KATHOLISCHE PFARREI
HEILIGER MARTIN

Stand: 01.06.2020, Version 1.0

Katholische Pfarrei Hl. Martin

Richtlinie zum Datenschutz der Pfarrei

Die nachfolgenden Bestimmungen sollen sicherstellen, dass alle Abläufe in unserer Pfarrei den Vorgaben des Kirchlichen Datenschutzrechts entsprechen. Maßgeblich sind hier vor allem die Bestimmungen des **Kirchlichen Datenschutzgesetzes (KDG)**.

Diese Dienstanweisung ist für alle in der Pfarrei Tätigen verbindlich, also auch für diejenigen die ehrenamtlich für die Pfarrei tätig sind oder diejenigen, die beim Bistum angestellt sind.

Der sorgfältige und datenschutzgerechte Umgang mit Personendaten ist wichtig, um das Ansehen von Pfarrei und Kirche zu schützen. Datenschutz betrifft jede Tätigkeit für die Pfarrei, bei der Daten von Personen verwendet werden (bspw. Adresslisten oder Anmeldeformulare).

Datenschutz fängt daher bei jedem einzelnen von uns an. Daher bitten wir Sie, die nachfolgenden Bestimmungen zu beachten, wenn Sie mit Personendaten umgehen. Für Ihre Unterstützung bei der Umsetzung des Datenschutzrechts bedanken wir uns herzlich.

Sofern Unklarheiten bestehen, unterstützen wir Sie selbstverständlich gerne. Setzen Sie sich hierzu mit uns unter **Tel.: 0 41 21 / 26 27 90-0, E-Mail:** gemeindebuero.elmshorn@pfarreihlmartin.de in Verbindung.

Herzlichst
Ihr Pfarrer Stefan Langer

Inhaltsverzeichnis

1. Organisation der Pfarrei

1.1. Zutrittsregelung

1.1.1. Schlüsselvergabe

Alle für die Pfarrei Tätigen erhalten die für die jeweilige Tätigkeit erforderlichen Schlüssel zu den einzelnen Büros und Gemeindebüros oder den übrigen Räumlichkeiten der Pfarrei. Es sollen nur die Schlüssel ausgegeben werden, die der einzelne für seine Arbeit tatsächlich benötigt. Die Ausgabe und Rücknahme der Schlüssel werden schriftlich in den Gemeindebüros (Ausnahme Uetersen: bei der KiTa-Leitung) dokumentiert.

1.1.2. Schließregelung

Wichtig: Die Person, die das Büro zuletzt verlässt muss das Büro abschließen.

1.1.3. Diskretion

Wichtig: Es dürfen sich keine Personen (Besucher, Handwerker, Ehrenamtliche) unbegleitet in den Räumlichkeiten der Pfarrei aufhalten, sofern ein Zugriff auf Personendaten möglich ist (bspw. unbeaufsichtigte Handwerksarbeiten im Archiv).

Sofern sich mehrere Personen im Büro (Besucher, Handwerker) aufhalten oder wenn Sie in Anwesenheit eines anderen telefonieren, ist sicherzustellen, dass Dritte keine Kenntnis vom Inhalt persönlicher Gespräche erlangen. Bei vertraulichen Gesprächen bitten Sie Dritte, das Büro für die Dauer des Gesprächs zu verlassen.

1.1.4. Beginn/Beendigung Tätigkeit in der Pfarrei

Bei Beginn oder Beendigung einer ehrenamtlichen oder hauptamtlichen Tätigkeit in der Pfarrei ist der **Ablaufplan** im **Anhang 1** zu dieser Dienstanweisung zu beachten.

1.2. Organisation des Arbeitsplatzes

1.2.1. Bildschirm

Der Bildschirm muss so ausgerichtet sein, dass der Bildschirminhalt des Arbeitsplatzcomputers weder für Besucher des Büros oder durch das Fenster sichtbar ist. Der Bildschirm sollte bei kurzfristigem Verlassen des Arbeitsplatzes (Microsoft-Taste & L-Taste gleichzeitig betätigen) gesperrt werden; bei längerfristigem Verlassen des Büros ist der Computer herunterzufahren.

