliegend ist der Verantwortliche einzig die NAK Österreich), Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

(8) *Auftragsverarbeiter* ist eine natürliche oder juristische Person (z.B. das für den technologischen Unterhalt der Mitgliederverwaltung/MDV[2] beauftragte Unternehmen), Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

(9) *Empfänger* ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht.

(10) *Dritter* ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, ausser der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die

[2] MDV = Mitgliederdatenverwaltung.

unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

(11) Eine *Einwilligung* der betroffenen Person ist jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

§ 4 Datenschutzorganisation

(1) Die NAK Österreich hat einen Datenschutzbeauftragten[3] bestellt. Diesen erreichen Sie unter folgenden Kontaktdaten:

Neuapostolische Kirche Österreich
Datenschutzbeauftragter
Mittersteig 10
1051 Wien / Österreich

E-Mail: privacy@nak.at

(2) Der Datenschutzbeauftragte überwacht die Einhaltung der europäischen Datenschutz-Grundverordnung (DSGVO) sowie anderer gesetzlichen Vorgaben, einschliesslich der Vorgaben dieser und anderer Richtlinien der NAK Österreich zum Datenschutz. Der Datenschutzbeauftragte berät und unterrichtet den Kirchenpräsidenten sowie die Leitung Administration NAK Österreich hinsichtlich bestehender Datenschutzpflichten und ist zuständig bei der Kommunikation mit der Datenschutzbehörde. Ausgewählte Prozesse werden stichprobenartig, risikoorientiert und in angemessenen Zeitabständen durch ihn auf ihre Datenschutzkonformität hin kontrolliert.

(3) Der Datenschutzbeauftragte nimmt seine Aufgaben weisungsfrei und unter Anwendung seines Fachwissens wahr. Er berichtet unmittelbar dem Kirchenpräsidenten NAK Österreich oder seinem gesetzlichen Vertreter.

(4) Der Kirchenpräsident und die Administration NAK Österreich bzw. ihre Mitarbeitenden haben den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen.

§ 5 Umgang mit personenbezogenen Daten

(1) Bei der Verarbeitung personenbezogener Daten sind jeweils die Grundsätze der DSGVO zu beachten (vgl. Art. 5 DSGVO): Rechtmässigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit der personenbezogenen Daten, Speicherbegrenzung («Recht auf Vergessen»), Integrität, Vertraulichkeit und Verfügbarkeit («Informationssicherheit») und Rechenschaftspflicht.

(2) Die Verarbeitung personenbezogener Daten ist grundsätzlich verboten, es sei denn, eine gesetzliche Norm erlaubt explizit den Datenumgang. Personenbezogene Daten dürfen nach der DSGVO grundsätzlich verarbeitet werden:

– Bei einem bestehenden Vertragsverhältnis mit der betroffenen Person.

Beispiel: Die Speicherung und Verwendung erforderlicher personenbezogener Daten im Rahmen der Mitgliedschaft zur NAK Österreich oder eines Anstellungsvertrages oder Auftrages für die Administration der NAK Österreich.

– Im Zuge vorvertraglicher Massnahmen auf Anfrage der betroffenen Person sowie der Vertragsabwicklung mit der betroffenen Person.

Beispiel: Im Rahmen eines Anstellungsprozesses für eine Stelle bei der Administration der NAK Österreich werden die hierfür notwendigen personenbezogenen Daten erhoben.

---

[3] Der Einfachheit halber wird vorliegend, entsprechend der Bezeichnung in der DSGVO, lediglich die männliche Schreibweise verwendet.

– Wenn und soweit die betroffene Person eingewilligt hat.

Beispiel: Die betroffene Person willigt ein, dass die für die Mitgliedschaft notwendigen Daten erhoben und verarbeitet werden. Die Mitgliedschaft zur NAK Österreich wird durch die heilige Versiegelung begründet.

– Wenn eine rechtliche Verpflichtung besteht, der die NAK Österreich unterliegt.

Beispiel: Gesetzliche Aufbewahrungsfristen.

– Wenn berechtigte Interessen der NAK Österreich bestehen, sofern nicht die Interessen oder Grundrechte der betroffenen Person überwiegen, insbesondere wenn es sich um ein Kind[4] handelt. Datenverarbeitungen unter Berufung auf ein berechtigtes Interesse sollten jedoch nicht ohne vorherige Beratung durch den Datenschutzbeauftragten vorgenommen werden.

