

## Häufig gestellte Fragen: Datenschutz

### DVR-Nummer in Signatur:

#### **Warum?**

- ⇒ Weil es das Gesetz so vorsieht: laut § 25 Abs. 1 DSGVO gilt: „Bei Übermittlungen und bei Mitteilungen an Betroffene hat der Auftraggeber seine Identität in geeigneter Weise offenzulegen, sodaß den Betroffenen die Verfolgung ihrer Rechte möglich ist. Bei meldepflichtigen Datenanwendungen ist in Mitteilungen an Betroffene die Registernummer des Auftraggebers anzuführen.“ (Pflicht zur Offenlegung der Identität des Auftraggebers)

Da es im Einzelfall oft nicht möglich oder sehr schwierig ist, zu entscheiden, ob die Daten aus einer meldepflichtigen oder nicht meldepflichtigen Datenanwendung stammen, empfiehlt die Datenschutzbehörde, die DVR-Nummer standardmäßig in **jedem Schreiben** an Betroffene anzuführen. Dies kann beispielsweise durch Aufnahme der DVR-Nummer in den Brief- bzw. E-Mail-Kopf und oder Fuß geschehen.

#### **DVR-Nummer auch bei E-Mails?**

- ⇒ Ja! Die Datenschutzbehörde empfiehlt, die DVR-Nummer standardmäßig in **jedem Schreiben** an Betroffene anzuführen. Dies kann beispielsweise durch Aufnahme der DVR-Nummer in den Brief- bzw. E-Mail-Kopf und oder Fuß geschehen.

#### **Pfarrblattdruck (oder Jahresbericht): Adressweitergabe an Druckerei zwecks Adressierung des Druckwerkes unter welchen Bedingungen?**

- ⇒ Hierbei handelt es sich um den klassischen Fall einer Datenweitergabe an einen Dienstleister. Laut § 10 Abs. 1 DSGVO gilt: „Auftraggeber dürfen bei ihren Datenanwendungen Dienstleister in Anspruch nehmen, wenn diese ausreichende Gewähr für eine rechtmäßige und sichere Datenverwendung bieten. Der Auftraggeber hat mit dem Dienstleister die hierfür notwendigen **Vereinbarungen** zu treffen und sich von ihrer Einhaltung durch Einholung der erforderlichen Informationen über die vom Dienstleister tatsächlich getroffenen Maßnahmen zu überzeugen.“ (Zulässigkeit der Überlassung von Daten zur Erbringung von Dienstleistungen)

Es ist daher in diesem Fall eine **Dienstleistervereinbarung** mit der Druckerei abzuschließen (Muster beim Datenschutzbeauftragten erhältlich)!

⇒

#### **Welche DVR-Nummer schreibe ich unter E-Mails, wenn ich in einer Pfarre und einer Institution arbeite?**

- ⇒ Streng genommen müsste man sagen, je nachdem, woher die Daten der Empfänger stammen (z.B. aus der Pfarrkartei oder einer Institutions-spezifischen Datenanwendung). Da es aber einen verwaltungstechnisch hohen Aufwand darstellt, hier zu unterscheiden bzw. die DVR-Nummer in der E-Mail-Signatur jeweils zu wechseln, empfehle ich, beide Nummern anzuführen. Im Zweifelsfall ist es aber immer noch besser, nur eine der beiden Nummern anzugeben, als gar keine.  
MitarbeiterInnen der **Abteilung Pastorale Berufe** verwenden in ihren Signaturen (Brief, Mail) die DVR-Nummer der Abteilung Pastorale Berufe. **DVR: 0029874(1871)**

### **Hat ein Dekanat eine DVR-Nummer?**

- ⇒ Dekanate haben keine eigene DVR-Nummer, da sie keine eigenständigen Rechtsträger sind (sondern eher „Verwaltungsbezirke“). MitarbeiterInnen, die einem Dekanat zugeteilt sind (z.B. DekanatsassistentInnen), verwenden daher in ihren Signaturen (Brief, Mail) die DVR-Nummer der **Abteilung Pastorale Berufe. DVR: 0029874(1871)**

