Datenschutzrichtlinie der Neuapostolischen Kirche Norddeutschland (NAK Nord) mit den Gebietskirchen Bremen, Hamburg, Mecklenburg-Vorpommern und Schleswig-Holstein – jeweils Körperschaft des öffentlichen Rechts (nachfolgend Kirche genannt)[1]

Inhalt

§ 1 Zweck und Geltungsbereich

§ 2 Begriffsbestimmungen

§ 3 Datenerhebung

§ 4 Datenverarbeitung, -speicherung, -veränderung und –nutzung

§ 5 Datenübermittlung an kirchliche oder sonstige öffentliche Stellen

§ 6 Datenübermittlung an sonstige Stellen

§ 7 Datengeheimnis

§ 8 Gewährleistung des Datenschutzes

§ 9 Wartung

§ 10 Datenschutzbeauftragter

§ 11 Rechte der Betroffenen

§ 12 Anrufung des Beauftragten für den Datenschutz

§ 13 Auskunft

§ 14 Berichtigung, Löschung und Sperrung von Daten

§ 15 Schadensersatz

§ 16 Sanktionen

§ 17 Ergänzende Bestimmungen

§ 18 Inkrafttreten

Anlage zu § 2 (13)

---

1 In Anlehnung an den Entwurf einer einheitlichen Datenschutz-Richtlinie der Neuapostolischen Gebietskirchen in Deutschland (Stand: Juli 2010) in der Fassung vom 27. Dezember 2013

§ 1 Zweck und Geltungsbereich

(1) Zweck dieser Richtlinie ist der Schutz des Einzelnen vor einer Beeinträchtigung durch den Umgang mit seinen personenbezogenen Daten. Zweck dieser Richtlinie ist es ferner, die in kirchlichen Dateien enthaltenen personenbezogenen Daten vor Missbrauch zu schützen.

(2) Diese Richtlinie gilt für alle kirchlichen Einrichtungen sowie für die in der Kirchenverwaltung, in den Bezirken und in den Gemeinden tätigen Amtsträger und sonstigen kirchlichen Mitarbeiter und Mitarbeiterinnen (persönlicher Geltungsbereich).

(3) Diese Richtlinie gilt ferner für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die in Ziffer 2 bestimmten Stellen oder Personen (sachlicher Geltungsbereich), soweit nachfolgend nichts anderes bestimmt ist.

(4) Seelsorger, ehrenamtliche Helfer und Helferinnen oder sonstige Mitarbeiter und Mitarbeiterinnen der Kirche dürfen in Wahrnehmung ihres Auftrags eigene Aufzeichnungen führen und verwenden. Eigene Aufzeichnungen mit personenbezogenen Daten dürfen Dritten nicht zugänglich sein.

(5) Bestimmungen zur Schweigepflicht bleiben unberührt. Soweit Seelsorger in Ausübung ihrer seelsorgerischen Tätigkeit besondere Kenntnisse über persönliche Angelegenheiten Betroffener erhalten, unterliegen sie der Verpflichtung zur Verschwiegenheit.

§ 2 Begriffsbestimmungen

(1) Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

(2) Eine Datei ist

1. eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden kann (automatisierte Datei), oder

2. jede sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden kann (nichtautomatisierte Datei).
   Nicht hierzu gehören Akten und Aktensammlungen, es sei denn, dass sie durch automatisierte Verfahren umgeordnet und ausgewertet werden können.

(3) Eine Akte ist jede sonstige amtlichen oder dienstlichen Zwecken dienende Unterlage; dazu zählen auch Bild- und Tonträger. Nicht hierunter fallen Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen.

(4) Erheben ist das Beschaffen von Daten über den Betroffenen.

(5) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren:

1. Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung,

2. Verändern das inhaltliche Umgestalten gespeicherter personenbezogener Daten,

3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten (Empfänger) in der Weise, dass

   a. die Daten durch die speichernde Stelle an den Empfänger weitergegeben werden oder

   b. der Empfänger von der speichernden Stelle zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft,

4. Sperren das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung einzuschränken,

5. Löschen das Unkenntlichmachen gespeicherter personenbezogener Daten.

(6) Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.

(7) Anonymisieren ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

(8) Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Identifizierung der betroffenen Person auszuschließen oder wesentlich zu erschweren.