1.2.2. Dokumente mit personenbezogenen Daten

Solche Dokumente wie bspw. ausgedruckte Adresslisten, Anschreiben, ausgefüllte Anmeldeformulare sind so zu verwahren, dass sie für unbefugte Dritte (bspw. Besucher, Handwerker) nicht einsehbar sind. Sie sollten in Schränken unter Verschluss gehalten werden.

1.2.3. Personalakten

Diese sind grundsätzlich in einem verschlossenen Schrank zu verwahren, auf den nur der Pfarrer und diejenigen, die zur Einsicht befugt sind, Zugriff haben.

1.2.4. Datenverarbeitung

Dienstliche Dateien sollen nach Möglichkeit nicht lokal auf privaten Computern gespeichert werden. Es ist daher stets zu prüfen, ob eine Speicherung von Daten für die Erledigung der konkreten Aufgabe tatsächlich erforderlich ist. Besteht dieses Erfordernis, dann sollten die (bearbeiteten) Daten auf

einem (verschlüsselten) USB-Stick gespeichert werden. Sofern dienstliche Daten lokal auf dem privaten Rechner gespeichert wurden, sind diese unverzüglich zu löschen, sobald sie nicht mehr benötigt werden.

Der private Computer, der für Aufgaben der Pfarrei (Gremien- oder Gruppenarbeit) genutzt wird, muss mit einem Virenscanner und einer Firewall ausgestattet sein. Diese Software ist auf dem neusten Stand zu halten und stets zu verwenden.

1.3. Technische Geräte

1.3.1. Dienstliche Nutzung von privaten Kommunikationsmitteln und IT-Arbeitsmitteln

Wichtig: Die dienstliche Nutzung privater Kommunikationsmittel oder IT-Systeme (Arbeitsplatzcomputer, Datenträger wie USB-Sticks, E-Mail, Internet, Fax, Telefon) ist grundsätzlich nicht zulässig.

Ausnahmeregelung muss schriftlich erfolgen.

Im Hinblick auf die ehrenamtliche Tätigkeit, insbesondere in den Gremien der Pfarrei, ist die Nutzung privater IT-Systeme durch die Pfarrei (Homeoffice) gestattet, soweit dies für die Aufgabenerledigung erforderlich oder sinnvoll ist. Bitte beachten Sie die unter **Punkt 2.1** genannten Maßnahmen zur Sicherung des Heimarbeitsplatzes.

1.3.2. Private Nutzung von Systemen der Pfarrei

Wichtig: Die private Nutzung dienstlicher Kommunikationsmittel/IT-Systeme ist ebenfalls unzulässig, es sei denn, persönliche Erfordernisse machen dies notwendig.

1.4. Software

1.4.1. Kennwortregelung

Ihr PC muss kennwortgeschützt sein. Die von Ihnen verwendeten Kennworte müssen folgende Anforderungen erfüllen:

- Länge mindestens 8 Zeichen
- groß und klein geschriebene Buchstaben,
- Zahlen und Sonderzeichen enthalten.

Bitte wechseln Sie das Kennwort regelmäßig.

Wenn Sie sich das Kennwort aufschreiben, verwahren Sie es an einem sicheren Ort. Zur Sicherheit sollten schriftlich notierte Kennworte zusätzlich in einem geschlossenen Briefumschlag aufbewahrt werden. So ist erkennbar, ob Unbefugte Kenntnis vom Kennwort erlangt haben.

Bitte teilen Sie Ihre Kennworte keinen Dritten mit.

1.4.2. Nutzung e-mip

Kennzeichnungen im elektronischen Gemeindemitgliederverzeichnis „e-mip“ sind hilfreich, um innerhalb der Pfarrei Gruppen zu organisieren. Kennzeichnungen und Angaben in Freitextfelder sind nur zur Erfüllung von Aufgaben der Pfarrei zulässig. Sie sind auf das notwendige Maß zu beschränken.