### **Bei Vergabe der EDV-Wartung: Braucht man hier eine Geheimhaltungserklärung?**

- ⇒ Wenn der Dienstleister (EDV-Warter) bei seiner Tätigkeit die Möglichkeit hat, Kenntnis von personenbezogenen Daten oder anderen vertraulichen, firmeninternen Daten/Informationen des Auftraggebers (Diözese, Pfarre...) zu erlangen, so ist eine sogenannte **Dienstleistervereinbarung gemäß § 10 Datenschutzgesetz** abzuschließen (Muster beim Datenschutzbeauftragten vorhanden). Ist also durch die EDV-Wartung ein solcher Zugang zu Daten möglich/gegeben (z.B. im Sinne eines Administrators), dann ist eine Dienstleistervereinbarung mit dem Wartungs-Dienstleister abzuschließen, wenn nicht (z.B. bei reiner Hardware-Wartung), dann ist dies nicht notwendig.

### **WhatsApp Gruppen, Telefonnummer Weitergabe**

- ⇒ Für die Weitergabe von Telefonnummern gilt grundsätzlich: ist die Telefonnummer bereits veröffentlicht (Telefonbuch, Homepage, Facebook...), so darf sie weitergegeben werden, ansonsten nur mit Zustimmung des Betroffenen.  
Telefonnummern dürfen beruflich auch nur für jenen Zweck verwendet werden, für den sie vom Betroffenen hergegeben wurden – z.B. darf die Telefonnummer, die vom Betroffenen der Kirchenbeitragsstelle oder der Katholischen Jugend gemeldet wurde, auch nur im jeweiligen Bereich verwendet werden. Sprich: die Weitergabe einer der Katholischen Jugend gemeldeten Telefonnummer darf wohl von einem Jugendleiter an einen anderen Jugendleiter erfolgen (für berufliche Zwecke!), nicht aber etwa an alle Mitglieder einer Jugendgruppe. Es gilt auch hier die Geheimhaltungsverpflichtung für „beruflich anvertraute Daten“.

### **2-3 Arbeitsplätze. Drop Box als einzige Chance in effektiverweise, Dokumente, Bilder zu Verfügung zu haben.**

- ⇒ Zum Thema „document sharing services“ (Dropbox, Cloud-Dienste...) gibt es vom Datenschutzbeauftragten eine eigene Stellungnahme, die zu dem Schluss führt, dass aufgrund verschiedenster Sicherheitsrisiken das Verwenden von sogenannten „Public Clouds“ **grundsätzlich abzulehnen** ist! Als größtes Manko wird empfunden, dass die Dateien zumeist unverschlüsselt auf dem Cloud-Speicher abgelegt werden. Verschafft sich also jemand Zugriff auf den entsprechenden Cloud-Server, kann diese Person auf die dort abgelegten Daten zugreifen!  
**Firmeninterne Daten** (egal ob personenbezogen oder nicht) dürfen somit nur gespeichert werden, wenn die Public Cloud bestimmte Voraussetzungen erfüllt (Verschlüsselung!), was aber in den allermeisten Fällen nicht der Fall sein wird - ansonsten dürfen diese Public Clouds **nur für die Speicherung privater bzw. eigener Daten oder bei Zustimmung des/der Betroffenen verwendet werden!**  
Die Diözese Linz hat eine interne CLOUD eingerichtet. Nähere Informationen gibt es bei der Diözesanen IT.  
**Hinweis 1:** die Verpflichtungserklärung auf das Datengeheimnis bzw. die allgemeinen Vorschriften zum Datenschutz und zur Datensicherheit gelten auch für Private Clouds und sind weiterhin zu beachten (z.B. erhöhte Vorsicht bei vertraulichen Dokumenten, nicht mehr

benötigte Dateninhalte löschen...)! So sollen z.B. nur jene auf berufliche Daten zugreifen können, die sie auch für ihre Tätigkeit benötigen („kein unbeschränkter Zugriff“).

**Hinweis 2:** bei personenbezogenen „privaten“ Daten (z.B. Fotos) darf nicht vergessen werden, dass das Grundrecht auf Datenschutz und somit das Datenschutzgesetz auch im privaten Bereich gelten!

