

SELBSTÄNDIGE EVANGELISCH-LUTHERISCHE KIRCHE

DER KIRCHLICHE BEAUFTRAGTE FÜR DEN DATENSCHUTZ



**Anwendungsempfehlungen für die
Richtlinie über den Datenschutz in der Selbständigen Evangelisch-Lutherischen Kirche
vom 02.05.2018 (RDS-SELK) in ihrer letzten Fassung vom 24.05.2019**

Version vom 01.03.2021 (2.4)

1. Anwendungsbereich

Die Richtlinie für den Datenschutz in der SELK (RDS-SELK) gilt für die Verarbeitung personenbezogener Daten durch die Selbständige Evangelisch-Lutherische Kirche (SELK) sowie die ihr zugeordneten kirchlichen und diakonischen Dienste, Einrichtungen, Gemeinden und Werke ohne Rücksicht auf deren Rechtsform (kirchliche Stelle).

Die RDS-SELK stellt nach Art. 91 der Verordnung (EU) 2016/679 des Europäischen Parlamentes und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, kurz: DSGVO) in Verbindung mit Art. 137 Abs. 3 der Weimarer Reichsverfassung (WRV) und Art. 140 des Grundgesetzes (GG) eine eigenständige Datenschutznorm für alle Einrichtungen der Evangelisch-Lutherischen Kirche dar.

Die RDS-SELK geht damit der DSGVO vor. Sie ist die für die SELK und ihre Gemeinden und Einrichtungen einzig verbindliche Datenschutzrichtlinie.

2. Anwendungsfälle und Anwendungsgrundsätze

Personenbezogene Daten dürfen auch nach der RDS-SELK nur nach bestimmten Grundsätzen verarbeitet werden. Diese **Grundsätze** sind im § 5 detailliert aufgeführt.

Hervorzuheben sind:

- **Zweckbindung:** Jeder bekommt und verarbeitet nur die Daten, die er für die Erfüllung seines kirchlichen Auftrages benötigt; wer den Gemeindebrief verteilt, braucht nur die Adressen der Empfänger, nicht jedoch deren Taufdatum.
- **Datenminimierung:** Es wird nur das personenbezogen gespeichert, was erforderlich ist. Beitragslisten lassen sich (häufig) pseudonymisieren.
- **Integrität und Vertraulichkeit:** Es muss gewährleistet sein, dass nur derjenige Zugriff auf Daten hat, der auch die Berechtigung dazu besitzt. Das bedeutet, dass Kirchenbücher und

Karteien unter Verschluss zu halten sind. Es bedeutet, dass EDV-gestützte Systeme zu sichern sind (Zugriffs- und Passwortschutz, Verschlüsselung).

Evident abweichend von den Regelungen der DSGVO ist die umfassende Definition von Datenverarbeitung in § 2 Abs. 2 RDS-SELK. Die Bestimmungen der RDS-SELK gelten nicht nur für die automatisierte Datenverarbeitung (mit Computern), sondern auch für Verfahren, die nicht EDV-gestützt sind. Das heißt: Auch das Führen einer „klassischen“ Gemeindekartei auf Karteikarten oder eines Kirchenbuchs zählt als Verarbeitung von Daten.

Zu beachten ist, dass es eine „**besondere Kategorie personenbezogener Daten**“ gibt, zu denen nach § 2 Abs. 2 lit. a) RDS-SELK auch Angaben zur religiösen Überzeugung gehören. Die Zugehörigkeit zu einer Kirche ist davon ausdrücklich ausgenommen, nicht jedoch Daten, die auf religiöse Praxis schließen lassen, wie etwa Einträge in einem **Kommunikantenverzeichnis**. Bei diesen Daten ist besondere Sorgfalt geboten.