(9) Speichernde Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst speichert oder durch andere im Auftrag speichern lässt.

(10) Dritter ist jede Person oder Stelle außerhalb der speichernden Stelle. Dritte sind nicht der Betroffene sowie diejenigen Personen und Stellen, die im Geltungsbereich dieser Richtlinie personenbezogene Daten im Auftrag verarbeiten oder nutzen.

(11) Als Datenverarbeitungsanlagen (DV-Anlagen) gelten

1. vernetzte und nicht vernetzte Computer

2. tragbare Computer (etwa Notebooks, Laptops)

3. alle weiteren zur Verarbeitung von Daten nutzbaren Geräte.

(12) Datenverarbeitungsverfahren (DV-Verfahren) sind sämtliche im Rahmen kirchlicher Verwaltungstätigkeit genutzten und zur Benutzung freigegebenen Bearbeitungsmöglichkeiten von geschützten Daten.

(13) Im Übrigen gelten die Begriffsbestimmungen und zu treffenden Maßnahmen des Bundesdatenschutzgesetzes in der jeweils geltenden Fassung nach der Anlage zu dieser Richtlinie.

§ 3 Datenerhebung

(1) Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung kirchlicher Aufgaben der erhebenden Stelle erforderlich ist. Erhobene Daten dürfen rundsätzlich nur zu dem Zweck weiterverarbeitet werden, zu dem sie erhoben oder gespeichert worden sind.

(2) Personenbezogene Daten sind bei der betroffenen Person zu erheben. Ohne ihre Mitwirkung dürfen sie nur erhoben werden, wenn

1. eine kirchliche oder staatliche Rechtsvorschrift dies vorsieht oder

2. die Wahrnehmung des kirchlichen Auftrages die Erhebung erfordert und keine Anhaltspunkte dafür ersichtlich sind, dass überwiegende schutzwürdige Interessen verletzt werden, sofern

   a. die Erhebung bei der betroffenen Person einen unverhältnismäßigen Aufwand erforderte oder

   b. die betroffene Person einer bestehenden Auskunftspflicht nicht nachgekommen und über die beabsichtigte Erhebung der Daten unterrichtet worden ist.

(3) Werden personenbezogene Daten bei der betroffenen Person erhoben, so ist sie auf Verlangen über den Erhebungszweck, über die Rechtsvorschrift, die zur Auskunft verpflichtet, ansonsten auf die Freiwilligkeit ihrer Angaben hinzuweisen. Dies gilt nicht, wenn

1. die betroffene Person davon auf andere Weise Kenntnis erlangt hat,

2. die Unterrichtung einen unverhältnismäßig großen Aufwand erfordert oder

3. die Speicherung und Übermittlung der erhobenen Daten durch Rechtsvorschrift ausdrücklich vorgesehen ist.

(4) Werden personenbezogene Daten statt bei der betroffenen Person bei einer nichtkirchlichen oder nicht-öffentlichen Stelle erhoben, so ist die Stelle auf die Rechtsvorschrift, die zur Auskunft verpflichtet, ansonsten auf die Freiwilligkeit ihrer Angaben hinzuweisen.

(5) Bei der automatisierten Verarbeitung personenbezogener Daten sind die in der Anlage zu dieser Richtlinie genannten Maßnahmen zum Schutz personenbezogener Daten zu treffen, soweit ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

§ 4 Datenverarbeitung, -speicherung, -veränderung und –nutzung

(1) Die Verarbeitung personenbezogener Daten ist nur zulässig, wenn diese Richtlinie oder eine andere Rechtsvorschrift sie gestattet oder anordnet oder eine Einwilligung der betroffenen Person vorliegt.

(2) Im Falle der eingeholten Einwilligung ist die betroffene Person auf den Zweck der Maßnahme und einer vorgesehenen Übermittlung hinzuweisen.

(3) Das Speichern, Verändern oder Nutzen ist im Übrigen nur zulässig, wenn

1. offensichtlich ist, dass es im Interesse der betroffenen Person liegt und kein Grund zu der Annahme besteht, dass sie in Kenntnis des Zwecks ihre Einwilligung verweigern würde,

2. Angaben der betroffenen Person überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,

3. die Daten aus allgemein zugänglichen Quellen entnommen werden können oder die speichernde kirchliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse der betroffenen Person offensichtlich überwiegt,

4. Grund zu der Annahme besteht, dass anderenfalls die Wahrnehmung des kirchlichen Auftrags gefährdet würde oder

5. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist.