Beispiel: Die Nutzung der postalischen Anschrift von ehemaligen Geschwistern einer Kirchengemeinde zur Einladung an eine Jubiläumsfeier.

(3) Abweichend zu Absatz (2) dürfen alle Amtsträger (Seelsorger) zum Zweck ihres Seelsorgeauftrags eigene Aufzeichnungen («persönliche Notizen») führen. Dies hat sich jedoch auf jene Kirchenmitglieder zu beschränken, die sie im Rahmen des Seelsorgeauftrages persönlich betreuen. Der Inhalt dieser Aufzeichnungen muss in einem direkten Bezug zur Seelsorgetätigkeit stehen. Diese Aufzeichnungen dürfen niemandem zugänglich gemacht werden. Dazu hat der betreffende Amtsträger (Seelsorger) geeignete technische oder organisatorische Massnahmen zu treffen.

(4) Betroffene Personen dürfen nicht einer ausschliesslich auf einer automatisierten Verarbeitung – so auch dem Profiling – beruhenden Entscheidung unterworfen werden, die ihnen gegenüber eine rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

(5) Personenbezogene Daten sind für einen zuvor festgelegten, eindeutigen und legitimen Zweck zu verarbeiten. Eine Datenhaltung ohne Zweck, so beispielsweise die Speicherung von Daten auf Vorrat, ist unzulässig.

(6) Falls möglich, sollte auf einen personenbezogenen Datenumgang verzichtet werden. Pseudonyme oder anonyme Datenverarbeitungen sind vorzuziehen.

(7) Die Änderung einer Ziel- und Zweckbestimmung, die einem Datenumgang ursprünglich zugrunde gelegt wurde, ist – neben der erklärten Einwilligung durch die betroffene Person – nur zulässig, wenn der Zweck der Weiterverarbeitung mit dem ursprünglichen Zweck vereinbar ist (z.B. beim Übertritt in eine andere Unterrichtsstufe). Hierbei sind insbesondere die vernünftigen Erwartungen der betroffenen Person hinsichtlich einer solchen Weiterverarbeitung gegenüber der NAK Österreich, die Art der verwendeten Daten, die Folgen für die betroffene Person sowie Möglichkeiten einer Verschlüsselung oder Pseudonymisierung zu berücksichtigen.

(8) Die betroffene Person ist bei der Erhebung ihrer personenbezogenen Daten umfassend über den Umgang mit ihren Daten zu informieren. Die Information hat die Zweckbestimmung, die Identität der verantwortlichen Stelle, die Empfänger ihrer personenbezogenen Daten sowie alle sonstigen Information im Sinne des Art. 13 DSGVO zu beinhalten, um eine faire und transparente Verarbeitung zu gewährleisten. Die Information ist in einer verständlichen und leicht zugänglichen Form sowie einer möglichst einfachen Sprache zu verfassen.

(9) Personenbezogene Daten müssen sachlich richtig und, wenn nötig, auf dem neusten Stand sein. Der Umfang der Datenverarbeitung sollte hinsichtlich der festgelegten Zweckbestimmung erforderlich und relevant sein. Die Administration der NAK Österreich hat für die Umsetzung durch die Etab-

[4] Vgl. staatlich verpflichtender Religionsunterricht. Die Daten der Schüler müssen für die Dauer der Unterrichtspflicht gespeichert werden und der entsprechenden Lehrkraft bzw. der Schulbehörde zugänglich sein.

lierung entsprechender Prozesse Sorge zu tragen. Dazu ist sie durch den Kirchenpräsidenten weisungsbefugt. Ebenso sind Datenbestände regelmässig auf ihre Richtigkeit, Erforderlichkeit und Aktualität hin zu überprüfen.

§ 6 Besondere Kategorien personenbezogener Daten

Besondere Kategorien personenbezogener Daten dürfen **grundsätzlich nur mit Einwilligung der betroffenen Person oder ausnahmsweise aufgrund einer expliziten gesetzlichen Erlaubnis erhoben**, verarbeitet oder genutzt werden. Ferner sind zusätzliche technische und organisatorische Massnahmen (z. B. Verschlüsselung beim Transport, minimale Rechtevergabe) zum Schutz besonderer personenbezogener Daten zu ergreifen.