### ***Veröffentlichung auf FB via Button „teilen“ – rechtliches Problem?***

- ⇒ Beim „teilen“-Button besteht das datenschutzrechtliche Problem darin, dass Daten des Anklickers (also EIGENE Daten) im Hintergrund an den jeweiligen Betreiber des sozialen Netzwerkes gesendet werden. Dort können dann Surfprofile erstellt werden. Laut Telekommunikationsgesetz dürfen aber keine Daten ohne Zustimmung des Betroffenen an Dritte übermittelt werden. Auch im Datenschutzgesetz gibt es eine derartige Bestimmung. Daher entschließen sich immer mehr Seitenbetreiber für die Variante des „zweistufigen“ Buttons, um die User zu warnen bzw. zu informieren.

Siehe dazu: <http://www.heise.de/ct/artikel/2-Klicks-fuer-mehr-Datenschutz-1333879.html>

Unabhängig, ob ein einstufiges oder zweistufiges Verfahren verwendet wird, letztlich entscheidet der Benutzer selbst, ob er „seine“ Daten (z.B. die URL der aktuellen Seite!) an Dritte weitergibt oder nicht – bei der Verwendung firmeninterner „kirchlicher“ Accounts ist daher große Sorgfalt geboten, welche Inhalte man „teilt“, da im Hintergrund Surfprofile erstellt werden können!

Ebensolches gilt für den „like“-Button – hier kommt allerdings noch dazu, dass der zustimmende Account auf der besuchten Seite sichtbar ist! Man stimmt also einem Inhalt, einer Aussage zu – auch hier ist, wie oben, besondere Vorsicht bei nicht privaten Identitäten geboten und im Zweifelsfall eher abzuraten!

Dass auf privaten Facebookseiten etc. keine firmeninternen Daten/Informationen (personenbezogen oder nicht) veröffentlicht werden dürfen, sei sicherheitshalber noch erwähnt.

### ***Müssen Ehrenamtliche in einem Jungschlar-Dekanatsteam eine Geheimhaltungserklärung unterschreiben?***

- ⇒ JA, wenn für den Ehrenamtlichen bei der Ausübung seiner Tätigkeit ein Zugang zu Daten (personenbezogene oder sonstige kirchliche Daten) möglich oder erforderlich ist (Anwesenheitslisten, Teilnehmerlisten, Steuerlisten...). Zum Teil handelt es sich dabei sogar um sensible Daten (Sozialfälle, Obdachlose).

Die gesetzlichen Bestimmungen zum **Datengeheimnis** finden sich in § 15 Absatz 1 DSG 2000 und in § 9 Decretum Generale über den Datenschutz in der Katholischen Kirche in Österreich und ihren Einrichtungen („Kirchliche Datenschutzverordnung“).

### ***Bilder und Datenschutz:***

#### ***Ab wann ist eine Veranstaltung öffentlich?***

- ⇒ Eine Veranstaltung ist immer öffentlich, wenn sie **allgemein zugänglich** ist. Eine konkrete Zahl kann im Zusammenhang mit Bildveröffentlichungen nicht genannt werden – es kommt immer auf den **Kontext des Bildes** (und somit auf den Einzelfall) an.

Siehe dazu den sehr informativen Beitrag der Rechtsanwaltskanzlei „DBJ“:

<http://www.dbj.at/publications/vorsicht-bei-ver%C3%B6ffentlichung-von-event-fotos>

**Fazit:**

**„Vor der Veröffentlichung von Fotos von Personen sollte nach Möglichkeit deren Zustimmung eingeholt werden. Ist das im konkreten Fall nicht machbar, so ist bei der Wahl des Motivs (Person und Situation) sowie der Begleittexte Vorsicht geboten. Fotos "prominenter" Personen bzw. Aufnahmen im öffentlichen Bereich sind grundsätzlich risikoärmer, aber auch hier gibt es Grenzen. Im Zweifel sollte daher die Wahl auf ein neutrales Foto fallen, denn ein Gerichtsverfahren erzeugt außer Kosten auch negative Publicity.“**

Was ist speziell im **kirchlichen Bereich** zu beachten?