(4) Die Speicherung, Verarbeitung und Nutzung personenbezogener Daten wird von der Kirche in eigener Verantwortung durchgeführt. Die Speicherung, Verarbeitung und Nutzung personenbezogener Daten durch andere Stellen oder Personen, insbesondere eine Auftragsdatenverarbeitung, findet nicht statt.

(5) Ein automatisiertes Verfahren, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, ist zulässig, soweit dies zur Erstellung von Listen und Briefen aus dem NAK-Portal heraus erforderlich ist und schutzwürdige Interessen der Betroffenen nicht entgegenstehen.

Ein Abspeichern oder Weiterleiten der in der Zwischenablage befindlichen personenbezogenen Daten ist nicht zulässig. Der temporäre Speicher ist unmittelbar nach Durchführung der notwendigen Arbeitsschritte wieder zu löschen.

Um die Einhaltung des Datenschutzes zu gewährleisten, halten die zuständigen MDV-Beauftragten in einer maschinell zu führenden Datei fest, wann sie für welche Maßnahme welche personenbezogenen Daten zur weiteren Nutzung temporär geladen hatten.

Auf Anforderung des Präsidenten bzw. des Datenschutzbeauftragten ist diese Datei durch Weiterleitung zur Verfügung zu stellen. Dass soll – zum Schutz der MDV-Beauftragten – auch anlassbezogene Prüfungen ermöglichen.

Die Datei ist während der gesamten Zeit der Beauftragung fortzuschreiben und elektronisch zu archivieren. Bei Beendigung der Beauftragung ist die Datei in jedem Falle an den Datenschutzbeauftragten weiterzuleiten.

§ 5 Datenübermittlung an kirchliche oder sonstige öffentliche Stellen

(1) Die Übermittlung von personenbezogenen Daten an kirchliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden oder der empfangenden kirchlichen Stelle liegenden Aufgaben erforderlich ist und

2. die Zulässigkeitsvoraussetzungen des § 4 vorliegen.

(2) Verantwortlich für die Zulässigkeit der Übermittlung ist die übermittelnde kirchliche Stelle. Erfolgt die Übermittlung auf Ersuchen der empfangenden kirchlichen Stelle, trägt diese die Verantwortung. In diesem Falle prüft die übermittelnde kirchliche Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben der Daten empfangenden kirchlichen Stelle liegt, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht.

(3) Die Daten empfangende kirchliche Stelle darf die übermittelten Daten für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihr übermittelt werden. Eine Verarbeitung oder Nutzung für andere Zwecke ist nur unter den Voraussetzungen des § 4 zulässig.

(4) Sind mit personenbezogenen Daten, die nach Absatz 1 übermittelt werden dürfen, weitere personenbezogene Daten der betroffenen oder einer anderen Person in Akten so verbunden, dass eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, so ist die Übermittlung auch dieser Daten zulässig, soweit nicht berechtigte Interessen der betroffenen oder einer anderen Person an deren Geheimhaltung offensichtlich überwiegen; eine Nutzung dieser Daten ist unzulässig.

(5) Absatz 4 gilt entsprechend, wenn personenbezogene Daten innerhalb der Kirche weitergegeben werden.

§ 6 Datenübermittlung an sonstige Stellen

(1) Die Übermittlung von personenbezogenen Daten an sonstige Stellen oder Personen ist zulässig, wenn

1. personenbezogene Daten an Behörden und sonstige öffentliche Stellen des Bundes, der Länder und der Gemeinden und der sonstigen Aufsicht des Bundes oder eines Landes unterstehenden juristischen Personen des öffentlichen Rechts übermittelt werden, wenn das zur Erfüllung der kirchlichem Aufgaben erforderlich ist und

2. die Daten empfangenden Stellen oder Personen ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegen und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, es sei denn, dass der Grund zu der Annahme besteht, dass durch die Übermittlung die Wahrnehmung des Auftrags der Kirche gefährdet würde.

(2) Verantwortlich für die Zulässigkeit der Übermittlung ist die übermittelnde kirchliche Stelle.