§ 7 Datenübermittlung

(1) Die Übermittlung von personenbezogenen Daten an Dritte ist nur aufgrund gesetzlicher Erlaubnis oder der Einwilligung der betroffenen Person zulässig.

(2) Befindet sich der Empfänger personenbezogener Daten ausserhalb der Europäischen Union oder des Europäischen Wirtschaftsraums, bedarf es besonderer Massnahmen zur Wahrung von Rechten und Interessen der betroffenen Personen. Eine Datenübermittlung ist zu unterlassen, wenn bei der empfangenden Stelle kein angemessenes Datenschutzniveau vorhanden ist oder beispielsweise über besondere Vertragsklauseln nicht hergestellt werden kann.

§ 8 Externe Dienstleister

(1) Sofern externe Dienstleister Zugriff auf personenbezogene Daten erhalten sollen, ist der Datenschutzbeauftragte vorab zu informieren.

(2) Dienstleister mit einem möglichen Zugriff auf personenbezogene Daten sind vor der Auftragserteilung sorgfältig auszuwählen. Die Auswahl ist zu dokumentieren und sollte insbesondere die folgenden Aspekte berücksichtigen:

– Fachliche Eignung des Auftragnehmers für den konkreten Datenumgang
– Technisch-organisatorische Sicherheitsmassnahmen
– Erfahrung des Anbieters im Markt
– Sonstige Aspekte, die auf eine Zuverlässigkeit des Anbieters schliessen lassen (Datenschutz-Dokumentationen, Kooperationsbereitschaft, Reaktionszeiten, usw.)

(3) Soll ein Dienstleister personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen, bedarf es des Abschlusses eines Vertrags zur Auftragsverarbeitung sowie entsprechender Geheimhaltungserklärungen. Hierin sind Datenschutz- und IT-Sicherheitsaspekte zu regeln.

(4) Der Dienstleister ist im Hinblick auf die mit ihm vertraglich vereinbarten technisch-organisatorischen Massnahmen regelmässig zu überprüfen. Das Ergebnis ist zu dokumentieren.

§ 9 Aufbewahrung, Archivierung und Löschung

(1) Als Grundsatz gilt: Personendaten, die nicht mehr benötigt werden und auch nicht archivwürdig sind, müssen dauerhaft gelöscht bzw. vernichtet (z.B. Aktenvernichter) werden.

(2) Ausnahmen sind:

– Anonymisierte Personendaten
– Personendaten, welche im Rahmen einer unwiderruflichen und nicht wiederholbaren heiligen Handlung wie der Taufe oder Versiegelung erhoben worden sind oder für allfällige spätere kirchliche Handlungen wie z.B. Eheschliessung oder Beerdigung benötigt werden (z.B. Taufbescheinigung, Versiegelungsbescheinigung)
– Personendaten, welche zu Beweis- oder Sicherheitszwecken oder zur Wahrung der schutzwürdigen Interessen der betroffenen Person aufbewahrt werden müssen

(3) Einzelheiten sind in einem Lösch- und Archivierungskonzept zu regeln.

§ 10 Datenminimierung, Privacy by Desgin/Privacy by Default

(1) Der Umgang mit personenbezogenen Daten ist an dem Ziel auszurichten, so wenige Daten wie möglich von einer betroffenen Person zu erheben, zu verarbeiten oder zu nutzen („Datenminimierung"). Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist. Beispielsweise wird es im Rahmen einer statistischen Auswertung von Daten nicht notwendig sein, den vollen Namen einer betroffenen Person zu kennen und zu verwenden. Vielmehr kann diese Information durch einen Zufallswert ersetzt werden, der eine Unterscheidbarkeit der zugrunde liegenden Information ebenfalls gewährleisten kann.

(2) Entsprechendes gilt für die Auswahl und Gestaltung von Datenverarbeitungssystemen (z.B. die MDV). Der Datenschutz ist von Anfang an in die Spezifikationen und die Architektur von Datenverarbeitungssystemen zu integrieren, um die Einhaltung der Grundsätze des Schutzes der Privatsphäre und des Datenschutzes zu erleichtern, so insbesondere den Grundsatz der Datenminimierung.