Daten (= auch Bilder) von Personen über ihre **religiöse Überzeugung** sind laut § 4 Z 2 DSGVO 2000 „**sensible Daten**“ und daher besonders schutzwürdig! Bilder also, die Personen bei der Ausübung einer religiösen Tätigkeit zeigen, können somit berechnigte schutzwürdige Geheimhaltungsinteressen verletzen -> **die Zustimmung des Betroffenen zur Bildveröffentlichung ist daher auf jeden Fall einzuholen!**

Gemäß § 78 Urheberrechtsgesetz („Recht am eigenen Bild“) dürfen Bilder von Personen dann nicht veröffentlicht werden, wenn die Veröffentlichung berechnigte (schutzwürdige) Interessen des Abgebildeten verletzen würde. Das ist u.a. dann der Fall, wenn die Fotos für Werbezwecke (auch für pfarrliche Aktivitäten/Veranstaltungen) verwendet werden oder die Person in einem negativen Kontext darstellen („bloßstellen“). Die Judikatur hat bzgl. Bildveröffentlichungen allerdings eine Rechtsprechungswende vollzogen: **demnach ist eine Fotoaufnahme, auf welcher der Abgebildete deutlich zu identifizieren ist, in der Regel nur mit Einwilligung des Abgebildeten zulässig – dies gilt dann wohl erst recht für die Veröffentlichung!**

Generell gilt bei **öffentlichen Veranstaltungen** ein weniger strenger Maßstab als bei nicht öffentlichen Veranstaltungen (wer z.B. zu einer Kirchweihe geht, muss eher damit rechnen, dass er auf einem Foto dieser Feierlichkeit veröffentlicht wird, während die Teilnehmenden an einer Bibelrunde das wohl nicht müssen). Jedoch kann selbst die Veröffentlichung eines bei einer öffentlichen Veranstaltung entstandenen Fotos gegen berechnigte Interessen einer abgebildeten Person verstoßen (z.B. eine Person wird sichtlich betrunken beim Pfarrfasching fotografiert). Es empfiehlt sich also vor jeder Veröffentlichung zu überlegen, ob ein objektiver Grund gegen diese sprechen könnte, wobei im Zweifelsfall die Genehmigung der betroffenen Person einzuholen ist.

Ist das Ziel eines Fotos, dass darauf **bestimmte Personen** (also nicht „die Menge“) abgebildet werden und werden in der Bildunterschrift unter Umständen auch noch deren Namen genannt (Gruppenfoto der Erstkommunionkinder, Firmlinge, etc.), ist vor der Veröffentlichung **jedenfalls eine Zustimmung** der Personen oder ihrer gesetzlichen Vertreter einzuholen.

Ausnahmen bestehen hinsichtlich **Personen des öffentlichen Lebens** (z.B. Mitglieder des PGR), welche grundsätzlich damit rechnen müssen, dass ihr öffentliches Handeln auch auf Fotos abgebildet und später veröffentlicht wird. Selbstverständlich dürfen aber auch in diesem Fall die Bilder nicht „wahllos“ veröffentlicht werden!

Die Veröffentlichung von Bildern, auf denen die Abgebildeten nicht oder nur sehr flüchtig erkennbar sind, bedürfen dagegen keiner Zustimmung der Abgebildeten - zumal wenn es sich, wie zuvor gesagt, um Abbildungen öffentlicher Veranstaltungen handelt (z.B. Foto vom Sommerfest der Pfarre).

Zuletzt sei noch auf Folgendes hingewiesen: das Veröffentlichen von Daten (Bildern) aus **Datenanwendungen** (also „gespeicherten“ Daten aus Archiven etc.) entspricht datenschutzrechtlich einer **Übermittlung an die Öffentlichkeit**, deren Zulässigkeit geprüft werden muss (-> **Zustimmung des Betroffenen**)!