1.4.3. Cloud-Lösungen

In der Pfarrei werden zwei Cloud-Lösungen erlaubt: Datenserver der Pfarrei in Pinneberg und Datenserver des Erzbistums Hamburg „Ecclesias“.

2. Tätigkeit im Ehrenamt

2.1. Organisation des Heimarbeitsplatzes

2.1.1. Akten unter Verschluss

Die Mitnahme von Akten/Schriftstücken der Pfarrei in die häusliche Umgebung ist nur dann zulässig, wenn diese Unterlagen für die Erledigung von Aufgaben der Pfarrei erforderlich sind. In diesem Fall muss sichergestellt sein, dass die Akten sicher verwahrt und vor dem Zugriff unbefugter Dritter (auch Familienangehörige, Haushaltsmitglieder) geschützt sind, etwa indem sie in einem Schrank unter Verschluss gehalten werden.

2.1.2. Nutzung E-Mail

Auf die Veröffentlichung von E-Mail-Adressen, die sich nicht auf die Domäne der Pfarrei oder eines Dienstleisters, der den Mail-Server im Auftrag der Pfarrei administriert, beziehen, ist zu verzichten. Dies gilt insbesondere für private E-Mail-Adressen von Ehrenamtlichen bzw. Gremienmitgliedern. Hierdurch soll vermieden werden, dass Dritte Angelegenheiten der Pfarrei über die private E-Mail-Adresse kommunizieren. Andernfalls besteht die Gefahr, dass an diese Adressen auch dann noch Nachrichten mit Angelegenheiten der Pfarrei versandt werden, wenn der Adressinhaber nicht mehr für die Pfarrei aktiv ist.

Sofern keine dienstliche E-Mail-Adresse eingerichtet werden kann, ist es vertretbar, dass eingehende E-Mails durch die ehrenamtlichen und hauptamtlichen Mitarbeiter der Pfarrei weitergeleitet werden. Diese Möglichkeit erschöpft sich jedoch auf die E-Mail-Accounts, deren Anbieter ihren Sitz und die E-Mail-Server in der EU/dem EWR haben. Unzulässig ist unter anderem die Verwendung der Dienste von Google, Apple und Microsoft.

2.1.3. Nutzung USB-Stick

Nach Möglichkeit sollten keine personenbezogenen Daten der Pfarrei auf mobilen Datenträgern (bspw. USB-Stick) gespeichert werden.

Wichtig: Sofern die Speicherung von Daten auf einem USB-Stick für die sachgerechte Aufgabenerledigung erforderlich ist, sind diese Daten auf dem Datenträger nach Möglichkeit zu verschlüsseln.

Dies gilt insbesondere dann, wenn der USB-Stick zur Weitergabe von Daten an Dritte verwendet werden soll. Eigene USB-Sticks dürfen aus Gründen der Datensicherheit nur nach Rücksprache mit Verantwortlichen (Pfarrei) verwendet werden.

Hier bestehen zwei Möglichkeiten: Entweder wird der gesamte Datenträger verschlüsselt (bspw. Datenträgerverschlüsselung mit „VeraCrypt“) oder nur die auf dem Datenträger gespeicherten Dateien.

Einzelne Dateien Daten können entweder in Form eines

- ZIP-Archivs mit der Software „7Zip“,
- PDF mit der Software „PDFCreator“ oder
- Sie versehen das Office-Dokument bei der Speicherung mit einem Kennwort (unter Tools/Allgemeine Optionen).

Es sollte immer der Verschlüsselungsstandard „AES256“ gewählt werden, mindestens aber „AES128“.

Bitte teilen Sie dem Empfänger des Datenträgers das Kennwort persönlich oder telefonisch mit. Bitte beachten Sie die Kennwortregelung unter **Punkt 1.4**.

2.1.4. Nutzung Laptops

Bei Laptops der Pfarrei soll zusätzlich die Festplatte vollverschlüsselt werden (bspw. mit „BitLocker“). Hierbei ist die Kennwortregelung unter **Punkt 1.4** zu beachten.

