– Vorblatt –

Datenschutzkonzept nach § 15 Abs. 4 KDG-DVO

Datenschutzrechtlich Verantwortlicher

Name der Organisation	Pfarrei Franz von Assisi
Anschrift	Rathausstraße 5, 24103 Kiel 0431 / 260923 – 0 E-Mail: pfarrei@franz-von-assisi-kiel.de
Telefon	0431-260923-0
E-Mail	pfarrbuero@franz-von-assisi-kiel.de

Vertretungsberechtigte Person/en

Name	Propst Dr. Jürgen Wätjer
Art der Vertretungsberechtigung	Pfarrer
E-Mail	propst@franz-von-assisi-kiel.de

Datenschutzbeauftragte/r

Name	Dr. Uwe Schläger
Anschrift	Konsul-Smidt-Str. 88 Bremen
E-Mail	kirche@datenschutz-nord.de

Vertreter in der EU für in Drittstaaten ansässige Verantwortliche (gemäß Art. 27 DSGVO)

Anschrift	–
E-Mail	–

Gemeinsam Verantwortliche/r

Soweit eine gemeinsame Verantwortlichkeit vorliegt, werden die Kontaktdaten des gemeinsam Verantwortlichen an entsprechender Stelle genannt.

Datenschutzkonzept nach § 15 Abs. 4 KDG-DVO besonderer Teil

Version

Datenschutzkonzept der Pfarrei nach § 15 Abs. 4 KDG-DVO

1. Schutzniveau I

Das IT-System, auf dem die schützenswerten personenbezogenen Daten abgelegt sind, ist nicht frei zugänglich; es befindet sich z.B. in einem abschließbaren Gebäude oder unter ständiger Aufsicht.

Die IT-Systeme der Pfarrei Franz von Assisi befinden sich in den Räumlichkeiten der Rathausstraße 5 in 24103 Kiel und in den Büros der Gemeinden, die der Pfarrei zugeordnet sind. Es besteht die Anweisung, die Büroräume auch bei kurzfristiger Abwesenheit zu verschließen (vgl. „Richtlinie zum Datenschutz in der Pfarrei" – nachfolgend „RiLi" genannt – unter Punkt 1.1.2).

Die für die Pfarrei Tätigen verfügen jeweils über eigene Schlüssel. Die Schlüsselausgabe dort erfolgt restriktiv und wird schriftlich dokumentiert. Der Propst wohnt im Haus des Pfarrbüros. Der Zutritt zu den jeweiligen Büroräumen ist auf die dort tätigen Mitarbeiter beschränkt. In den Büros werden schriftliche Unterlagen zusätzlich in verschlossenen Schränken verwahrt. Es besteht die klare Anweisung, dass sich externe Dritte (bspw. Handwerker, IT-Dienstleister, Besucher) nicht unbeaufsichtigt in den einzelnen Büros aufhalten dürfen. Die Beschäftigten sind zudem angewiesen, das Büro während eines Besuchstermins nicht zu verlassen. Sollte dies dennoch im Ausnahmefall vorkommen, besteht die Vorgabe, Besucher für die Dauer der Abwesenheit aus dem Büro zu bitten und dieses abzuschließen (vgl. RiLi unter Punkt 8.2).

In den Räumlichkeiten in der Rathausstraße wird ein elektronisches Schlüsselsystem genutzt.

Die Anmeldung am IT-System ist nur nach Eingabe eines geeigneten benutzerdefinierten Kennwortes oder unter Verwendung eines anderen, dem aktuellen Stand der Technik und dem jeweiligen Sicherheitsbedarf entsprechenden Authentifizierungsverfahrens möglich.

Der Zugang zu den Arbeitsplatzcomputern/Laptops (Clients) ist durch ein Kennwort gesichert. Die Softwarelösungen „e-mip" und „Ecclesias" (Fachanwendungen) sind durch Kennwort und PIN geschützt.
Durch die „Richtlinie zum Datenschutz in der Pfarrei" bestehen klare Vorgaben zur Verwendung geeigneter Kennwörter (vgl. RiLi unter Punkt 1.4.1): Das Kennwort soll mindestens acht Zeichen lang sein, groß- und klein geschriebene Buchstaben, Zahlen sowie Sonderzeichen enthalten.