3. Datenschutzüberwachung und -aufsicht

Nicht jede Gemeinde oder Einrichtung der SELK braucht einen **eigenen Datenschutzbeauftragten**. Auch in dieser Frage hat die RDS-SELK eine andere Grundrichtung eingeschlagen als die DSGVO. Für die Einhaltung der Bestimmungen des Datenschutzes in den Gemeinden und Einrichtungen sollen auf Dauer vielmehr **Regionale Datenschutzbeauftragte** (§§ 36 bis 38 RDS-SELK) zuständig sein, die primäre Ansprechpartner der Gemeinden und Gemeindeglieder bzw. der Einrichtungen sein werden und die verantwortlichen kirchlichen Stellen bei der Sicherstellung des Datenschutzes unterstützen. Im Wesentlichen sollen diese die Gemeinden und sonstigen kirchlichen Stellen bei der Sicherstellung des Datenschutzes unterstützen und entsprechende Hilfen und Hinweise geben.

Es ist beabsichtigt, in der SELK insgesamt vier Regionale Datenschutzbeauftragte zu bestellen. Diese werden derzeit von der Kirchenleitung gesucht. Die Stellen sind somit gegenwärtig vakant, sodass die kirchlichen Stellen vorerst allein für die Umsetzung der RDS-SELK sorgen müssen.

Den Regionalen Datenschutzbeauftragten übergeordnet ist der **Kirchliche Datenschutzbeauftragte** (§§ 39 ff. RDS-SELK) als unabhängige Aufsichtsbehörde für den Datenschutz in der gesamten SELK. Ihm obliegt die Überwachung der Einhaltung der RDS-SELK, allerdings nicht proaktiv, sondern nur auf die Beschwerden oder Eingaben kirchlicher Stellen oder von Datenverarbeitung betroffener Personen.

4. Sofort-Pflichten aller kirchlichen Stellen

Jede von Datenverarbeitung betroffene Person hat das Recht zu erfahren, welche Daten von ihr verarbeitet und wie mit ihren Daten umgegangen wird. Um dieser Informationspflicht kurzfristig nachkommen zu können, muss bei jeder datenverarbeitenden kirchlichen Stelle intern geklärt werden, wie der Umgang mit und die Verarbeitung von Daten erfolgt. Jede kirchliche Stelle muss insoweit rechenschaftsfähig sein.

Die RDS-SELK statuiert deshalb eine Pflicht zur Führung von **Verarbeitungsverzeichnissen**. § 31 RDS-SELK verpflichtet jede verantwortliche Stelle, die mindestens 250 Beschäftigte hat, ein um-

fassendes Verzeichnis zu führen, das Angaben über alle Verarbeitungstätigkeiten enthalten muss. Einzelheiten sind in § 31 Abs. 1 RDS-SELK geregelt. Verantwortliche Stellen, die weniger als 250 Beschäftigte haben, müssen ein „abgespecktes“ Verzeichnis führen, das Angaben nur hinsichtlich der Verfahren zu enthalten hat, die die Verarbeitung besonderer Kategorien personenbezogener Daten einschließen.

Das Verzeichnis ist der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.

Es empfiehlt sich aber, das Verarbeitungsverzeichnis nicht erst zu erstellen, wenn die Aufsichtsbehörde anfragt, denn bereits die Erstellung verschafft jeder kirchlichen Stelle eine gute Gelegenheit, sich über die Art und den Umfang der eigenen Datenverarbeitungsvorgänge klar zu werden.

Der Kirchliche Datenschutzbeauftragte veröffentlicht als Hilfe zum Erstellen dieser Verzeichnisse wird ein Muster, das auf <https://www.selk.de/index.php/datenschutz> abrufbar sein wird. Solange dieses Muster nicht online zur Verfügung steht, ist auch keine überstürzte Eile angesagt. Zwar setzt die RDS-SELK in § 55 Abs. 3 eine Frist zur endgültigen Fertigstellung bis zum 30.06.2019; die Durchsetzung dieser Bestimmung durch den Kirchlichen Datenschutzbeauftragten wird aber vorläufig ausgesetzt.