2.2. Umgang mit Listen

2.2.1. Gemeindebesuche/Pfarrbriefverteilung

Die Adresslisten, die für die Durchführung von Aufgaben im Ehrenamt erforderlich sind (bspw. Besuche von Gemeindemitgliedern, Verteilung Pfarrbrief), müssen besonders sorgfältig verwahrt werden. Die Listen sind an das jeweilige Gemeindebüro zurückzugeben, wenn sie nicht mehr benötigt werden. Eine Nutzung dieser Personendaten für andere Zwecke ist strengstens untersagt.

2.2.2. Veranstaltung von Reisen

Bei der Durchführung von Reisen (Jugendreisen) erhalten die Reiseleitung oder das Gemeindebüro in der Regel Listen mit Notfallkontaktdaten, Nahrungsgewohnheiten, Nahrungsmittelunverträglichkeiten, erforderlichen Medikamentengaben oder Allergien.

Wichtig: Hierbei handelt es sich häufig um besonders schützenswerte Gesundheitsdaten. Daher sind diese Listen so zu verwahren, dass eine Kenntnisnahme Dritter ausgeschlossen ist. Unmittelbar nach Beendigung der Reise sind diese Listen an das jeweilige Gemeindebüro zurückzugeben, damit sie dort datenschutzkonform vernichtet werden.

3. Datenübermittlung

3.1. Brief

Der Versand von Poststücken auf dem Postweg ist eine sichere Form der Datenübermittlung. Gleiches gilt für die persönliche Übergabe von Dokumenten, sofern Ihnen der Empfänger bekannt ist.

3.2. Fax

Die Übermittlung von Schriftstücken per Fax erfolgt unverschlüsselt. Daher darf dieser Kommunikationsweg nur in Ausnahmefällen genutzt werden. Voraussetzung hierfür ist, dass

- ein Eilfall vorliegt, also der Empfänger das übermittelte Dokument bei einem Versand per Post nicht rechtzeitig erhalten würde und
- der Empfänger vorab informiert wurde, dass eine Fax-Sendung auf dem Weg ist, sodass sichergestellt ist, dass er das übermittelte Schreiben unmittelbar nach dem Versand entgegennehmen kann. Hierdurch soll verhindert werden, dass unbefugte Dritte Kenntnis von dem Schreiben nehmen können, wenn es im Ausgangsfach des Fax-Gerätes liegt.

Bitte stellen Sie auch sicher, dass an die Pfarrei gerichtete Fax-Sendungen möglichst unmittelbar nach ihrem Empfang aus dem Ausgangsfach des Fax-Geräts genommen werden.

3.3. E-Mail

Die private Nutzung des dienstlichen E-Mail-Kontos ist nicht erlaubt, da der kirchliche Dienstgeber andernfalls das Fernmeldegeheimnis nach § 88 TKG beachten müsste. Dies hätte unter anderem zur Folge, dass die Pfarrei im Falle einer ungeplanten Abwesenheit nicht auf die E-Mails dieser Person zugreifen dürfte. Ausnahmen müssen schriftlich dokumentiert werden.

Sofern die E-Mail an mehrere Adressaten gleichzeitig übermittelt werden soll (Verteilerliste), dürfen gegenüber dem Empfänger die übrigen Adressaten nicht offengelegt werden. In diesem Fall muss die E-Mail-Adresse des Versenders in das „An-Feld" und die Verteilerliste in das BCC-Feld (Blindkopie-Feld) eingetragen werden.

Die ehrenamtlichen und hauptamtlichen Mitarbeiter_innen, die über einen Ecclesias-Account verfügen, können alle E-Mail-Adressen in das An-Feld eintragen und vor dem Absenden den Button „Massen-Mail" (Blindkopie) in der oberen Leiste einschalten.

Wichtig: Personenbezogene Daten dürfen nicht unverschlüsselt per E-Mail übermittelt werden. Sofern Personendaten übermittelt werden sollen, sollten diese nicht im Text der E-Mail stehen, sondern in einer verschlüsselten Anlage (verschlüsseltes Office-Dokument, Zip-Datei oder verschlüsseltes PDF) verschickt werden. Bitte übermitteln Sie dem Adressaten das Kennwort zum Öffnen der Datei auf einem anderen Kommunikationsweg.