Ein Wechsel der Kennwörter erfolgt zurzeit jährlich. Ob ein Passwortwechsel überhaupt erforderlich ist, wird zurzeit geprüft (vgl. „Hinweise zum sicheren Umgang mit Passwörtern" des LfDI Baden-Württemberg vom 12. Februar 2019).

Zudem wurden die für die Pfarrei Tätigen darauf hingewiesen, dass aufgeschriebene Kennwörter sicher verwahrt werden müssen (verschlossener Schrank, Schreibtisch o.ä.). Das Kennwort selbst sollte

sich zusätzlich noch in einem verschlossenen Briefumschlag befinden, damit unbefugte Zugriffe erkannt werden können. Dritten sollen Kennworte nicht mitgeteilt werden (vgl. RiLi a.a.O.).

Sicherungskopien der Datenbestände sind verschlossen aufzubewahren.

In einigen Gemeindebüros werden die auf den dort befindlichen IT-Systemen lokal gespeicherten Daten auf USB-Sticks gesichert. Diese werden anschließend sicher in einem Tresor oder verschlossenem Schrank verwahrt.

Es besteht für die Pfarrei jedoch keine Notwendigkeit einer Sicherung ihres Datenbestandes, da alle für die Erledigung kirchlicher Aufgaben erforderlichen Daten (kommunaler Datensatz, kirchliche Amtshandlungsdaten) direkt aus dem
elektronischen Gemeindemitgliederverzeichnis „e-mip" stammen. Hierbei handelt es sich um eine webbasierte Anwendung, die vom Rechenzentrum des Bistums Mainz gehostet wird, sodass diese Daten nicht lokal auf den IT-Systemen
der Pfarrei gespeichert sind.

Die Daten im e-mip werden regelmäßig durch die Meldeämter aktualisiert.

Vor der Weitergabe eines IT-Systems, insbesondere eines Datenträgers für einen anderen Einsatzzweck sind die auf ihm befindlichen Daten so zu löschen, dass ihre Lesbarkeit und ihre Wiederherstellung ausgeschlossen sind.

Eine Weitergabe oder ein Verkauf von IT-Systemen der Pfarrei findet nicht statt.
Sofern IT-Systeme nicht mehr benötigt werden, erfolgt vor ihrer Entsorgung ein Ausbau der Datenträger. Nach dem Ausbau werden die Datenträger bis zur Verschrottung sicher verwahrt (Tresor, verschlossener Schrank). Datenträger
(bspw. Festplatten, USB-Sticks) werden physikalisch nach Maßgabe der DIN P66399 durch einen zertifizierten Entsorgungsbetrieb vernichtet (vgl. RiLi unter Punkt 7).

Nicht öffentlich verfügbare Daten werden nur dann weitergegeben, wenn sie durch geeignete Schutzmaßnahmen geschützt sind. Die Art und Weise des Schutzes ist vor Ort zu definieren.

In der "Richtlinie zum Datenschutz in der Pfarrei" bestehen klare Handlungsvorgaben zur Datenübermittlung:
1. Verbot der Nutzung privater Kommunikationsmittel und IT-Arbeitsmittel zu dienstlichen Zwecken mit Erlaubnisvorbehalt (vgl. Punkt 1.3.1),
2. Vorgaben zur dienstlichen Verarbeitung personenbezogener Daten am Heimarbeitsplatz ehrenamtlich Tätiger, zur Aufbewahrung von Schriftgut sowie Regelungen zum Umgang mit Daten (vgl. Punkte 2.1.1 f),
3. Nutzung USB-Sticks zur Datenweitergabe ist nur zulässig, wenn dies für die sachgerechte Aufgabenerledigung in der Pfarrei erforderlich ist (vgl. Punkte 2.1.3 und 2.1.4).
4. USB-Sticks, auf denen personenbezogene Daten gespeichert werden, sind zu verschlüsseln (vgl. Punkt 2.1.4),
5. Nutzung des BCC-Feldes bei E-Mail-Versand an E-Mail-Verteiler (vgl. Punkt 3.3) und
6. Vorgaben zur Nutzung der Kommunikationswege Brief, Fax und E-Mail, insbesondere zur Verschlüsselung von E-Mail-Anhängen (vgl. Punkt 3).

2. Schutzniveau II

Die Anmeldung am IT-System ist nur nach Eingabe eines geeigneten benutzerdefinierten Kennwortes möglich, dessen Erneuerung in regelmäßigen Abständen möglichst systemseitig vorgesehen werden muss.