(3) In den Fällen der Übermittlung nach Abs. 1 Nr. 2 unterrichtet die übermittelnde kirchliche Stelle die betroffene Person von der Übermittlung ihrer Daten, es sei denn, es ist damit zu rechnen, dass sie davon auf andere Weise Kenntnis erlangt.

(4) Die Daten empfangenden Stellen und Personen dürfen die übermittelten Daten nur für den Zweck verarbeiten oder nutzen, zu dessen Erfüllung sie ihnen übermittelt werden. Zur Sicherstellung hat die übermittelnde Stelle sie darauf zu verpflichten.

§ 7 Datengeheimnis

(1) Personenbezogene Daten in Dateien der Kirche sind bei der Datenverarbeitung vor Missbrauch zu schützen.

(2) Den bei der Datenverarbeitung beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten oder zu nutzen (Datengeheimnis). Diese Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis schriftlich zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

§ 8 Gewährleistung des Datenschutzes

(1) Kirchliche Stellen, die personenbezogene Daten verarbeiten, haben die technischen, personellen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung dieser Richtlinie zu gewährleisten. Die Angemessenheit der Maßnahmen bemisst sich an dem Verhältnis von Aufwand zu dem angestrebten Schutzzweck. Die Maßnahmen haben dem Stand der Technik zu entsprechen.

(2) Die mit der Datenverarbeitung Beauftragten sind verpflichtet, Arbeitsmittel und Datenträger so aufzubewahren, dass sie dem Zugriff Unbefugter entzogen sind.

(3) Der Kirchenpräsident ist verantwortlich für die Einhaltung des Datenschutzes und veranlasst die in Ausführung dieser Richtlinien erforderlichen Maßnahmen.

(4) Er hat dafür zu sorgen, dass die für die Verarbeitung von personenbezogenen Daten eingerichteten DV-Systeme ordnungsgemäß funktionieren (vgl. § 9). Hierzu ist ein Systembetreuer zu bestellen.

(5) Veränderungen an Datenverarbeitungsanlagen in kirchlichen Verwaltungsstellen dürfen nur im Einvernehmen mit dem Systembetreuer vorgenommen werden. Dies gilt insbesondere für das Öffnen der Geräte, den Einbau zusätzlicher Steckkarten oder die Installation von Software.

§ 9 Wartung

(1) Datenverarbeitungssysteme sind so zu gestalten, dass bei ihrer Wartung möglichst nicht auf personenbezogene Daten zugegriffen werden kann. Sofern dies nicht sichergestellt ist, hat die datenverarbeitende Stelle durch technische und organisatorische Maßnahmen sicherzustellen, dass nur auf die für die Wartung unbedingt erforderlichen personenbezogenen Daten zugegriffen werden kann. Dabei ist:

1. sicherzustellen, dass nur dafür autorisiertes Personal die Wartung vornimmt,

2. sicherzustellen, dass jeder Wartungsvorgang nur mit Wissen und Wollen der speichernden Stelle erfolgen kann,

3. zu verhindern, dass personenbezogene Daten im Rahmen der Wartung unbefugt entfernt oder übertragen werden,

4. sicherzustellen, dass alle Wartungsvorgänge während der Durchführung kontrolliert werden können,

5. sicherzustellen, dass alle Wartungsvorgänge nach der Durchführung nachvollzogen werden können,
6. zu verhindern, dass bei der Wartung Programme unbefugt aufgerufen werden können, die für die Wartung nicht benötigt werden,

7. zu verhindern, dass bei der Wartung Datenverarbeitungsprogramme unbefugt verändert werden können, und

8. die Wartung so zu organisieren und zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird.