**Achtung:** es ist immer auch die Zustimmung des (Bild-)Autors = Fotografen einzuholen!

### ***Darf ich als Dekanatsleiter Daten erfassen, sammeln, kombinieren?***

- ⇒ JA, wenn **Zweck und Inhalt** der Daten durch die beim Datenverarbeitungsregister (DVR) bereits registrierten Datenanwendungen der katholischen Kirche (etwa „Pfarrliche Seelsorge“ oder „Spendenerfassung für kirchliche Zwecke“) bzw. durch staatliche Standardanwendungen (wie etwa „Mitgliederverwaltung“) abgedeckt sind. Eine Daten-Weitergabe (Übermittlung) an eine andere kirchliche Einrichtung ist nur dann zulässig, wenn die empfangende kirchliche Einrichtung die Daten zur **Erfüllung des gleichen Zweckes** (z.B. „Seelsorge“ oder „Kirchenbeitragswesen“) benötigt, für den sie die weiterleitende kirchliche Einrichtung ermittelt hat.

### ***Krankenhaus-Besuche***

#### ***Weitergabe der Patientendaten/-listen durch das Krankenhaus***

- ⇒ Im Konkordat vom 5. Juni 1933 (BGBl II Nr. 2/1934) heißt es im Artikel XVI (**"Anstaltsseelsorge"**):

*„Für die in öffentlichen Spitälern, Heil-, Versorgungs- und dergleichen Anstalten sowie in Gefangenenhäusern, Strafanstalten, Arbeitshäusern und Anstalten für Erziehungsbedürftige und dergleichen Anstalten untergebrachten Personen wird, soweit nicht für die einzelne Anstalt im Einvernehmen mit dem zuständigen Diözesanordinarius eine eigene Anstaltsseelsorge eingerichtet ist, dem Ortsseelsorger und dem an seiner Stelle beauftragten Geistlichen das Recht des freien Zutritts zu den Anstaltsinsassen behufs freier Ausübung seines geistlichen Amtes gewährleistet.“*

Der Grundsatz der freien Seelsorge-Ausübung findet als Ausfluss der "Inneren Angelegenheiten der katholischen Kirche" (Artikel 15 Staatsgrundgesetz) in den genannten Anstalten ausdrückliche und allgemeine Anerkennung. Die Anstaltsseelsorge, also der Zutritt der Seelsorger zu allen Patienten, die der jeweiligen gesetzlich anerkannten Kirche/Religionsgesellschaft angehören, muss also gewährleistet sein. Die Krankenhaus-Verwaltung muss aus diesem Grund das Religionsbekenntnis ermitteln, um die Seelsorge durchführen zu können - es wäre sonst nicht gesichert, dass der Seelsorger zu den "richtigen" Patienten kommt (es darf keine Missionierung stattfinden) -> **der Zugang zu Personen-Stammdaten und dem Religionsbekenntnis ist daher für die Anstaltsseelsorge zulässig, nicht aber der Zugang zu Gesundheitsdaten!**

**Hinweis:** die Kombination aus Gesundheitsdaten (das Wissen um einen Spitalsaufenthalt) und dem Religionsbekenntnis ist äußerst sensibel und es ist daher mit großer Vorsicht zu handeln -> **nur ausdrücklich dafür autorisierte Personen dürfen Zugang zu den Patientenlisten haben!**

### **Bezgl. Geheimhaltungserklärung**

***Darf ich wirklich alles, was ich „bei Gelegenheit erfahren“ habe, nicht mit KollegInnen besprechen?***

***Die unterliegen ja auch der Dienstverschwiegenheit! (z.B.: Ich erfahre von schwerer Erkrankung einer Ehrenamtlichen MA! Darf ich das an KollegInnen weitersagen? Weil das für die Arbeit wichtig ist!)***

- ⇒ Das Grundrecht auf Datenschutz, geregelt im § 1 DSG 2000, besagt u.a., dass „jedermann, insbesondere auch im Hinblick auf die **Achtung seines Privat- und Familienlebens**, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten hat, soweit ein schutzwürdiges Interesse daran besteht.“

Die Verpflichtungserklärung auf das Datengeheimnis lt. § 15 DSG bedeutet nicht, dass man privat „nichts mehr sagen darf“, sondern dass Daten, **die ausschließlich aufgrund der berufsmäßigen Beschäftigung anvertraut oder zugänglich gemacht wurden (z.B. aus Datenanwendungen), grundsätzlich geheim zu halten sind und nur unter ganz bestimmten Voraussetzungen übermittelt/weitergegeben werden dürfen** („bei Gelegenheit erfahren“ bezieht sich auf diese firmeninternen Daten und bedeutet in dem Zusammenhang z.B., man findet einen nicht abgeholten Ausdruck beim Drucker oder hört unabsichtlich ein Gespräch mit).