5. Pflichten auf Anforderung des Betroffenen im Einzelfall

Zu beachten ist **Informationspflicht** der datenverarbeitenden Stellen (korrespondierend zu den in Abschnitt 4 dargestellten Rechten der betroffenen Personen). Anders als die DSGVO für den weltlichen Bereich besteht innerhalb der SELK diese Pflicht nach § 17 Abs. 1 RDS-SELK aber nur „auf Verlangen“. Eine unaufgeforderte, vorausseilende Informationspflicht besteht danach nicht.

Da aber schon innerhalb der SELK kaum bekannt ist, dass nicht die DSGVO, sondern die RDS-SELK Maßstab für Datenschutz und Informationspflichten ist, wird allen verantwortlichen kirchlichen Stellen empfohlen, auf ihren Internetseiten zumindest folgenden Hinweis zu erteilen:

Datenverarbeitende Stelle ist *[Name und Anschrift]*, ein/e der Selbständigen Evangelisch-Lutherischen Kirchen angehörig/e ... *[Gemeinde, diakonischer Dienst, Einrichtung...]* Der Datenschutz in der SELK und allen ihr zugeordneten kirchlichen und diakonischen Diensten, Einrichtungen, Gemeinden und Werken ohne Rücksicht auf deren Rechtsform unterliegt wegen des verfassungsrechtlichen Grundsatzes der kirchlichen Selbstverwaltung nicht der Europäischen Datenschutzgrundverordnung (DSGVO), sondern eigenen Regeln zum Schutz natürlicher Personen bei der Verarbeitung von personenbezogenen Daten, der „Richtlinie für den Datenschutz in der SELK“ (kurz: RDS-SELK). Diese ist abrufbar unter: https://www.selk.de/download/datenschutz/Richtlinie-Datenschutz-SELK_05-2019.pdf

Anders als nach Art. 13 DSGVO besteht für die SELK und ihre kirchlichen Stellen eine Informationspflicht der betroffenen Person über Art, Zweck und Umfang der Datenverarbeitung nicht bereits bei Erhebung von personenbezogenen Daten, sondern erst auf Verlangen der betroffenen Person (§ 17 Abs. 1 RDS-SELK). Ihr Auskunftsverlangen richten Sie bitte an *[Ansprechpartner – nicht den Namen des Regionalen Datenschutzbeauftragten oder etwa des Kirchlichen Datenschutzbeauftragten!]*.

Empfohlen wird, für den Fall des Auskunftsverlangens ein Informationsblatt vorzubereiten. Der Kirchliche Datenschutzbeauftragte wird als Hilfe zum Erstellen dieser Information ein Muster veröffentlichen, das auf <https://www.selk.de/index.php/datenschutz> abrufbar sein wird.

Sollten Beschwerden von Betroffenen in der kirchlichen Stelle eingehen, sind diese zuständigkeithalber dem Kirchlichen Datenschutzbeauftragten weiterzuleiten. Für Anfragen und Erläuterungsbitten von Betroffenen ist hingegen der jeweilige Regionale Datenschutzbeauftragte zuständig (sobald dieser bestellt ist).

Die verantwortliche Stelle ist hingegen zur anlasslosen, **unverzüglichen Meldung von Verletzungen des Schutzes personenbezogener Daten an den Kirchlichen Datenschutzbeauftragten** als Aufsichtsbehörde verpflichtet, wenn diese Verletzung voraussichtlich zu einem nicht unerheblichen Risiko für die Rechte natürlicher Personen führt (§ 32 Abs. 1). Hat die **Verletzung voraussichtlich ein hohes Risiko für die persönlichen Rechte des Betroffenen** zur Folge, hat die verantwortliche Stelle die betroffene Person unverzüglich von der Verletzung zu benachrichtigen (§ 33 Abs. 1).

Was „unverzüglich“ bedeutet, ist in der RDS-SELK nicht ausdrücklich geregelt. Nach den Maßstäben der DSGVO und des Bundesdatenschutzgesetzes ist von „innerhalb 72 Stunden“ ab Kenntnis der verantwortlichen Stelle auszugehen.