3.4. Verschlüsselung Datenträger

Sofern personenbezogene Daten wie Adresslisten auf einem Datenträger (USB-Stick) an einen anderen weitergegeben werden sollen, muss dieser Datenträger verschlüsselt sein. Hierzu soll die Software VeraCrypt verwendet werden.

4. Verarbeitung von Fotos und Angaben zur Person

Eine Erstellung bzw. Verarbeitung von Fotos und sonstigen Angaben zur Person (Veröffentlichung) durch die Pfarrei erfolgt in der Regel auf der Grundlage einer Einwilligung (vgl. unter **Punkt 4.1**) Es besteht für die Pfarrei die Verpflichtung, die Rechtmäßigkeit der Verarbeitung von Fotos jederzeit gegenüber der Datenschutzaufsicht nachweisen zu können. Aus diesem Grund müssen die Einwilligungserklärungen so abgelegt werden, dass sie jederzeit verfügbar sind.

Ausnahmsweise kann eine Verarbeitung dieser Daten auch ohne Einwilligung erfolgen, und zwar wenn

- dies im öffentlichen Interesse der Pfarrei liegt. Dies betrifft in der Regel geschlossene Veranstaltungen.
- die Fotos im Rahmen eines Aufzuges, einer Versammlung oder einer ähnlichen Veranstaltung aufgenommen wurden, bei denen nicht die abgebildete Person, sondern das Ereignis selbst im Vordergrund steht.

Sollten Sie unsicher sein, ob Fotos ohne Einwilligung verwendet oder veröffentlicht werden dürfen, setzen Sie sich bitte mit unserem Datenschutzbeauftragten in Verbindung.

4.1. Fotos

Für die Veröffentlichung oder anderweitige Verwendung von Fotos ist regelmäßig eine Einwilligungserklärung der betroffenen Person bzw. ihres Sorgeberechtigten erforderlich. Diese Erklärung sollte bereits vor Anfertigung des Fotos eingeholt werden, da bereits das Speichern von Bilddaten auf dem Speicherchip der Kamera eine Verarbeitung im Sinne des Datenschutzrechts darstellt. Bitte verwenden Sie hierzu die Vorlagen, die Ihnen die Pfarrei bzw. der betriebliche Datenschutzbeauftragte zur Verfügung stellt.

4.2. Weitere Personendaten

Auch die Verarbeitung von anderen personenbezogenen Daten (bspw. Name, das Ereignis, an dem die Person teilgenommen hat bzw. der Anlass, Alter der Person oder Angaben zur Tätigkeit in der Pfarrei) darf ebenfalls regelmäßig nur auf der Grundlage einer Einwilligung der betroffenen Person erfolgen.

5. Auskünfte

5.1. Allgemeine Hinweise

Die Pflicht, Dritten Auskunft zu erteilen, kann sich aus verschiedenen Gründen ergeben, etwa aus dem Kirchenrecht oder aus einer vertraglichen Beziehung. Ein Sonderfall bildet hier der Auskunftsanspruch aus dem kirchlichen Datenschutzrecht, der unter **Punkt 5.2** erläutert wird.

Sofern Dritte um Auskunft bitten, ist in jedem Fall sicherzustellen, dass die Person auch auskunftsberechtigt ist. Andernfalls besteht die Gefahr einer Datenschutzverletzung. Daher muss vor Auskunftserteilung in jedem Fall die Personenidentität geklärt sein.

Auskünfte sollten wegen der damit verbundenen Risiken nach Möglichkeit nicht auf telefonischem Wege erfolgen, sondern schriftlich beantwortet werden.

5.2. Auskunftsanspruch nach § 17 KDG

Es besteht die Verpflichtung, Dritten Auskunft zu erteilen, ob in schriftlicher oder elektronischer Form Daten über sie in der Pfarrei vorliegen.

Sofern jemand ein Auskunftsersuchen an die Pfarrei richtet, muss diese Person **innerhalb einer Frist von einem Monat** darüber informiert werden, welche Daten von der Pfarrei über sie gespeichert sind.