Bei den webbasierten Softwarelösungen „e-mip“ und „Ecclesias“ besteht neben der Kennworteingabe zusätzlich die Notwendigkeit einer PIN-Eingabe, damit auf besonders schützenswerte Daten zugegriffen werden kann. Bei „Ecclesias“ erfolgt zudem eine Zwei-Faktor-Authentifizierung (Bestätigung SMS). Die systemseitig vorgegebene Mindest-Passwortlänge beträgt hier beträgt 12 Zeichen.

Für die Software „Ecclesias“ wurde seitens der IT-Abteilung des Erzbistums Hamburg ein Datenschutzkonzept erstellt.

Das Starten des IT-Systems darf nur mit dem dafür bereit gestellten Betriebssystem erfolgen.

In der Verwaltung der Pfarrei und den Gemeindebüros werden ausschließlich die jeweils bereit gestellten IT-Systeme und Betriebssysteme genutzt. Eine Ausnahme bilden hier die ehrenamtlich Tätigen, die dienstliche Aufgaben (bspw. Gremienarbeit, Gruppen- oder Veranstaltungsorganisation) auf eigenen IT-Systemen zuhause (Homeoffice) bearbeiten dürfen. Für die Tätigkeit im Homeoffice bestehen in der RiLi unter Punkt 2 klare Handlungsvorgaben.

Sicherungskopien und Ausdrucke der Datenbestände sind vor Fremdzugriff und vor der gleichzeitigen Vernichtung mit den Originaldaten zu schützen.

Sofern in den Gemeindebüros Datensicherungen erfolgen, werden die hierfür verwendeten USB-Sticks im Tresor bzw. verschlossenen Schrank aufbewahrt. Auch Ausdrucke werden so verwahrt, dass Unbefugte keine Kenntnis von ihrem Inhalt nehmen können. Im Übrigen gelten die Zutrittsregelungen oben unter Punkt 5.1 dieses Konzeptes.

Die Daten der Schutzklasse II sind auf zentralen Systemen in besonders gegen unbefugten Zutritt gesicherten Räumen zu speichern, sofern keine begründeten Ausnahmefälle gegeben sind. Diese sind schriftlich dem betrieblichen Datenschutzbeauftragten zu melden.

Die IT-Systeme sind mit einer Firewall und einem Virenschutz ausgestattet. Mobile Datenträger sollen nach Möglichkeit nicht verwendet werden. Im Übrigen bestehen für die Nutzung von mobilen Datenträgern USB-Sticks klare Vorgaben in der „Richtlinie zum Datenschutz in der Pfarrei“ unter den Punkten 2.1.3 und 1.4. So soll bei Laptops der Pfarrei grundsätzlich die Festplatte vollverschlüsselt werden (BitLocker)

Die Übermittlung personenbezogener Daten außerhalb eines geschlossenen und gesicherten Netzwerks (auch über automatisierte Schnittstellen) hat grundsätzlich verschlüsselt zu erfolgen.

Ein unverschlüsselter Versand von E-Mails mit personenbezogenen Daten ist untersagt (vgl. RiLi unter den Punkten 3.1.3 und 1.4).

3. Schutzniveau 3

Ist es aus dienstlichen Gründen zwingend erforderlich, dass Daten der Datenschutzklasse III auf mobilen Geräten im Sinne des § 4 Absatz 2 oder Datenträgern gespeichert werden, sind diese Daten nur verschlüsselt abzuspeichern.

Sollten ausnahmsweise USB-Sticks eingesetzt werden, besteht die Verpflichtung, diese zu verschlüsseln (VeraCrypt
mit AES256-Verschlüsselung). Die Passwortvorgaben unter Punkt 1.4 der „Richtlinie zum Datenschutz in der Pfarrei" sind zu beachten. Kennworte sind Empfängern auf einem anderen Kommunikationsweg mitzuteilen. Laptops werden nur eingesetzt, wenn die Festplatte verschlüsselt ist (BitLocker). Hierzu existiert in der Pfarrei eine Arbeitshilfe.

Eine langfristige Lesbarkeit der zu speichernden Daten ist sicher zu stellen. So müssen z.B. bei verschlüsselten Daten die Sicherheit des Schlüssels und die erforderliche Entschlüsselung auch in dem nach § 16 Absatz 1 zu erstellenden Datensicherungskonzept berücksichtigt werden.