6. Weitergabe von Daten

Sorgfalt ist angezeigt bei der **Übermittlung und Offenlegung von Daten an Dritte** (§§ 8 ff.). Es wird vorausgesetzt, dass bei der Weitergabe von Daten (die nur unter bestimmten Voraussetzungen erlaubt ist) die empfangende Stelle das in der RDS-SELK geforderte Niveau des Datenschutzes einhält. Bei der kirchlichen Überweisung von einer Gemeinde der SELK in eine andere ist dies kein Problem, da beide der RDS-SELK unterliegen.

Schwieriger wird es bei der Übermittlung von Daten an **außereuropäische und internationale Organisationen**. Bei einer kirchlichen Überweisung etwa in eine Gemeinde der LC-MS ist vorher die Einwilligung der betroffenen Person einzuholen und diese über unterschiedliche Regelungen zum Datenschutz zu informieren (§ 10 Abs. 2).

7. Einzelfragen

- **Abendmahl, Teilnehmerlisten**

Die Teilnahme am Heiligen Abendmahl stellt eine Information dar, aus der eine religiöse Überzeugung hervorgeht; zusammen mit dem Namen des Teilnehmers wird dies ein sog. „**besonderes personenbezogenes Datum**“, das nach § 13 Abs. 1 RDS-SELK grundsätzlich nicht verarbeitet werden darf. § 13 Abs. 2 RDS-SELK stellt einen Erlaubnisvorbehalt für dieses generelle Verbot auf. Nur in den dort definierten Fällen ist eine Verarbeitung ausnahmsweise zulässig ist.

Das **Führen namentlicher Listen** von Teilnehmern am Heiligen Abendmahl ist beispielsweise zu seelsorgerischen Zwecken zulässig. Die Namens-Listen sind allerdings als pfarramtsinterne Dokumente streng vertraulich zu behandeln und ausschließlich für den Pastor zur Erfüllung seines seelsorgliche Auftrag zu verwenden, ggf. noch für andere Personen, die diesem Auftrag nachkommen oder den Pastor hierin wesentlich unterstützen.

Die Listen können aus den üblichen namentlichen Anmeldungen in der Sakristei mit den Einträgen in ein (nicht öffentliches) **Kommunikantenbuch** erstellt werden. Ein Auslegen von Listen in der Kirche oder im Gemeindesaal, in welche sich die Teilnehmer am Abendmahl namentliche eintragen können oder sollen, verstößt gegen das datenschutzrechtliche Vertraulichkeitsgebot und stellt somit regelmäßig eine Datenschutzverletzung dar. Denn die bloße Eintragung in eine Teilnehmerliste wird den Anforderungen an eine ausdrückliche Einwilligung nach § 11 RDS-SELK in die Erhebung besonderer personenbezogener Daten nicht gerecht. Wird das Kommunikantenbuch nur zu Zwecken statistischer Auswertung geführt, dürfte die Erhebung von Namen aber generell nicht erforderlich sein.

Das gleiche gilt generell auch für die **Weitergabe von nicht-anonymisierten Liste**. Diese ist **unzulässig**. Eine Übermittlung solcher Namenslisten wäre nicht einmal an die Kirchenleitung zur statistischen Auswertung zulässig. Die Kirchenleitung hat dementsprechend zu keiner Zeit namentliche Listen von Abendmalsteilnehmenden gefordert. Sie erfasst in einer Statistik lediglich die nicht mit Namen verknüpften Zahlen von Teilnahmen am Heiligen Abendmahl, die im Laufe eines Jahres am Abendmahl teilnehmen, differenziert nach Gemeindegliedern und Gästen. Die Übermittlung dieser Daten durch die Gemeinden hat daher in einer anonymen, rein zahlenorientierten Auswertung zu erfolgen.

- **Beitragserhebung**

Die Verarbeitung von personenbezogenen Daten zu Zwecken der **Beitragserhebung** und **Abwicklung von Spenden** innerhalb der Finanzkommission eine Gemeinde oder sonstigen kirchlichen Stelle ist ohne Einwilligung der Betroffenen zulässig. Sie ist jedenfalls durch § 6 Ziff. 3, 4, 6 und 8 RDS-SELK legitimiert.