Falls eine Zusammenstellung dieser Daten länger als einen Monat in Anspruch nehmen sollte, besteht die Möglichkeit diese Antwortfrist auf drei Monate zu verlängern. In diesem Fall muss die Person, die den Auskunftsanspruch geltend macht, innerhalb eines Monats nach Eingang des Auskunftsersuchens unter Angabe der Gründe über die Verzögerung informiert werden.

Für das Antwortschreiben ist die entsprechende Vorlage der Pfarrei zu verwenden.

6. Datenpannen

Jeder, der eine Datenschutzverletzung feststellt, ist verpflichtet, die Verantwortliche (Pfarrer oder Ansprechpartner/in für Fragen im Bereich des Datenschutzes) sofort hierüber zu informieren.

Wichtig: Hier ist Eile geboten, da die möglicherweise erforderlichen Benachrichtigungen an die Aufsichtsbehörde und die betroffene Person **innerhalb von 72 Stunden** erfolgen müssen!

Eine Datenschutzverletzung ist jede Verletzung der Datensicherheit, „die – ob unbeabsichtigt oder unrechtmäßig – zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden."

Klassische Fälle sind bspw.

- das falsch adressierte Schreiben mit personenbezogenen Daten per E-Mail, Fax oder Brief (Anlage wird dem falschen Schreiben zugeordnet) oder
- der Verlust oder Diebstahl eines unverschlüsselten Datenträgers (bspw. Laptop, USB-Stick, Speicherchip einer Kamera).

Sollten Unsicherheiten bestehen, ob eine Datenschutzverletzung vorliegt, setzen Sie sich bitte zur Klärung mit der internen Datenschutzkoordinator_in in Verbindung.

7. Aktenvernichtung und Datenträgerentsorgung

Es besteht die gesetzliche Verpflichtung Unterlagen mit personenbezogenen Daten zu vernichten, wenn diese für den Zweck, für den sie erhoben wurden, nicht mehr benötigt werden und auch keine anderweitigen gesetzlichen oder kirchlichen Aufbewahrungsfristen bestehen. Dies gilt sowohl für Papierunterlagen als auch für elektronisch gespeicherte Daten.

Nicht mehr benötigte Papierunterlagen sollten unverzüglich vernichtet werden. Hierzu ist der Aktenvernichter (Schredder) der Pfarrei zu verwenden.

Sofern Datenträger nicht mehr benötigt werden (USB-Sticks, Festplatten von Arbeitsplatzcomputern), sind diese der Verantwortlichen (Pfarrei) zu übergeben, damit diese von einem nach DIN 66399 zertifizierten Entsorgungsbetrieb datenschutzkonform vernichtet werden. Die Datenträger sind bis zur Vernichtung sicher zu verwahren.

8. Umgang mit Dienstleistungsunternehmen

8.1. Abschluss eines Vertrages zur Auftragsverarbeitung

Sofern die Pfarrei Dienstleistungsunternehmen in Anspruch nimmt, ist stets zu prüfen, ob neben dem Hauptvertrag zusätzlich ein Vertrag zur Auftragsverarbeitung nach § 29 KDG zu schließen ist. Bei diesen Verträgen muss der Dienstleister immer nachweisen, dass er technische und organisatorische Maßnahmen zur Informationssicherheit getroffen hat. Der Vertrag und die beschriebenen Maßnahmen sind an die datenschutz nord GmbH zur Prüfung weiterzuleiten.

Eine Auftragsverarbeitung liegt immer dann vor, wenn ein Unternehmen streng weisungsgebunden für die Pfarrei personenbezogene Daten verarbeitet.

Die IT-Systeme verbleiben grundsätzlich in den Räumlichkeiten der Pfarrei bzw. der Gemeindebüros. Für den Fall von Garantieansprüchen werden Datenträger vor der Verbringung entfernt und – falls möglich und erforderlich – auf den Werkszustand zurückgesetzt.

8.2. Externe Dritte

Externe Dritte (bspw. Handwerker, IT-Dienstleister, Besucher) dürfen sich nicht unbeaufsichtigt in den einzelnen Büros und Gemeindebüros aufhalten.