Ein **Datenaustausch** unter Kollegen des **gleichen Aufgabengebietes** ist möglich, nicht aber zwischen **verschiedenen** Aufgabengebieten. Beispiel: ein Kirchenbeitragsmitarbeiter kann Daten eines Beitragspflichtigen mit einem anderen Kirchenbeitragsmitarbeiter (im Rahmen der beruflichen Tätigkeit!) besprechen, nicht aber mit einem Dekanatsassistenten. Die Sicherheitsbestimmungen des Datenschutzgesetzes fordern weiters, dass eine auf Daten zugreifende Person nur Einblick in jene Daten erhalten soll, die für die Erfüllung ihrer Aufgaben berufsgruppenspezifisch erforderlich sind.

Gesundheitsdaten sind laut § 4 Z 2 DSG 2000 **sensible Daten** – daher ist besondere Vorsicht geboten! Natürlich wird es erlaubt sein, von Erkrankungen = Absenzen zu sprechen, wenn dies für die Arbeit im konkreten Team relevant ist (ob die Art der Krankheit eine Rolle spielt, ist fraglich -> Privatsphäre) – sicher **nicht erlaubt** ist allerdings, diesbezügliche Informationen aus **internen Datenanwendungen** (z.B. einem Personalakt, Krankenstandsbestätigungen etc.) unbefugt zu verbreiten (-> siehe oben: Dienstgeheimnis, Geheimhaltungserklärung)!

### ***DVR-Nummer für Jugendleiter für E-Mails?***

- ⇒ Ja! Die Datenschutzbehörde empfiehlt, die DVR-Nummer standardmäßig in **jedem Schreiben** an Betroffene anzuführen. Dies kann beispielsweise durch Aufnahme der DVR-Nummer in den Brief- bzw. E-Mail-Kopf und/oder Fuß geschehen. Jugendleiter/Jugendleiterinnen sind Mitarbeiter/Mitarbeiterinnen der **Abteilung Pastorale Berufe** und haben als solche in ihren Signaturen (Brief, Mail) die DVR-Nummer der Abteilung Pastorale Berufe zu verwenden.  
**DVR: 0029874(1871)**

### ***Innerbetriebliche Datenweitergabe? Zugang Pfarrkarteien, Jugendleiter und Dekanatsassistent?***

- ⇒ Ein zentraler Grundsatz im Datenschutzgesetz ist der sogenannte „Zweckbindungsgrundsatz“ im § 6 Absatz 1 Z 2 DSG 2000: „**Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden.**“ Wenn Daten also für einen bestimmten Zweck rechtmäßig ermittelt wurden, dürfen sie auch nur für diesen Zweck verwendet werden (z.B. im Kirchenbeitrag). Weiters gilt, **dass Mitarbeiter nur Zugang zu jenen Daten haben sollen,**

**welche sie für ihre Tätigkeit benötigen** („nur jene für die Arbeit notwendigen Daten“). Eine innerbetriebliche Datenweitergabe ist demnach in gewissen Grenzen möglich, wenn (rechtmäßig erhobene) Daten innerhalb ihres „Zweckes“ bleiben bzw. nur dort verwendet werden (z.B. für den Zweck „Pfarrliche Seelsorge“), ansonsten wären es **Übermittlungen**, für die man jeweils Rechtfertigungsgründe (z.B. die Zustimmung der Betroffenen zur Datenweitergabe) bräuchte. Die **Kirchliche Datenschutzverordnung** („Decretum Generale über den Datenschutz in der Katholischen Kirche in Österreich und ihren Einrichtungen“) erlaubt im § 7 Absatz 1 und Absatz 2 die Datenweitergabe im kirchlichen Bereich (also zwischen kirchlichen Einrichtungen) unter gewissen Voraussetzungen, nämlich dann, wenn:

- sie zur **Erfüllung des kirchlichen Auftrages** erforderlich ist, welche entweder der weitergebenden oder der empfangenden Einrichtung obliegt („Pastoraler Zweck“).
- die empfangende kirchliche Einrichtung die Daten zur **Erfüllung des gleichen Zweckes** (z.B. „Pfarrliche Seelsorge“ oder „Kirchenbeitragswesen“) benötigt, für den sie die weiterleitende kirchliche Einrichtung ermittelt hat.