Eine Sicherung des Datenbestandes der Pfarrei ist nicht erforderlich (s. oben unter Punkt 5.1 dieses Konzeptes).

4. Sonderfälle Beicht- oder Seelsorgegeheimnis

Das Beichtgeheimnis nach cc. 983 ff. CIC ist zu wahren; personenbezogene Daten, die dem Beichtgeheimnis unterliegen, dürfen nicht verarbeitet werden.

Daten, die dem Beichtgeheimnis unterliegen, werden weder elektronisch noch papierbaisert verarbeitet.

Personenbezogene Daten, die, ohne Gegenstand eines Beichtgeheimnisses nach cc. 983 ff. CIC zu sein, dem Seelsorgegeheimnis unterliegen, dürfen nur verarbeitet werden, wenn dem besonderen Schutzniveau angepasste, erforderlichenfalls über das Schutzniveau der Datenschutzklasse III hinausgehende technische und organisatorische Maßnahmen ergriffen werden.

Eine elektronische Erfassung der Daten erfolgt nicht. Sofern sich der Pfarrer oder Mitglieder des Seelsorge-Teams im Rahmen der Seelsorge Notizen machen sollte, werden diese umgehend datenschutzkonform vernichtet.

5. Maßnahmen des Verantwortlichen

Der Verantwortliche klärt seine Mitarbeiter über Gefahren und Risiken auf, die insbesondere aus der Nutzung eines IT-Systems erwachsen können.

Die Mitarbeiter wurden gemäß § 5 KDG bei Aufnahme ihrer Tätigkeit schriftlich auf das Datengeheimnis verpflichtet. In diesem Rahmen wird dem zu Verpflichtenden ein "Merkblatt zum Datenschutz" erläutert und ausgehändigt, welches auf besondere Gefahrenlagen hinweist. Es werden Schulungs- und Sensibilisierungsmaßnahmen seitens des betrieblichen Datenschutzbeauftragten angeboten.

Erfolgt die Verarbeitung personenbezogener Daten durch einen Auftragsverarbeiter, so ist der Verantwortliche verpflichtet, die technischen und organisatorischen Maßnahmen des

Auftragsverarbeiters regelmäßig, mindestens jedoch im Abstand von jeweils zwei Jahren auf ihre Wirksamkeit zu überprüfen und dies zu dokumentieren.

Im Rahmen des Vertragsschlusses werden die technischen und organisatorischen Maßnahmen des Dienstleisters auf ihre Geeignetheit geprüft. Dienstleister, die nicht dem KDG unterliegen, unterzeichnen eine Zusatzvereinbarung zum KDG (sog. KDG/DSGVO-Annex), durch sie die Kenntnis und Einhaltung des Kirchlichen Datenschutzgesetzes bestätigen.

Der Verantwortliche hat ein Datensicherungskonzept zu erstellen und entsprechend umzusetzen. Dabei ist die langfristige Lesbarkeit der zu speichernden Daten in der Datensicherung anzustreben.

Die Notwendigkeit der Erstellung eines Datensicherungskonzeptes besteht für die Pfarreibzw. die Gemeindebüros nicht, da alle für die Aufgabenerfüllung relevanten Daten aus „e-mip" nicht lokal in der Pfarrei bzw. den einzelnen Gemeindebüros gespeichert sind (siehe oben unter Schutzniveau I). Zudem erfolgt regelmäßig eine Aktualisierung dieses Datenbestandes (Gemeindemitgliederverzeichnis)

Es sind geeignete technische Abwehrmaßnahmen gegen Angriffe und den Befall von Schadsoftware z.B. durch den Einsatz aktueller Sicherheitstechnik wie Virenscanner, Firewall-Technologien und eines regelmäßigen Patch-Managements (geplante Systemaktualisierungen) vorzunehmen.

—

Virenscanner

Es wird folgender Virenscanner eingesetzt: Windows Defender Security Center

Firewall

Folgende Firewall wird genutzt: Windows Defender Firewall

Patch-Management

Systemseitige Aktualisierung (Updates)

Dokumente

—

6. Maßnahmen der Beschäftigten

Jeder Mitarbeiter trägt die Verantwortung für die datenschutzkonforme Ausübung seiner Tätigkeit. Es ist ihm untersagt, personenbezogene Daten zu einem anderen als dem in der jeweils rechtmäßigen Aufgabenerfüllung liegenden Zweck zu verarbeiten.