Wichtig: Sollten sich externe Dritte in den Räumlichkeiten der Pfarrei (auch Archiv) aufhalten, muss stets sichergestellt werden, dass sie keine Kenntnis von personenbezogenen Daten erlangen können.

Sofern ein externer Dritter Sie in Ihrem Büro aufsucht, sollte das Büro in seiner Anwesenheit nicht verlassen werden.

8.3. Fernwartungszugriff

In den Fällen, in denen ein Dienstleistungsunternehmen per Fernwartung auf IT-Systeme der Pfarrei zugreift, ist nach Möglichkeit sicherzustellen, dass auf dem Bildschirm, auf den zugegriffen wird, keine personenbezogenen Daten sichtbar sind (bspw. offenes Word-Dokument, Eingabemaske in „e-mip"). Nach Abschluss der Wartungsarbeiten ist der Zugriff unverzüglich zu beenden.

9. Inkrafttreten

Diese Dienstanweisung tritt mit dem Datum ihrer Bekanntmachung in Kraft.

Elmshorn, 5.06.2020	(Pfarrer Stefan Langer)
ORT, DATUM	**UNTERSCHRIFT**

Anhang 1

Ablaufplan – Beginn und Beendigung der Tätigkeit in der Pfarrei

Beginn der Tätigkeit

Datenschutz

☐ Verpflichtung auf das Datengeheimnis

☐ Merkblatt zum Datenschutz

☐ Dienstanweisung zum Datenschutz

☐ Einwilligung Foto und Personendaten in Print- und elektronischen Medien

Zutritt

☐ Schlüssel für das Gemeindebüro/Gemeinderäume

Welche? _____

☐ Schlüssel, Token – Anz.: ___

Welche? _____

Zugangsdaten

☐ Einrichtung E-Mail-Konto

☐ Einrichtung Benutzerkonto „e-mip“

☐ Einrichtung Benutzerkonto „Eclessias“

Technische Geräte

☐ Aushändigung Diensthandy

☐ Aushändigung Laptop

☐ Aushändigung USB-Stick/s – Anz.: ___

☐ Aushändigung anderer IT-Geräte

Welche? _____

Beendigung der Tätigkeit

Datenschutz

☐ Rückgabe Schlüssel für das Gemeindebüro/Gemeinderäume

Welche? _____

☐ Rückgabe Schlüssel, Token – Anz.: ___

Welche? _____

☐ Fotos und Personenangaben von der Webseite gelöscht

Zugangsdaten

☐ E-Mail-Konto löschen

☐ Benutzerkonto „e-mip“ löschen

☐ Benutzerkonto „Ecclesias“ löschen

Technische Geräte

☐ Rückgabe Diensthandy

☐ Rückgabe Laptop

☐ Rückgabe USB-Stick/s – Anz.: ___

☐ Rückgabe anderer IT-Geräte

Welche? _____

Anhang 2

Zuständigkeiten in der Pfarrei

Verantwortlich für den Datenschutz in der Pfarrei	
Pfarrer Stefan Langer	Katholische Pfarrei Hl. Martin Beselerstraße 6, 25335 Elmshorn Telefonnummer: 0 41 21 / 26 27 90-1 E-Mail: gemeindebuero.elmshorn@pfarreihlmartin.de

Ansprechpartner/in für Fragen im Bereich des Datenschutzes	
Christina Pobel Verwaltungskoordinatorin	Katholische Pfarrei Hl. Martin c/o Gemeinde St. Michael Fahltskamp 14, 25421 Pinneberg Tel.: 0157 / 53 05 34 71 E-Mail: christina.pobel@pfarreihlmartin.de

Datenschutzbeauftragter der Pfarrei	
datenschutz nord GmbH	Dr. Uwe Schläger Konsul-Smidt-Straße 88 in 28217 Bremen kirche@datenschutz-nord.de
Frank van Hettinga	Tel.: 0421/696632-367 E-Mail: FHettinga@datenschutz-nord.de