§ 11 Rechte von betroffenen Personen

(1) Die Ausübung der nachstehenden Rechte wie z.B. die Auskunftserteilung muss die richtige Person betreffen. Daher ist jeweils vorgängig die Berechtigung des Antragsstellers sowie dessen Identität zweifelsfrei festzustellen.

(2) Betroffene Personen haben das **Recht auf Auskunft** über alle personenbezogenen Daten, die über sie gespeichert sind und/oder verarbeitet werden.

(3) Die Auskunftserteilung erfolgt in der Regel schriftlich, es sei denn die betroffene Person hat den Antrag auf Auskunft elektronisch gestellt. Die Auskunft ist innerhalb von 30 Tagen seit Eingang des Auskunftsbegehrens zu erteilen. Der Auskunft ist eine Kopie der Daten der betroffenen Person beizufügen, die, neben den zur Person vorhandenen Daten, auch die Empfänger von Daten, den Zweck der Speicherung sowie alle weiteren gesetzlich geforderten Informationen nach Art. 15 DSGVO beinhaltet, um der betroffenen Person die Verarbeitung bewusst zu machen und die Rechtmässigkeit selbst beurteilen zu lassen. Auf besonderen Wunsch der betroffenen Person werden die Daten in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung gestellt. Die zuständige IT-Abteilung legt den hierfür vorzusehenden Standard fest.

(4) Die betroffenen Personen haben einen **Anspruch auf Berichtigung** ihrer personenbezogenen Daten, wenn sich diese als unrichtig erweisen. Ebenso können sie die Vervollständigung unvollständiger personenbezogener Daten verlangen.

(5) Die betroffene Person hat das **Recht auf Löschung** ihrer personenbezogenen Daten unter den folgenden Voraussetzungen:

– die Kenntnis der Daten ist für die Erfüllung des Zwecks der Speicherung nicht mehr erforderlich,

– die betroffene Person hat eine Einwilligung widerrufen und es fehlt an einer anderweitigen Rechtsgrundlage für die Verarbeitung,

– ihre Verarbeitung ist unzulässig,

– die betroffene Person legt Widerspruch gegen die Verarbeitung ein oder beruft sich auf ein Widerspruchsrecht aufgrund einer besonderen – zu begründenden – persönlichen Situation,

– es handelt sich um besondere personenbezogene Daten, deren Richtigkeit nicht bewiesen werden kann, oder

– es besteht eine anderweitige rechtliche Verpflichtung zur Datenlöschung.

Besteht eine Verpflichtung zur Löschung und wurden die personenbezogenen Daten zuvor öffentlich gemacht, sind weitere Verantwortliche für die Datenverarbeitung über ein Löschbegehren der betroffenen Person hinsichtlich aller Kopien ihrer Daten sowie aller Links zu diesen Daten zu informieren.

(6) Die betroffene Person kann die **Einschränkung der Verarbeitung** ihrer Daten verlangen, wenn

– die Richtigkeit ihrer personenbezogenen Daten strittig ist (z.B. falsch erfasster Name nach erfolgter Eheschliessung). Diese Einschränkung der Verarbeitung gilt jedoch nur so lange, bis die Richtigkeit durch die zuständige Organisationseinheit (z.B. die Administration der NAK Österreich oder die Kirchengemeinde, wo die betroffene Person zugehört) geklärt ist oder

– die Verarbeitung unzulässig ist, die betroffene Person die Datenlöschung aber ablehnt, oder

– die NAK Österreich die personenbezogenen Daten für Zwecke der Verarbeitung nicht mehr benötigt, die betroffene Person die Daten jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt, oder

– die betroffene Person Widerspruch gegen die Verarbeitung aufgrund einer besonderen Situation eingelegt hat und die zuständige Organisationseinheit (z.B. die Administration der NAK Österreich oder die Kirchengemeinde, wo die betroffene Person zugehört) noch mit der Prüfung des Widerspruchs befasst ist.

(7) Die betroffene Person ist spätestens innerhalb eines Monats über alle ergriffenen Massnahmen, die auf ihren Antrag hin erfolgt sind, zu informieren.

