Grundsätze zur Datensicherheit

Alle für die Pfarrei Franz von Assisi Tätigen müssen das kirchliche Datenschutzrecht (KDG) beachten, denn die Pfarrei muss als Verantwortliche für jedes Fehlverhalten ihrer Mitarbeitenden einstehen. Außerdem kann ein unsachgemäßer Umgang mit Personendaten das Ansehen unserer Pfarrei erheblich beschädigen.

Daher haben wir hier die wichtigsten Pflichten im Bereich des Datenschutzrechts zusammengefasst.

Bitte machen Sie sich mit diesen Datenschutzgrundsätzen vertraut – und halten diese (soweit anwendbar) bei Ihrer Tätigkeit für unsere Pfarrei ein.

1. Büroorganisation

Unbefugte sollten keinen Zugriff auf die Ihnen anvertrauten personenbezogenen Daten haben.

- Richten Sie den **Bildschirm Ihres Computers** (im Pfarrbüro) so aus, dass Dritte (z.B. Besucher/innen im Pfarrbüro, Blick durch das Fenster) den Bildschirminhalt nicht sehen können.
- **Ablagekörbe** sollten so aufgestellt sein, dass Dritte keine Kenntnis vom Inhalt der dort abgelegten Dokumente erlangen können.
- **Sperren Sie Ihren Bildschirm** (Windows-Taste + L), wenn Sie den Arbeitsplatz kurzzeitig verlassen und die Gefahr einer Kenntnisnahme durch Dritte besteht.
- **Lassen Sie keine Unterlagen am Drucker, Kopierer oder Fax liegen**, wenn diese Geräte unbeaufsichtigt und für unbefugte Dritte zugänglich sind (z.B. Standort des Geräts im Flur).
- **Lassen Sie fremde Personen nicht unbeaufsichtigt im Gebäude (z.B. Pfarrbüro).**
- Sprechen Sie **fremde Personen** im Gebäude auf ihren Besuch an und begleiten Sie diese zur gewünschten Ansprechperson.
- Lassen Sie auch **Reinigungskräfte oder Handwerker** nach Möglichkeit nicht unbeaufsichtigt, wenn sich diese in Bereichen befinden, in denen personenbezogene Daten verwahrt werden (z.B. Büro, Archiv). Ist eine Beaufsichtigung nicht möglich, stellen Sie sicher, dass Unterlagen mit personenbezogenen Daten für Dritte nicht zugänglich sind und Ihr Bildschirm gesperrt ist, um eine unbefugte Einsichtnahme zu verhindern.
- **Auch im „Homeoffice" (n. a. auch bei ehrenamtlicher Tätigkeit) muss der Datenschutz beachtet werden: Auch hier dürfen Unbefugte**, dies betrifft auch Familienmitglieder und Freunde, die Sie besuchen, **keine Kenntnis von den Ihnen anvertrauten Daten erlangen.**
- **Auch sollte vermieden werden, dass sich dienstliche und private Daten vermischen.** Eine sinnvolle Maßnahme wäre bspw. die Einrichtung eines Microsoft-Benutzerkontos für Ihre dienstliche Tätigkeit oder eine Speicherung dienstlicher Daten ausschließlich auf einem USB-Stick, der vor einem Zugriff Dritter geschützt wird (sichere Verwahrung in verschlossenem Schrank).

- **Soweit anwendbar, gelten sämtliche Datenschutzgrundsätze auch für Ihre dienstliche Tätigkeit im „Homeoffice"!**

Schließen Sie vertrauliche Unterlagen weg.

- **Lassen Sie möglichst keine vertraulichen Unterlagen mit personenbezogenen Daten auf dem Schreibtisch liegen,** wenn Sie Ihren Schreibtisch verlassen, sondern schließen Sie diese nach Möglichkeit sicher weg.
- Lassen Sie **Fenster und Türen** nicht geöffnet, wenn der Raum unbeaufsichtigt ist.
- **Festplatten und andere Datenträger** mit personenbezogenen Daten (z.B. Datensicherungen) sollten **sicher verwahrt** werden (z.B. verschlossener Schrank oder Schreibtisch, Safe im Pfarrbüro) und **nach Möglichkeit verschlüsselt** sein.

Schützen Sie vertrauliche Gespräche.

- Haben Sie einmal etwas Vertrauliches zu besprechen? Dann **suchen Sie einen Bereich auf, in welchem andere Personen das Gespräch nicht mithören können.**
- **Üben Sie Zurückhaltung im privaten Umfeld!** Sie dürfen niemals dienstliche Informationen über Personen im privaten Gespräch oder auf privat genutzten sozialen Medien offenbaren.

2. Sichere Passwörter

Verwenden Sie sichere Passwörter!

- Wählen Sie möglichst **komplexe Passwörter** aus. Sicher sind **mindestens zehnstellige Passwörter, bestehend aus Klein- und Großbuchstaben, Zahlen und Sonderzeichen.** Vermeiden Sie unsichere und triviale Passwörter.
- **Geben Sie Ihre Passwörter niemals an Unbefugte weiter.**
- **Verwahren Sie notierte Passwörter sicher** (z.B. verschlossener Briefumschlag im Safe des Pfarrbüros). Ein häufiger Fehler ist eine Passwortnotiz unter der Tastatur oder am Bildschirm.

3. Elektronische Kommunikation: E-Mail

Kommunizieren Sie datenschutzkonform.