Bei jeglicher Datenweitergabe ist natürlich immer auch zu beachten, dass keine schutzwürdigen Geheimhaltungsinteressen der Betroffenen verletzt werden bzw. dass das Datengeheimnis gewahrt bleibt. Im Zweifelsfall ist daher immer Rücksprache mit dem Datenschutzbeauftragten zu halten.

Regeln für die innerbetriebliche Datenweitergabe bzw. für die Zugriffe auf Daten allgemein („Wer darf auf welche Daten zugreifen?“) sind ein zentraler Punkt für das Design der **ÖKD-Neu** und werden derzeit laufend diskutiert und ausgearbeitet.

#### **Austrittswillige – Kontakt – aufnehmen – Erlaubt?**

- ⇒ Das Kontakt-Aufnehmen zu Austrittswilligen durch dafür autorisierte Mitarbeiter gehört zu den Aufgaben der pfarrlichen Seelsorge und ist an sich kein datenschutzrechtliches Problem, wenn die Pfarre offiziell vom Austrittswilligen verständigt wurde (eine Kontaktaufnahme aufgrund „Hörensagens“ halte ich nicht für sinnvoll bzw. hängt diese vom Einzelfall ab, da die Frage im Raum steht, „woher man das weiß“). Grundsätzlich gilt natürlich auch hier - wie bei allen anderen Informationen, **die den Mitarbeitern ausschließlich aufgrund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind** – das Datengeheimnis. Somit sind Informationen über Austrittswillige oder bereits Ausgetretene **geheim** zu halten (nach „Außen“) und („Innen“) nur an jene Mitarbeiter weiterzugeben, die diese Information für ihre Tätigkeit tatsächlich benötigen (Seelsorge).

**Als (Basis-)Mitarbeiterin in der Pfarre: dass Ehrenamtliche ganz generell zu den "Dritten" zählen finde ich mit Blick auf die Organisationsstruktur unserer Kirche schon recht eigenwillig und nicht ganz realitätsnah. Oder kommen da ganz konkrete Bestimmungen / zu Unterzeichnendes auch auf die Ehrenamtlichen zu?**

- ⇒ "Dritter" ist ein juristischer Begriff und kein Begriff, der klassifizieren oder werten soll. Ein Rechtsverhältnis, typischerweise ein Vertrag, besteht meistens zwischen 2 Personen oder zwischen 2 Personenkreisen. Ein Dritter ist jeder, der nicht zu diesen beiden Personen bzw. Personenkreisen gehört. Im konkreten Fall "Kirche" haben wir **Hauptamtliche**, also Mitarbeiter mit einem **Arbeitsvertrag**, und **Ehrenamtliche**, die ihre hochgeschätzte Tätigkeit freiwillig, also **OHNE** Vertrag, erbringen. Daher sind diese, aus juristischer Sicht, "Dritte".

- ⇒ Ehrenamtliche Mitarbeiter haben nur dann eine **Vertraulichkeitserklärung** (eigenes Dokument für Ehrenamtliche) zu unterzeichnen, wenn sie bei ihrer Tätigkeit mit personenbezogenen oder wirtschaftlichen/steuerlichen Daten in Berührung kommen.