(2) Eine Wartung der in der Verwaltung befindlichen Datenverarbeitungsanlagen durch andere Stellen darf über die Anforderungen nach Absatz 1 hinaus nur auf Grund schriftlicher Vereinbarungen erfolgen. Darin sind folgende Regelungen zu treffen:

1. Art und Umfang der Wartung,

2. Abgrenzung der Rechte und Pflichten zwischen Auftraggeber und Auftragnehmer,

3. eine Protokollierungspflicht beim Auftraggeber und die Verpflichtung des Auftragnehmers, Weisungen des Auftraggebers zum Umgang mit den Daten auszuführen und sich an dessen Weisungen zu halten,

4. Regelung, dass die Daten ausschließlich für den Zweck der Wartung verwendet werden dürfen,

5. Sicherstellung, dass keine Datenübermittlung an andere Stellen durch den Auftragnehmer erfolgt,

6. Löschung der für den Zweck der Wartung verwendeten Daten nach Abschluss der Wartungsarbeiten,

7. Sicherstellung der Anwesenheit des Systembetreuers.

(3) Die mit Wartungsarbeiten betrauten Personen sind zur Wahrung des Datengeheimnisses zu verpflichten.

(4) Ist bei Wartungsarbeiten nur ein Zugriff auf Daten in verschlüsselter, pseudonymisierter oder anonymisierter Form gegeben, so dass seitens der mit der Wartung betrauten Stelle eine Reidentifizierung von Betroffenen nicht möglich ist, sind nur Maßnahmen nach Absatz 2 erforderlich. Ein Zugriff darf nur zweckgebunden erfolgen.

(5) Im Sinne dieser Richtlinie ist

1. Wartung die Summe der Maßnahmen zur Sicherstellung der Verfügbarkeit und Integrität der Hard- und Software von Datenverarbeitungsanlagen; dazu gehören die Installation, Pflege, Überprüfung und Korrektur der Software sowie Überprüfung und Reparatur oder Austausch von Hardware,

2. Fernwatung die Wartung der Hard- und Software von Datenverarbeitungsanlagen, die von einem Ort außerhalb der Stelle, bei der die Verarbeitung von personenbezogenen Daten erfolgt mittels Einrichtung zur Datenübertragung vorgenommen wird, und

3. Verschlüsselung das Ersetzen von Klartextbegriffen oder Zeichen durch andere in der Weise, dass der Klartext nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft wieder lesbar gemacht werden kann.

§ 10 Datenschutzbeauftragter

(1) Der Kirchenpräsident bestellt für einen Zeitraum von fünf Jahren einen Datenschutzbeauftragten/eine Datenschutzbeauftragte (nachfolgend: Datenschutzbeauftragter). Wiederbestellung ist zulässig. Nach dem Ende der Amtszeit bleibt der Datenschutzbeauftragte auf Aufforderung des Kirchenpräsidenten bis zur Ernennung eines Nachfolgers im Amt. Bei Vorliegen eines wichtigen Grundes kann der Kirchenpräsident den Datenschutzbeauftragten vorzeitig abberufen.

(2) Die Bestellung kann ehrenamtlich oder auch hauptberuflich erfolgen.

(3) Die Bestellung, Wiederbestellung, Neubestellung und Abberufung des Datenschutzbeauftragten ist in der Kirche in einer Weise bekannt zu machen, die es jedem ermöglicht, jederzeit Kenntnis über die Person des aktuell bestellten Datenschutzbeauftragten zu erlangen.

(4) Zum Datenschutzbeauftragten darf nur bestellt werden, wer die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzt. Der Datenschutzbeauftragte ist auf die gewissenhafte Erfüllung der Amtspflichten und die Einhaltung der kirchlichen Ordnungen schriftlich zu verpflichten.

(5) Der Datenschutzbeauftragte wacht über die Einhaltung der Vorschriften über den Datenschutz in eigener Verantwortlichkeit. Der Datenschutzbeauftragte untersteht direkt dem Kirchenpräsidenten. Er ist in Ausübung seines Amtes an Weisungen nicht gebunden und nur dem geltenden Recht unterworfen.

(6) Er erhält für die Erfüllung seiner Aufgaben die notwendige Ausstattung. Datenverarbeitende Stellen und Personen sind bei datenschutzrelevanten Fragen zur Auskunftserteilung gegenüber dem Datenschutzbeauftragten verpflichtet.

(7) Der Datenschutzbeauftragte ist in Ausübung seiner Tätigkeit befugt, Einsicht zu nehmen in die kirchlichen Unterlagen und Akten, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen, insbesondere in die gespeicherten Daten und Datenverarbeitungsprogramme. Er ist berechtigt, die datenführenden Stellen und Personen jederzeit aufzusuchen. Sie sind ihm gegenüber zur Auskunft verpflichtet über Fragen, die der Erfüllung der Aufgabe dienen.