(8) Der Datenschutzbeauftragte steht bei der Wahrung der Betroffenenrechte beratend zur Verfügung.

§ 12 Auskunftsersuchen Dritter über betroffene Personen

Die NAK Österreich gibt grundsätzlich keine personenbezogenen Daten an Dritte weiter. Sollte eine Stelle Informationen über betroffene Personen fordern, so beispielsweise eine Behörde oder eine Soziale Einrichtung, ist eine Weitergabe von Informationen nur zulässig, wenn

– die Auskunft ersuchende Stelle ein berechtigtes Interesse hierfür darlegen kann, und

– eine gesetzliche Norm zur Auskunft verpflichtet, sowie

– die Identität des Anfragenden oder der anfragenden Stelle zweifelsfrei feststeht.

§ 13 Verzeichnis von Verarbeitungstätigkeiten

(1) Die NAK Österreich führt ein Verzeichnis über alle Datenverarbeitungen und verantwortlichen Personen dieser Datenverarbeitungen (vgl. Art. 30 DSGVO). Der Datenschutzbeauftragte kann zur Beratung hinsichtlich der gesetzlich geforderten Informationen hinzugezogen werden.

(2) Die NAK Österreich stellt der zuständigen Datenschutzbehörde das Verzeichnis auf Anfrage zur Verfügung. Zuständig hierfür ist der Datenschutzbeauftragte im Einvernehmen mit dem Kirchenpräsidenten der NAK Österreich.

§ 14 Schulung

(1) Personen, die ständig oder regelmässig Zugang zu personenbezogenen Daten der NAK Österreich haben, solche Daten erheben oder Systeme zur Verarbeitung solcher Daten entwickeln, sind in geeigneter Weise über die datenschutzrechtlichen Vorgaben zu schulen. Die Datenschutzbeauftragte entscheidet im Einvernehmen mit dem Kirchenpräsidenten der NAK Österreich über Form und Turnus der entsprechenden Schulungen.

§ 15 Datengeheimnis, Seelsorgegeheimnis und Amtsverschwiegenheit

(1) Personen, welche für die Administration NAK Österreich tätig sind, ist es untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Sie sind vor Aufnahme ihrer Tätigkeit auf einen vertraulichen Umgang mit personenbezogenen Daten zu verpflichten (Unterzeichnen einer Geheimhaltungserklärung).

(2) Personen mit besonderen Geheimhaltungsverpflichtungen (z.B. MDV-Verantwortliche) werden ergänzend darauf schriftlich verpflichtet.

(3) Aufzeichnungen («persönliche Notizen»), die in Ausübung eines kirchlichen Seelsorgeauftrages erstellt werden, dürfen dritten Personen nicht zugänglich sein. Die besonderen Bestimmungen über den Schutz des Seelsorgegeheimnisses bleiben unberührt. Gleiches gilt für die sonstigen Verschwiegenheitsverpflichtungen zur Wahrung gesetzlicher Geheimhaltungs- und Verschwiegenheitspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen.

(4) Diese Geheimhaltungspflichten sind zeitlich unbefristet. Sie gelten auch für Informationen, die vor der allfälligen Unterzeichnung einer Geheimhaltungserklärung ausgetauscht oder zugänglich gemacht worden sind. Sie sind unwiderruflich und bleiben auch nach Beendigung der Zusammenarbeit bzw. des Vertragsverhältnisses oder der Erfüllung der vereinbarten Leistungen sowie nach Auflösung eines Arbeits- oder Auftragsverhältnisses weiter.

§ 16 Beschwerden

(1) Jede betroffene Person hat das Recht, sich über eine Verarbeitung ihrer Daten zu beschweren, sollte sie sich hierdurch in ihren Rechten verletzt fühlen.

(2) Die zuständige Stelle für die oben genannten Beschwerden ist der Datenschutzbeauftragte als interne unabhängige und weisungsfreie Instanz.

§ 17 Audits

(1) Um ein hohes Datenschutzniveau zu gewährleisten, können relevante Prozesse durch regelmässige Audits interner Stellen oder durch externe Auditoren überprüft werden. Im Falle der Feststellung eines Verbesserungspotentials sind unmittelbare Abhilfemassnahmen zu treffen.