***Wir in den Altenheimen geben den Herkunftspfarrern oft die Namen neuer Bewohnerinnen weiter, damit diese von den Besuchsdiensten heimgesucht werden. Sollen wir künftig die Bewohnerinnen bzw. ihre Angehörigen beim Einzug um ihr Einverständnis dafür bitten?***

- ⇒ Grundsätzlich gilt: vorher (z.B. bei der Aufnahme) eine **Zustimmung** einzuholen ist immer der beste, einfachste und datenschutzrechtlich sauberste Weg - in dem Fall wäre auch gleich geklärt, ob der Bewohner/die Bewohnerin den Besuchsdienst überhaupt in Anspruch nehmen möchte.
- ⇒ Für die "**Anstaltsseelsorge**" im Speziellen gilt übrigens Folgendes: **im Konkordat vom 5. Juni 1933** (BGBl II Nr. 2/1934) heißt es im **Artikel XVI**:
- ⇒ "Für die in öffentlichen Spitälern, Heil-, Versorgungs- und dergleichen Anstalten sowie in Gefangenenhäusern, Strafanstalten, Arbeitshäusern und Anstalten für Erziehungsbedürftige und dergleichen Anstalten untergebrachten Personen wird, soweit nicht für die einzelne Anstalt im Einvernehmen mit dem zuständigen Diözesanordinarius eine eigene Anstaltsseelsorge eingerichtet ist, dem Ortsseelsorger und dem an seiner Stelle beauftragten Geistlichen das Recht des freien Zutritts zu den Anstaltsinsassen behufs freier Ausübung seines geistlichen Amtes gewährleistet."
- ⇒ Das heisst: die Anstaltsseelsorge, also der Zutritt der **Seelsorger** zu allen Patienten/Bewohnern, **die der jeweiligen gesetzlich anerkannten Kirche/Religionsgesellschaft angehören**, muss also gewährleistet sein.

Zusammenfassend:

- Der Zugang zu Personen-Stammdaten (Namen) und dem Religionsbekenntnis ist daher für die **Anstaltsseelsorge** zulässig.
- Es dürfen nur die Daten der **Katholiken** an die Seelsorge weitergegeben werden -> keine "Missionierung"!
- Die Daten dürfen nur an ausdrücklich für die **Anstaltsseelsorge** berechnete Mitarbeiter weitergegeben werden (z.B. Mandat durch Ortsseelsorger/Pfarrer).

***Wir arbeiten als mehr oder minder ins System integrierte Gäste in den Häusern und nutzen deren (Infra-)Struktur. Das heißt, dass wir auf etliche in den neuen Bestimmungen genannten Regelungen keinen Einfluss haben - z.B. ob das Büro (sofern überhaupt vorhanden) versperrbar oder nicht doch mit einem weit verbreiteten Schlüssel zugänglich ist, wo der Drucker steht usw. Wir nutzen EDV und Ausstattung "Dritter" wie das so schön heißt - und wollen auch keine schlafenden Hunde wecken (etwa dass der Drucker nicht mehr im luftigen Foyer steht sondern in die Büroräume wandert und dort die Atemluft der Sekretärinnen verpestet). Sollen wir den Umstand, dass einiges in den Richtlinien Angeführte nicht in unserer Gestaltungskompetenz liegt, irgendwo offiziell deponieren? Ist es nötig, dass wir uns systematisch mit den entsprechenden Richtlinien der jeweiligen Träger vertraut machen und diese einhalten?***

- ⇒ Grundsätzlich sind die Häuser datenschutzrechtlich für ihre Infrastruktur **selbst verantwortlich** und haben sicher "eigene" Vorgaben - sich mit diesen zumindest grob vertraut zu machen, kann keinesfalls schaden, wenn man diese Infrastruktur nutzt [zur eigenen Absicherung] - wobei der Datenschutz unabhängig von Hausregeln so und so einzuhalten ist. Ansprechen würde ich grobe Unzulänglichkeiten (z.B. Patientenakten liegen am Gang oder dergleichen). Das Wichtigste ist, sensibilisiert auf das Thema Datenschutz und Datensicherheit zu sein - es sind oft kleine Dinge mit großer Wirkung: z.B. den Bildschirm

sperrern wenn man das Büro verlässt oder Ausdrucke nicht lange unbeaufsichtigt beim Drucker liegen lassen.

**Hinweis:** da es sich bei oben genannten Informationen um Daten über die religiöse Überzeugung handelt, sind diese zudem als **sensibel** einzustufen!

*Kontakt:*

*Mag. Alexander Marktler*

*E-Mail: alexander.marktler@dioezese-linz.at*