Bei der Behandlung der Daten sind die erforderlichen technischen und organisatorischen Maßnahmen zum Schutz der Daten und die Grundsätze der Datenverarbeitung nach § 5 RDS-SELK zu beachten. Dazu gehört der Grundsatz der Datensparsamkeit, die Beachtung der Zweckbindung und der Vertraulichkeit.

- **Cloud-Dienste**

Online-Speicher, Filehosting- oder „Cloud-Dienste“ wie **iCloud, Dropbox oder OneDrive** werden regelmäßig auf Server außerhalb der EU betrieben. Die Dienste unterliegen damit regelmäßig nicht der DSGVO, sondern unterfallen dem Datenschutzrecht anderer Länder, die häufig nicht das gleiche Datenschutzniveau gewährleisten. So hat beispielsweise der EuGH das Datenschutzniveau in den USA als nicht ausreichend erachtet, als dass eine Übermittlung von Daten auf Server in Übersee generell zulässig wäre. Die Nutzung außereuropäischer Cloud-Dienste ist daher datenschutzrechtlich unzulässig, wenn personenbezogene Daten betroffen sind.

Sicherere und vor allem datenschutzrechtlich unbedenkliche Alternativen bieten unter anderen die Deutsche Telekom (mit der „MagentaCloud“), von Strato (mit „HiDrive“) oder das niederländische „WeTransfer“.

- **E-Mail**

E-Mail ist heute immer noch eines der wichtigsten Kommunikationsmittel. Leider aber auch eines der unsichersten. Mails werden in der Regel unverschlüsselt über das Netz übertragen. Darüber hinaus wird die Mail-Technik auch intensiv missbraucht, um Malware, Phishing-Links und ähnliches zu übertragen. Das hängt vor allem mit den geringen Kosten und der Einfachheit, an riesige Mengen von Mail-Adressen zu kommen, zusammen.

Vor der Versendung von personenbezogenen Daten in unverschlüsselten E-Mails sollte deshalb die Einwilligung aller Betroffenen (damit ist nicht nur der Empfänger der Mail gemeint, sondern alle Personen, deren personenbezogenen Daten in der E-Mail enthalten sind) eingeholt werden. Liegt die Einwilligung nicht aller Betroffenen vor, wird der Versand von E-Mails mit Inhaltsverschlüsselung (beispielsweise als passwortgesicherte PDF-Datei) oder Transportverschlüsselung (S/MIME, OpenPGP) empfohlen. Beide Verfahren sind im nichtkommerziellen Bereich kostenlos erhältlich). Selbst die Verwendung von SSL oder eines gesicherten SMTP-Servers ist eigentlich nicht ausreichend, da diese nur die Übermittlungssicherheit vom Versender bis zu dessen eigenen Mailserver herstellt, die Weiterleitung der Mail auf dem weiteren Übertragungsweg aber ungesichert erfolgen kann.

Sollte keine wirtschaftlich vertretbare Alternative zur Versendung personenbezogener per E-Mail vorhanden sein (dies ist nur der Fall, wenn der Empfänger Nutzung von Transport- oder Inhaltsverschlüsselung technisch nicht bewerkstelligt), ist diese nach § 27 RDS-SELK unter Abwägung der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen auf die Versendung „einfacher“ personenbezogener Daten zu beschränken. Die unverschlüsselte **Versendung von personenbezogenen Daten, die einer besonderen Kategorie nach § 13 i.V.m. § 4 Ziff. 2 RDS-SELK angehören** (namentlich Informationen über religiöse oder weltanschauliche Überzeugungen, rassische und ethnische Herkunft, politische Meinungen oder die Gewerkschaftszugehörigkeit, genetische Daten, biometrische Daten, Gesundheitsdaten sowie Informationen zum Sexualleben oder der sexuellen Orientierung) ist **ausnahmslos nicht zulässig**, ohne dass diese Daten zuvor pseudonymisiert oder anonymisiert wurden. Das gilt selbst dann, wenn die betroffene Person ihre Einwilligung erteilt hat.