(8) Er ist verpflichtet, regelmäßig „Datenschutz-Checks“ durchzuführen und darüber dem Kirchenpräsidenten unaufgefordert zu berichten und erstellt darüber hinaus einen

Jahresbericht.

(9) Aufgabe des Datenschutzbeauftragten ist es ebenfalls sicherzustellen, dass keine nicht zulässigen Daten geführt werden. Dazu gehören insbesondere Daten mit personenbezogenem Inhalt, die dem

1. Beicht- und Seelsorgegeheimnis unterliegen,

2. Post- und Fernmeldegeheimnis unterliegen,

3. Arztgeheimnis unterliegen,

(10) Der Datenschutzbeauftragte berät den Kirchenpräsidenten in Angelegenheiten des Datenschutzes und erstattet auf dessen Anforderung Gutachten und Berichte. Er kann Empfehlungen für die Verbesserung des Datenschutzes abgeben und ist verpflichtet, Verstöße gegen die Datenschutzbestimmungen schriftlich zu beanstanden. Der Kirchenpräsident soll in angemessener Frist die Maßnahmen darstellen, die auf Grund der Beanstandungen des Datenschutzbeauftragten getroffen wurden.

(11) Der Datenschutzbeauftragte ist verpflichtet, Register über automatisiert geführte Dateien zu führen. Das Register kann von jeder Person, die ein berechtigtes Interesse nachweist, eingesehen werden.

(12) Der Datenschutzbeauftragte ist entsprechend den für Amtsträger geltenden Vorschriften zur Verschwiegenheit verpflichtet. Die Verschwiegenheitspflicht besteht nach Beendigung der Beauftragung fort. Äußerungen über Angelegenheiten, die der Verschwiegenheit unterliegen, dürfen nur mit Genehmigung des Kirchenpräsidenten abgegeben werden. Die Verschwiegenheitspflicht gilt nicht für Mitteilungen im dienstlichen Verkehr oder in Bezug auf Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Der Datenschutzbeauftragte darf, auch wenn er nicht mehr im Amt ist, über Angelegenheiten, die der Schweigepflicht unterliegen, ohne Genehmigung des Kirchenpräsidenten weder vor Gericht noch außergerichtlich vor anderen Stellen Erklärungen abgeben.

(13) Stellt der Datenschutzbeauftragte Verstöße gegen die Vorschriften dieser Richtlinie oder gegen andere Datenschutzvorschriften oder sonstige Mängel bei der Verarbeitung personenbezogener Daten fest, so beanstandet er dieses gegenüber dem Kirchenpräsidenten und fordert die datenverarbeitende Stelle, die Anlass zu der Beanstandung gegeben hatte zur Stellungnahme innerhalb einer von ihm zu bestimmenden Frist auf.

(14) Der Datenschutzbeauftragte kann von einer Beanstandung absehen oder auf eine Stellungnahme der betroffenen Stelle verzichten, wenn es sich um unerhebliche Mängel handelt.

(15) Mit der Beanstandung kann der Datenschutzbeauftragte Vorschläge zur Beseitigung der Mängel und zur sonstigen Verbesserung des Datenschutzes verbinden.

(16) Wird dem Mangel nicht hinreichend abgeholfen, so ist der Datenschutzbeauftragte verpflichtet, sich an den Kirchenpräsidenten zu wenden und zu berichten.

§ 11 Rechte der Betroffenen

(1) Die sich aus dieser Richtlinie ergebenden Rechte der betroffenen Personen können nicht durch Rechtsgeschäfte ausgeschlossen oder beschränkt werden. Eingaben von betroffenen Personen sind an den Datenschutzbeauftragten weiterzuleiten.

(2) Weitergehende Rechte ergeben sich aus den nachfolgenden Bestimmungen.

§ 12 Anrufung des Beauftragten für den Datenschutz

Jede Person kann sich an den Datenschutzbeauftragten wenden, wenn sie der Ansicht ist, bei der Erhebung, Verarbeitung oder Nutzung ihrer personenbezogenen Daten durch kirchliche Stellen in ihren Rechten verletzt worden zu sein.