Die Mitarbeiter wurden gemäß § 5 KDG bei Aufnahme ihrer Tätigkeit schriftlich auf das Datengeheimnis verpflichtet. Ein Merkblatt zum sachgerechten Umgang mit personenbezogenen Daten wird dem zu Verpflichtenden mit der Verpflichtungserklärung (vom Datenschutzbeauftragten bereitgestellt) ausgehändigt werden und hilft in der täglichen Routine.

7. Besondere Gefahrenlagen

Auf dienstlichen IT-Systemen dürfen ausschließlich vom Verantwortlichen autorisierte Programme und Kommunikationstechnologien verwendet werden. Die automatische Weiterleitung dienstlicher E-Mails auf private E-Mail-Konten ist in jedem Fall unzulässig.

In der Pfarrei und den Gemeindebüros wird auf dienstlichen IT-Systemen ausschließlich autorisierte Software genutzt.
Das Erzbistum Hamburg hat E-Mail-Postfächer mit einheitlicher Domain (@franz-von-assisi-kiel.de) für die dienstliche
Tätigkeit aller ehrenamtlich Tätigen in der Pfarrei eingerichtet. Die in der Pfarrei ehrenamtlich Tätigen verwenden diese E-Mail-Adressen für dienstliche Zwecke.

Die Nutzung dienstlicher IT-Systeme zu auch privaten Zwecken ist grundsätzlich unzulässig. Ausnahmen regelt der Verantwortliche unter Beachtung der jeweils geltenden gesetzlichen Regelungen.

Die private Nutzung dienstlicher Kommunikationsmittel und IT-Systeme ist grundsätzlich unzulässig. Die Verantwortliche
(Pfarrei) kann hier für den einzelnen Fall eine abweichende Regelung treffen.

Die Verarbeitung personenbezogener Daten auf privaten IT-Systemen zu dienstlichen Zwecken (BYOD) ist grundsätzlich unzulässig. Sie kann als Ausnahme von dem Verantwortlichen unter Beachtung der jeweils geltenden gesetzlichen Regelungen zugelassen werden.

Die dienstliche Nutzung privater Kommunikationsmittel/IT-Systeme (Arbeitsplatzcomputer, Datenträger wie USB-Sticks, E-Mail, Internet, Fax, Telefon) zu dienstlichen Zwecken (BYOD) ist grundsätzlich unzulässig. Etwas anderes gilt, wenn die Verantwortliche (Pfarrei) hier eine abweichende Regelung getroffen hat. Diese Ausnahmeregelung erfolgt schriftlich.In einzelnen Fällen ist die Nutzung eines privaten IT-Systems unumgänglich: Im Hinblick auf die ehrenamtliche Tätigkeit – insbesondere in den Gremien oder Gruppen der Pfarrei – ist die Nutzung privater IT-Systeme durch die die Verantwortliche (Pfarrei) ausdrücklich gestattet, soweit dies für die Aufgabenerledigung erforderlich oder sinnvoll ist (vgl. RiLi unter Punkt 1.3.1). Unter Punkt 2.1 der RiLi bestehen Vorgaben zur Organisation des Heimarbeitsplatzes.

8. Externe Zugriffe, Auftragsverarbeitung

Der Zugriff aus und von anderen IT-Systemen durch Externe (z.B. externe Dienstleister, externe Dienststellen) dürfen nur aufgrund vertraglicher Vereinbarung erfolgen.

Ein unbeaufsichtigter Zugriff Dritter auf die IT-Systeme ist ausgeschlossen. Die Beschäftigten der Pfarrei wurden entsprechend sensibilisiert. Wartungs- und Reparaturarbeiten vor Ort erfolgen unter Aufsicht eines Mitarbeiters und auf der Grundlage von Verträgen zur Auftragsverarbeitung nach § 29 KDG im Rahmen strenger datenschutzrechtlicher Vorgaben. Sofern Dienstleister (Auftragsverarbeiter) in Anspruch genommen werden, müssen diese ihre technischen und organisatorischen Maßnahmen zur IT-Sicherheit nachweisen. Im Übrigen bestehen hier Handlungsvorgaben zum Umgang mit Besuchern oder Dienstleistern vor Ort und bei Fernwartungszugriffen unter Punkt 8 der RiLi.