- **Zur Kommunikation in Angelegenheiten der Pfarrei ist grundsätzlich die dienstliche E-Mail-Adresse zu nutzen,** die Ihnen die Pfarrei über die Pfarrei-verwaltungssoftware *Ecclesias* zur Verfügung gestellt hat. Sollte es ausnahmsweise erforderlich sein, dass Sie Ihre **private E-Mail-Adresse** nutzen, dürfen in der E-Mail keine personenbezogenen Daten von Dritten enthalten sein. Die private E-Mail-Adresse sollte nur für „un-sensible" Themen wie beispielsweise Terminabstimmungen genutzt werden. Es besteht jedoch die Möglichkeit, eine **Benachrichtigung an Ihre private E-Mail-Adresse** einzurichten, damit Sie informiert werden, wenn Sie über Ecclesias eine E-Mail erhalten haben. **Eine automatische Weiterleitung von E-Mails aus Ecclesias an Ihre private E-Mail-Adresse ist jedoch nicht erlaubt.**
- Sofern Sie **eine E-Mail an mehrere Empfänger (Verteiler)** senden – bei denen davon auszugehen ist, dass diese sich untereinander nicht kennen bzw. deren E-Mail-Adressen untereinander nicht bekannt sind – **sollten Sie die Empfänger-Adressen stets in das BCC-Feld eintragen** („Blindkopie") und die E-Mail über das „An"-Feld an sich selbst adressieren. So erlangen die übrigen Adressaten keine Kenntnis darüber, an wen die E-Mail versandt wurde, und auch die E-Mail-Adressen der übrigen Empfänger sind nicht sichtbar. Wenn Sie innerhalb der Pfarrei oder mit Stellen im Generalvikariat kommunizieren ist die Nutzung des BCC-Feldes hingegen nicht erforderlich.
- **Personenbezogene Daten (z.B. Adresslisten) dürfen nicht unverschlüsselt per E-Mail übermittelt werden.** Diese sollten nicht im Text der E-Mail stehen, sondern in einer verschlüsselten Anlage (z.B. verschlüsseltes Office-Dokument, verschlüsselte Zip-Datei oder verschlüsseltes PDF) verschickt werden. Hierzu existiert eine Arbeitshilfe. Bitte übermitteln Sie dem Adressaten dann das Kennwort zum Öffnen der Datei auf einem anderen Kommunikationsweg (z.B. telefonisch, per SMS, persönlich).

4. Anfragen und Auskunftsersuchen

Prüfen Sie Anfragen zu personenbezogenen Daten.

- **Geben Sie vertrauliche Informationen und personenbezogene Daten grundsätzlich nicht telefonisch weiter.**
- **Beantworten Sie entsprechende Anfragen nach Möglichkeit schriftlich und erst nach Prüfung der Identität des Anfragenden.** Um sicher zu gehen, dass Sie die richtige Person informieren, gibt es mehrere Möglichkeiten, zum Beispiel persönliches Erscheinen im Pfarrbüro erbitten, der Versand der Unterlagen an eine bekannte Meldeadresse dieser Person oder Legitimation durch entsprechend geschwärzte Kopie des Personalausweises per E-Mail.

5. Datenpannen

Informieren Sie den Datenschutzbeauftragten und auch die Pfarrei im Falle einer Datenpanne.

Eine Datenpanne liegt zum Beispiel vor, wenn Ihnen ein Computer, Laptop oder anderer Datenträger, auf dem personenbezogene Daten gespeichert sind verloren geht oder gestohlen wird, beim „offenen Versand" einer E-Mail an einen E-Mail-Verteiler oder wenn Sie eine E-Mail nicht an den richtigen Adressaten übermitteln.

- Sollte Ihnen eine **Datenpanne** unterlaufen, setzen Sie sich bitte **unverzüglich mit unserem Datenschutzbeauftragten in Verbindung** (siehe **Punkt 7**). Eine sofortige Information ist wegen der kurzen Meldefristen (72 Stunden) dringend erforderlich. An diesen können Sie sich auch wenden, falls noch etwas unklar sein sollte.
- **Informieren Sie** umgehend – sofern diese Stellen noch keine Kenntnis von dem Vorfall haben – **auch das Pfarrbüro bzw. den Pfarrer, sowie die Verwaltungskoordinatorin und die Ansprechperson in der Pfarrei für Datenschutz** (Hr. Schröder) über diesen Sachverhalt.

6. Aktenvernichtung

Entsorgen Sie Papierunterlagen und Datenträger sicher.

Immer wieder hört man, dass Unterlagen von Unternehmen (auch kirchlichen Stellen) in falsche Hände gelangen, indem sie von fremden Personen aus Mülltonnen oder Papierkörben gefischt werden.

- **Entsorgen Sie daher Papierunterlagen mit personenbezogenen Daten datenschutzkonform.** Entweder mittels eines **Aktenschredders auf der Schutzstufe P4** (oder höher) oder **durch einen zertifizierten Entsorgungsbetrieb.**
- **Falls Ihnen dies nicht möglich ist, geben Sie die Papierunterlagen bitte an das Pfarrbüro zurück** (z.B. Adresslisten für Pfarrbriefverteilung und Besuchsdienste), damit diese dort datenschutzkonform vernichtet werden können.
- **Entsorgen Sie auch nicht mehr benötigte Computer und Datenträger mit Daten der Pfarrei (z.B. mobile Festplatte, USB-Stick) datenschutzkonform** – am besten durch einen zertifizierten Entsorgungsbetrieb.
- **Geben Sie nicht mehr benötigte Hardware der Pfarrei nicht an Dritte weiter.** Sollten Sie dies beabsichtigen, setzen Sie sich bitte mit uns in Verbindung.

7. Kontakt zum Datenschutzbeauftragten

Für weitergehende Informationen und in Zweifelsfällen wenden Sie sich bitte an den Datenschutzbeauftragten oder an seine Mitarbeitenden:

KONTAKTDATEN	
datenschutz nord GmbH Konsul-Smidt-Straße 88 28217 Bremen	Telefon: 0421/696632 - 0 E-Mail: kirche@datenschutz-nord.de