§ 13 Auskunft

(1) Jedem ist auf Antrag Auskunft zu erteilen

1. über die zu seiner Person bei kirchlichen Stellen gespeicherten Daten, auch soweit sie sich auf Herkunft oder empfangende Stellen dieser Daten beziehen, und

2. über den Zweck der Speicherung.

(2) Die speichernde Stelle bestimmt das Verfahren, insbesondere die Form der Auskunftserteilung nach pflichtgemäßem Ermessen.

(3) Auskunft kann nicht erteilt werden, wenn die Daten oder die Tatsache ihrer Speicherung geheim gehalten werden müssen und das Interesse der betroffenen Person dahinter zurücktreten muss. Auskunft kann ferner nicht erteilt werden, wenn durch die Auskunft die Wahrnehmung des Auftrags der Kirche gefährdet wird.

(4) Die Auskunft ist unentgeltlich.

§ 14 Berichtigung, Löschung und Sperrung von Daten

(1) Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind. Wird festgestellt, dass personenbezogene Daten unrichtig sind oder wird ihre Richtigkeit von der betroffenen Person bestritten, so ist dies aktenkundig zu machen oder auf sonstige Weise festzuhalten.

(2) Personenbezogene Daten in Dateien sind zu löschen, wenn

1. ihre Speicherung unzulässig war oder

2. ihre Kenntnis für die speichernde Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist.

(3) An die Stelle einer Löschung tritt eine Sperrung, soweit und solange

1. einer Löschung Rechtsvorschriften oder vertragliche Aufbewahrungsfristen entgegenstehen,

2. Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen der betroffenen Personen beeinträchtigt würden, oder

3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist.

(4) Personenbezogene Daten in Dateien sind ferner zu sperren, soweit ihre Richtigkeit von der betroffenen Person bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt.

(5) Personenbezogene Daten in Akten sind zu sperren, wenn die kirchliche Stelle im Einzelfall feststellt, dass ohne die Sperrung schutzwürdige Interessen der betroffenen Person beeinträchtigt würden und die Daten für die Aufgabenerfüllung nicht mehr erforderlich sind.

§ 15 Schadensersatz

(1) Fügt eine datenverarbeitende Stelle der betroffenen Person durch eine nach den Vorschriften dieser Richtlinie oder nach anderen kirchlichen Vorschriften über den Datenschutz unzulässige oder unrichtige automatisierte Verarbeitung ihrer personenbezogenen Daten einen Schaden zu, ist sie der betreffenden Person zum Ersatz des daraus resultierenden Schadens verpflichtet. Bei einer schweren Verletzung des Persönlichkeitsrechts ist der betroffenen Person der Schaden, der nicht Vermögensschaden ist, angemessen in Geld zu ersetzen. Die Betroffene Person ist für den Eintritt des Schadens sowie die Kausalität darlegungs- und beweispflichtig.

(2) Die Ansprüche nach Absatz 1 sind insgesamt bis zu einem Betrag in Höhe von 50.000,00 Euro begrenzt. Ist aufgrund desselben Ereignisses an mehrere Personen Schadensersatz zu leisten, der insgesamt den Höchstbetrag von 50.000,00 Euro übersteigt, so verringern sich die einzelnen Schadensersatzleistungen in dem Verhältnis, in dem ihr Gesamtbetrag zum Höchstbetrag steht.

(3) Sind bei einer automatisierten Verarbeitung mehrere Stellen speicherungsberechtigt und ist die geschädigte Person nicht in der Lage, die speichernde Stelle festzustellen, so haftet jede dieser Stellen.

(4) Mehrere Ersatzpflichtige haften als Gesamtschuldner im Sinne des Bürgerlichen Gesetzbuches.

(5) Auf das Mitverschulden der betroffenen Person ist § 254 und auf die Verjährung sind die §§ 199, 852 des Bürgerlichen Gesetzbuches entsprechend anzuwenden.

(6) Vorschriften, nach denen Ersatzpflichtige in weiterem Umfang als nach dieser Vorschrift haften oder nach denen andere für den Schaden verantwortlich sind, bleiben unberührt.

(7) Werden mit dem Erheben, Verarbeiten oder Nutzen von personenbezogenen Daten Personen betraut, die diese Aufgabe ehrenamtlich erfüllen, entfällt außer bei

vorsätzlichen Handeln und grober Fahrlässigkeit eine Haftung. Eine Haftung der Kirche bleibt davon unberührt.