Auftragsverarbeiter

—

Bei Zugriffen durch Externe ist mit besonderer Sorgfalt darauf zu achten und nicht nur vertraglich, sondern nach Möglichkeit auch technisch sicherzustellen, dass keine Kopien der personenbezogenen Datenbestände gefertigt werden können.

Externe Dritte (bspw. Handwerker, Dienstleister, Dritte) dürfen sich nicht unbeaufsichtigt in den Räumlichkeiten der Pfarrei aufhalten (Büro, Gemeindebüros, Archiv), damit ein unbefugter Zugriff auf Daten der Pfarrei ausgeschlossen ist (vgl. RiLi unter Punkt 8). Die Beschäftigten sollen Personen ansprechen, bei denen nicht klar ist, ob sie sich zulässigerweise in den Räumlichkeiten der Pfarrei aufhalten dürfen.

Muss dem Externen bei Vornahme der Arbeiten ein Systemzugang eröffnet werden, ist dieser Zugang entweder zu befristen oder unverzüglich nach Beendigung der Arbeiten zu deaktivieren. Im Zuge dieser Arbeiten vergebene Passwörter sind nach Beendigung der Arbeiten unverzüglich zu ändern.

Fernwartungszugriffe erfolgen nur nach Bestätigung durch den Nutzer am Client. Der Zugriff wird nach Erledigung der Wartungsaufgabe unverzüglich beendet. Kennwörter werden hierbei nicht verwendet (vgl. RiLi unter Punkt 8.3). Während des Zugriffs sollen auf dem Bildschirm keine personenbezogenen Daten sichtbar sein (bspw. geöffnete Dateien, Eingabemaske „e-mip“) sein.

Bei der dauerhaften Inanspruchnahme von externen IT-Dienstleistern sind geeignete vergleichbare Regelungen zu treffen.

Sofern Dienstleister (Auftragsverarbeiter) in Anspruch genommen werden, müssen diese ihre technischen und organisatorischen Maßnahmenzur IT-Sicherheit nachweisen (vgl. RiLi unter Punkt 8.1).

Eine Fernwartung von IT-Systemen darf nur erfolgen, wenn der Beginn aktiv seitens des Auftraggebers eingeleitet wurde und die Fernwartung systemseitig protokolliert wird.

Fernwartungszugriffe erfolgen unter Aufsicht eines Mitarbeiters und auf der Grundlage von Verträgen zur Auftragsverarbeitung nach § 29 KDG im Rahmen strenger datenschutzrechtlicher Vorgaben.

Die Verbringung von IT-Systemen mit Daten der Datenschutzklasse III zur Durchführung von Wartungsarbeiten in den Räumen eines Externen darf nur erfolgen, wenn die Durchführung der Wartungsarbeiten in eigenen Räumen nicht möglich ist und sie unter den Bedingungen einer Auftragsverarbeitung erfolgt

Die IT-Systeme verbleiben grundsätzlich in den Räumlichkeiten der Pfarrei. Für den Fall von Garantieansprüchen oder Reparaturen außer Haus werden Datenträger – falls erforderlich – vor der Verbringung außer Haus aus dem Gerät entfernt. Hardware wird – falls möglich und erforderlich – in diesen Fällen auf den Werkszustand zurückgesetzt

9. Verschrottung, Vernichtung, Abgabe von IT-Systemen

Bei der Verschrottung bzw. der Vernichtung von IT-Systemen, insbesondere Datenträgern, Faxgeräten und Druckern, sind den jeweiligen DIN-Normen entsprechende Maßnahmen zu

ergreifen, die die Lesbarkeit oder Wiederherstellbarkeit der Daten zuverlässig ausschließen. Dies gilt auch für den Fall der Abgabe von IT-Systemen, insbesondere Datenträgern, zur weiteren Nutzung.

Papierdokumente werden in der Pfarrei und den Gemeindebüros mit eigenen Schreddern auf der Schutzstufe P4 vernichtet. Sofern in den einzelnen Gemeindebüros noch Schredder im Einsatz sind, die eine Vernichtung von Schriftgut auf dieser Schutzstufe nicht ermöglichen, werden diese durch geeignete Aktenvernichter ersetzt werden. Datenträger und teilweise auch Schriftgut werden durch einen zertifizierten Dienstleister nach DIN 66399 datenschutzgerecht vernichtet (vgl. RiLi unter Punkt 7).