(2) Die beim Audit gewonnenen Erkenntnisse sind zu dokumentieren. Die Dokumentation ist der Datenschutzbeauftragten, den Fachverantwortlichen für den jeweiligen Prozess sowie dem Kirchenpräsidenten der NAK Österreich und in Kopie dem Leiter Administration BAB Schweiz[5] zu übergeben.

(3) Ein Audit ist erfolgreich abgeschlossen, wenn alle im Bericht dokumentierten Massnahmen umgesetzt sind. Bei Bedarf werden Follow-up-Audits durchgeführt, indem Empfehlungen des initialen Audits einer Überprüfung ihrer Implementierung unterzogen werden.

§ 16 Interne Ermittlungen

(1) Massnahmen zur Sachverhaltsaufklärung und zur Vermeidung oder Aufdeckung von Straftaten oder schwerwiegenden Pflichtverletzungen sind unter genauer Beachtung der einschlägigen gesetzlichen Datenschutzvorschriften durchzuführen. Insbesondere muss die damit einhergehende Datenerhebung und -verwendung zum Erreichen des Ermittlungszwecks erforderlich, angemessen und mit Blick auf die schutzwürdigen Interessen des Betroffenen verhältnismässig sein.

(2) Die betroffene Person ist so bald wie möglich über die zu ihrer Person durchgeführten Massnahmen zu informieren.

(3) Bei allen Formen der internen Ermittlungen ist die Datenschutzbeauftragte hinsichtlich der Auswahl und Ausgestaltung der Massnahmen vorab einzubeziehen.

§ 17 Verfügbarkeit, Vertraulichkeit und Integrität von Daten

(1) In Abhängigkeit der Art, des Umfangs, der Umstände und Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit hat für jedes Verfahren (z.B. Entwicklung einer neuen Datenbank mit personenbezogenen Daten von Kirchenmitgliedern) eine dokumentierte Schutzbedarfsfeststellung und Analyse hinsichtlich der Risiken für betroffene Personen zu erfolgen.

(2) Zur Wahrung der Verfügbarkeit, Vertraulichkeit und Integrität von Daten («Informationssicherheit») wird ein allgemeines Sicherheitskonzept in Abhängigkeit der Schutzbedarfsfeststellung und Risikoanalyse erstellt, das für alle Verfahren verbindlich ist. Hierin ist insbesondere der Stand der Technik

[5] BAB Schweiz = Bezirksapostelbereich Schweiz

ebenso zu berücksichtigen, wie Mittel und Massnahmen zur Verschlüsselung und Datensicherung. Das Sicherheitskonzept ist hinsichtlich der Wirksamkeit der dort vorgesehenen technisch-organisatorischen Massnahmen regelmässig zu überprüfen, zu bewerten und zu evaluieren.

(3) Es ist zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. Türen unbesetzter Räume sind zu verschliessen. Wirksame Massnahmen zur Zugangskontrolle an Geräten müssen vorhanden und aktiviert sein. Systemzugänge sind in Abwesenheit stets zu sperren.

(4) Passwörter ermöglichen einen Zugang zu Systemen und den darin gespeicherten personenbezogenen Daten. Sie stellen eine persönliche Kennung des Nutzers dar und sind nicht übertragbar. Es ist sicherzustellen, dass Passwörter stets unter Verschluss gehalten werden. Passwörter müssen eine minimale Länge von acht Zeichen aufweisen und aus einem Zeichenmix bestehen (Grossbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen). Passwörter dürfen nicht in einem Wörterbuch vorkommen oder aus leicht zu erratenden Begriffen gebildet werden, insbesondere nicht Begriffe, die im Zusammenhang mit der NAK Österreich stehen.

(5) Zugriffe auf personenbezogene Daten sollen nur diejenigen Personen erhalten, die im Zuge ihrer Aufgabenwahrnehmung Kenntnis von den jeweiligen Daten erhalten müssen („Need-to-know-Prinzip“). Zugriffsberechtigungen müssen genau und vollständig festgelegt und dokumentiert sein.

(6) Datenübertragungen durch öffentliche Netze sind nach Möglichkeit zu verschlüsseln. Eine Verschlüsselung hat zwingend zu erfolgen, falls der Schutzbedarf der personenbezogenen Daten dies erfordert.