§ 16 Sanktionen

(1) Wer unbefugt personenbezogene Daten, die nicht offenkundig sind,

1. übermittelt oder verändert oder

2. sich aus in Behältnissen verschlossenen Dateien verschafft, wird je nach Schwere der Tat und dem Maß des Verschuldens abgemahnt oder von seinem kirchlichen Amtsauftrag beurlaubt oder von seiner kirchlichen Beauftragung entbunden. Für die Entscheidung zuständig ist der Kirchenpräsident.

(2) Handelt der Täter gegen Entgelt oder in der Absicht, sich oder einen anderen zu bereichern oder einen anderen zu schädigen, so erfolgt die fristlose Kündigung des Arbeits- oder Dienstverhältnisses, bzw. die sofortige Amtsentlassung. (3) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt ist die betroffene Person sowie der kirchliche Datenschutzbeauftragte. Die Kirchenleitung kann auch aus eigener Entscheidung tätig werden.

§ 17 Ergänzende Bestimmungen

Der Kirchenpräsident kann zur Durchführung, wie auch zur Ergänzung dieser Richtlinie, insbesondere im Hinblick auf technikunterstützte Verfahren der Datenverarbeitung und zur Datensicherung weitere Bestimmungen erlassen, die jeweils in Form einer Anlage zu dieser Richtlinie gefasst werden.

§ 18 Schlussbestimmung, Inkrafttreten

Änderungen oder Ergänzungen dieser Richtlinie bedürfen der Schriftform. Diese Richtlinie tritt mit der Unterzeichnung und anschließenden Bekanntmachung durch den Kirchenpräsidenten (Bezirksapostel) in Kraft.

Anlage zu § 2 (13) der Datenschutzrichtlinie der NAK Nord in Anlehnung an die Anlage zu § 9 Satz 1 des Bundesdatenschutzgesetzes

Werden personenbezogene Daten automatisiert verarbeitet, sind Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind,

(1) Unbefugten den Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren (Zugangskontrolle),

(2) zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können (Datenträgerkontrolle),

(3) die unbefugte Eingabe in den Speicher sowie die unbefugte Kenntnisnahme, Veränderung oder Löschung gespeicherter personenbezogener Daten zu verhindern (Speicherkontrolle),

(4) zu verhindern, dass Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können (Benutzerkontrolle),

(5) zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können (Zugriffskontrolle),

(6) zu gewährleisten, dass überprüft und festgestellt werden kann, an welchen Stellen personenbezogene Daten durch Einrichtungen zur Datenübertragung übermittelt werden können (Übermittlungskontrolle),

(7) zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle),

(8) zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),

(9) zu verhindern, dass bei der Übertragung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können (Transportkontrolle),

(10) die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird (Organisationskontrolle).

Neuapostolische Kirche

Verpflichtungserklärung betreffend Datenschutz

Gemeinde: _____

Vor- und Familienname: _____

Straße, Hausnummer: _____

PLZ, Wohnort: _____

Telefonnummer: _____

Private Mail-Adresse für die
Nutzung im NAK-Portal: _____

Im Rahmen meiner Tätigkeit als _____*)

in der Neuapostolischen Kirche habe ich Zugang zu personenbezogenen Daten.

Ich verpflichte mich hiermit, die Datenschutzrichtlinie der Neuapostolischen Kirche in der jeweils gültigen Fassung einzuhalten.

Ich verpflichte mich insbesondere, über personenbezogene Daten Stillschweigen zu bewahren und diese nicht Dritten zugänglich zu machen. Dies gilt auch für die Zeit nach meinem Ausscheiden aus dieser Tätigkeit.

Ich verpflichte mich ferner, die mir zugänglich gemachten Daten einschließlich sämtlicher Kopien im Falle des Ausscheidens aus meiner Tätigkeit der Neuapostolischen Kirche vollständig zu übergeben.

_____
Datum

_____
Unterschrift des/der Verpflichteten

*) z.B. Amtsträger, MDV-Beauftragter, Kirchenbuchführer, Lehrkräfte…

Verteiler: - ein Exemplar an die/den Verpflichtete/n
- ein Exemplar an die Kirchenverwaltung