10. Passwortlisten der Systemverwaltung

Alle nicht zurücksetzbaren Passwörter (z.B. BIOS- und Administrationspasswörter) sind besonders gesichert aufzubewahren.

keine

11. Übermittlung personenbezogener Daten per Fax

Faxgeräte sind so aufzustellen und einzurichten, dass Unbefugte keine Kenntnis vom Inhalt eingehender oder übertragener Nachrichten erhalten können.

Die Faxgeräte befinden sich im Pfarr- bzw. den Gemeindebüros unter Aufsicht der dort Tätigen. Ein Faxversand erfolgt nur in Ausnahmefällen, i.d.R. auf Wunsch des Empfängers.

Sowohl die per Fax übermittelten als auch die in Sende-/Empfangsprotokollen enthaltenen personenbezogenen Daten unterliegen dem Datenschutz. Protokolle sind entsprechend sorgfältig zu behandeln.

In der Regel erfolgt eine Übermittlung per Fax nur in unbedingt notwendigen Eilfällen, wo der Postweg zu lange dauert,
in Absprache mit dem Empfänger, der die sofortige Übernahme der Sendung sicherstellt, damit das übertragene Schreiben nicht von Dritten gelesen werden kann. Es wird sichergestellt, dass empfangene Fax-Sendungen nicht unnötig lange im Ausgabefach des Fax-Gerätes verbleiben (vgl. RiLi unter Punkt 3.1.2).

Um eine datenschutzrechtlich unzulässige Übermittlung möglichst zu verhindern, ist bei Faxgeräten, die in Kommunikationsanlagen (Telefonanlagen) eingesetzt sind, eine Anrufumleitung und -weiterschaltung auszuschließen.

Eine Rufweiterleitung durch die Fax-Geräte in den Büros/Gemeindebüros der Pfarrei erfolgt nicht.

Daten der Datenschutzklassen II und III dürfen grundsätzlich nur unter Einhaltung zusätzlicher Sicherheitsvorkehrungen per Fax übertragen werden. So sind insbesondere mit dem Empfänger der Sendezeitpunkt und das Empfangsgerät abzustimmen, damit das Fax direkt entgegengenommen werden kann.

siehe oben

12. Sonstige Formen der Übermittlung personenbezogener Daten

E-Mails, die personenbezogene Daten der Datenschutzklasse II oder III enthalten, dürfen ausschließlich im Rahmen eines geschlossenen und gesicherten Netzwerks oder in verschlüsselter Form mit geeignetem Verschlüsselungsverfahren übermittelt werden.

Per E-Mail werden personenbezogene Daten ausschließlich in passwortgeschlüsselten Zip-Archiven oder PDF-Dateien (AES 256) mit achtstelligem Kennwort versendet (vgl. RiLi unter Punkt 3.1.3)

Eine Übermittlung personenbezogener Daten per E-Mail an Postfächer, auf die mehr als eine Person Zugriff haben (sog. Funktionspostfächer), ist in Fällen personenbezogener Daten der Datenschutzklassen II und III grundsätzlich nur zulässig, wenn durch vorherige Abstimmung mit dem Empfänger sichergestellt ist, dass ausschließlich autorisierte Personen Zugriff auf dieses Postfach haben.

Der Zugriff auf Funktionspostfächer ist auf die Personen beschränkt, die diese Daten für ihre Arbeit benötigen.
In der Softwareanwendung „Ecclesias" bestehen Gruppenrichtlinien, die sicherstellen, dass die Nutzer nur auf die für
sie bestimmten Daten zugreifen können. Hier ist meist zusätzlich eine PIN-Eingabe erforderlich.

13. Kopier- / Scangeräte

Bei Kopier-/Scangeräten mit eigener Speichereinheit ist sicherzustellen, dass ein Zugriff auf personenbezogene Daten durch unberechtigte Mitarbeiter oder sonstige Dritte nicht möglich ist.

Die Beschäftigten im Pfarr- bzw. in den Gemeindebüros haben keinen Zugriff auf die Speichereinheit der Multifunktionsgeräte (Kopierer, Drucker, Fax). Auch unbefugte Dritte haben keinen Zugang zu diesen Geräten.