- **Gemeindebrief**

In Druckausgaben werden üblicherweise Jubiläen, Amtshandlungen, (hohe) Geburtstage, Ein- und Austritte veröffentlicht. Das ist ohne Einwilligung des Betroffenen nicht zulässig.

In eine elektronische Ausgabe gehören diese Daten auf keinen Fall! Auch bei Bildern wäre ich zurückhaltend, zumindest bei solchen, auf denen Personen erkennbar sind. Was spricht dagegen, Gottesdiensttermine und einzelne Berichte aus dem Gemeindebrief online zu stellen, nicht aber das gesamte Werk? Zunehmend bekomme ich mit, dass (gedruckte) Gemeindebriefe als eine Art Werbung oder Selbst-darstellung in der Umgebung verteilt

werden. Das ist gut so, zumal viele auch eine gute Qualität haben. Kritisch wird es dann mit den persönlichen Daten. Wäre es eine Idee, den Gemeindebrief selbst ohne diese Daten zu gestalten und diese dann in einem Einlegeblatt beizugeben? Beim gedruckten Gemeindebrief empfehle ich, gelegentlich auf den Umgang mit solchen Jubiläen etc. hinzuweisen und darauf, dass man einer Veröffentlichung widersprechen kann.

(für elektronische Ausgaben des Gemeindebriefs: → „Internet-Veröffentlichungen“)

- **Gemeindeliste**

Darf eine Gemeindeliste erstellt und allgemein verteilt werden? Im Prinzip: Nein! Ein Gebetskreis braucht natürlich die Namen derjenigen, für die er beten soll. Ein Besuchsteam braucht entsprechende Adressen. Menschen, die bestimmte Aufgaben in der Gemeinde haben, sollen die Informationen erhalten (auch personenbezogene Daten), die sie für die Erfüllung ihrer Aufgaben benötigen (und sie auch nur dafür verwenden). Wichtig: Alle Mitarbeitenden in Gemeinden/Einrichtungen sollen auf die Einhaltung der Datenschutzvorschriften hingewiesen werden.

- **Gottesdienst, Video-Übertragung**

Besondere Regelungen hält die RDS-SELK auf für **Aufzeichnung oder Übertragung von Gottesdiensten oder kirchlichen Veranstaltungen** parat (§ 53). Diese ist grundsätzlich zulässig.

Eine Videoübertragung von Gottesdiensten ist nach § 53 RDS-SELK **generell zulässig**, allerdings nur, wenn die Teilnehmenden durch geeignete Maßnahmen über Art und Umfang der Aufzeichnung oder Übertragung informiert werden. Dies kann auf unterschiedlichen Wegen erfolgen.

Außerdem gibt es eine vorlaufende Informationspflicht (Gottesdienstbesucher müssen wissen, dass, was und welcher Bereich aufgezeichnet/übertragen wird). Den Gemeinden und Einrichtungen, die sich auf eine Umfrage des Kirchenbüros hin gemeldet haben (dass dort aufgezeichnet/übertragen würde oder werden sollte), wurden bereits weitere Informationen und Empfehlungen zukommen gelassen.

Denkbar ist beispielsweise, an allen Eingängen der Gottesdienstraumes einen entsprechend deutlich zu lesenden Hinweis anzubringen. Außerdem sollte im Gottesdienstzettel und im Gemeindebrief deutlich auf die Videoaufnahmen hingewiesen werden. Wichtig ist dabei, dass alle Teilnehmenden des Gottesdienstes durch geeignete Maßnahmen über Art und Umfang der Aufzeichnung und der Übertragung in den Nachbarraum informiert werden.