(7) Wartungsarbeiten an Systemen oder Telekommunikationseinrichtungen durch externe Dienstleister sind zu beaufsichtigen. Ferner ist zu gewährleisten, dass Dienstleister nicht unbefugt auf personenbezogene Daten zugreifen können. Fernwartungszugänge sind nur im Einzelfall zu gewähren und müssen dem Prinzip der minimalen Rechtevergabe folgen. Fernwartungsaktivitäten sind nach Möglichkeit aufzuzeichnen oder zu protokollieren.

§ 18 Datenschutz-Folgenabschätzung

(1) Die NAK Österreich ist zur Durchführung von Datenschutz-Folgenabschätzungen für Verfahren, die unter ihrer Verantwortung erfolgen, verpflichtet, wenn ein hohes Risiko für Rechte und Freiheiten von Betroffen aufgrund der Datenverarbeitung zu erwarten ist. Die Datenschutz-Folgenabschätzung enthält alle gesetzlich geforderten Beschreibungen des Art. 35 Abs. 7 DSGVO.

(2) Die Datenschutzbeauftragte berät die NAK Österreich bei der Durchführung der Datenschutz-Folgenabschätzung sowie bezüglich der Frage, wann Verarbeitungen ein hohes Risiko für betroffene Personen beinhalten können.

§ 19 Verletzungen des Schutzes von Daten („Datenpanne“)

(1) Sollten Daten der NAK Österreich oder einer Kirchengemeinde unrechtmässig Dritten offenbart worden sein, ist darüber unverzüglich der Kirchenpräsident der NAK Österreich und in Kopie der Leiter Administration BAB Schweiz zu informieren. Dieser bezieht unverzüglich den Datenschutzbeauftragten im Rahmen der Sachverhaltsaufklärung ein.

(2) Die Meldung hat alle relevanten Informationen zur Aufklärung des Sachverhalts zu umfassen, insbesondere die empfangende Stelle, die betroffenen Personen sowie Art und Umfang der übermittelten Daten.

(3) Die Erfüllung einer etwaigen Informationspflicht gegenüber der Datenschutzbehörde erfolgt ausschliesslich durch den Datenschutzbeauftragten im Einvernehmen mit dem Kirchenpräsidenten der NAK Österreich bzw. dessen gesetzlichen Vertreters und unter Information des Leiters Administration BAB Schweiz. Betroffene Personen werden durch die Kirchenleitung der NAK Österreich informiert, wobei der Datenschutzbeauftragte beratend hinzugezogen wird.

§ 20 Folgen von Verstössen

(1) Ein fahrlässiger oder gar mutwilliger Verstoss gegen diese Richtlinie kann arbeitsrechtliche Massnahmen nach sich ziehen, einschliesslich einer fristlosen oder fristgerechten Kündigung. Ebenso kommen strafrechtliche Sanktionen und zivilrechtliche Folgen wie Schadenersatz in Betracht.

§ 21 Rechenschaftspflicht

(1) Die Einhaltung der Vorgaben dieser Datenschutzrichtlinie muss jederzeit nachgewiesen werden können. Hierbei ist insbesondere auf die Nachvollziehbarkeit und Transparenz getroffener Massnahmen zu achten, so beispielsweise über zugehörige Dokumentationen.

§ 22 Aktualisierung der Richtlinie; Nachweisbarkeit

(1) Im Rahmen der Fortentwicklung des Datenschutzrechts sowie technologischer oder organisatorischer Veränderungen wird diese Datenschutzrichtlinie regelmässig auf einen Anpassungs- oder Ergänzungsbedarf hin überprüft.

(2) Änderungen an dieser Datenschutzrichtlinie sind formlos wirksam. Die Amtsträger, Funktionsträger und Beschäftigten der Administration NAK Österreich sind umgehend und in geeigneter Art und Weise über die geänderten Vorgaben in Kenntnis zu setzen.

§ 23 Schlussbestimmungen und Inkrafttreten

(1) Die vorliegende Datenschutzrichtlinie tritt am 1. März 2019 in Kraft.

Wien, 12. Februar 2019

Für die Neuapostolische Kirche Österreich:

Peter Jeram
Kirchenpräsident