Zusätzlich ist § 52 RDS-SELK („Videoüberwachung öffentlich zugänglicher Räume“) zu beachten (siehe Stichwort „Videoüberwachung“). Dieser bestimmt in Abs. 1 S. 2, dass das Interesse an der nicht überwachten **Teilnahme am Gottesdienst besonders schutzwürdig** ist. Es ist deshalb bei der Video-Übertragung von Gottesdiensten stets darauf zu achten, dass in der Gemeinde keine Einzelpersonen erkennbar werden, die lediglich an dem Gottesdienst teilnehmen, also nicht beispielsweise durch Übernahme besonderer Aufgaben (Mitwirken im Chor, musikalische Unterstützung, Lektorat usw.) aus der

amorphen Menge der Teilnehmenden heraustreten. Namentlich der Pastor ist durch § 52 Abs. 1 S. 2 RDS-SELK nicht geschützt.

Auch wenn in der RDS-SELK keine Regelung getroffen wurde, wie mit der Darstellung von Teilnehmenden am **Heiligen Abendmahl** zu verfahren ist, ist unter Berücksichtigung der datenschutzrechtlichen Grundsätze der Zweckbindung (§ 5 Abs. 1 Ziff. 2 RDS-SELK) und der Datenminimierung (§5 Abs. 1 Ziffer 3 RDS-SELK) zu berücksichtigen, dass eine Aufzeichnung und Übertragung des Abendmahls stets problematisch ist. Personenbezogene Daten dürfen generell nur für festgelegte, eindeutige und legitime Zwecke erhoben werden, wobei die Verarbeitung personenbezogener Daten auf das dem Zweck angemessene und notwendige Maß zu beschränken ist. Die personell zuordnungsfähige Teilnahme am Heiligen Abendmahl stellt überdies eine Information dar, aus der die religiöse oder weltanschauliche Überzeugung der identifizierbaren natürlichen Person hervorgeht, und damit „besondere Kategorie personenbezogener Daten“ im Sinne von § 4 Ziff. 2 a) RDS-SELK. Diese sind nach § 13 RDS-SELK besonders geschützt und dürfen generell nur in Ausnahmefällen verarbeitet werden, die aber bei einer Videoübertragung des Gottesdienstes nicht einschlägig sind.

Es wird deshalb generell empfohlen, keine einzelnen „einfachen“ Teilnehmer des Gottesdienstes in der Übertragung herauszustellen und bei der Übertragung des Heiligen Abendmahls die Kamera abzuschalten oder beispielsweise auf den Altar oder die Orgel auszurichten. Zu empfehlen ist ferner, auch bei dem Hinweis auf die Übertragung des Gottesdienstes entsprechend deutlich zu machen, dass die Teilnahme am Abendmahl nicht dargestellt wird.

- **Fotoaufnahmen**

Das **Recht am eigenen Bild** ist in Deutschland grundsätzlich geregelt durch das Kunsturheberrechtsgesetz (KUG). Dieses Gesetz, das schon 1907 erlassen wurde und seitdem weitgehend ausgehöhlt wurde (es gelten nur noch einzelne Paragraphen) ist auch weiterhin anzuwenden. Das bedeutet, dass auch weiterhin Fotos gemacht und unter bestimmten Voraussetzungen auch veröffentlicht werden dürfen, die natürliche Personen identifizierbar darstellen.

Zur Veröffentlichung von Bildern, zum Beispiel in Gemeindebriefen, auf denen natürliche Personen erkennbar abgebildet sind, ist stets deren **Einwilligung** erforderlich. Diese muss nicht unbedingt schriftlich gegeben werden, sondern kann auch durch sog. „schlüssiges Verhalten“, also konkludent erteilt werden. Generell wird die Einwilligung nach dem KUG angenommen, wenn der Abgebildete erkennen konnte, dass er fotografiert wird, und dem nicht widersprochen hat. Wenn gleichzeitig erkennbar war, zu welchem Zweck das Foto aufgenommen wurde, ist er auch mit der weiteren Verwendung im Rahmen dieses Zwecks im Zweifel einverstanden.

Natürliche Personen, die in **öffentlicher Funktion** auftreten, dürfen grundsätzlich abgebildet und die Bilder veröffentlicht werden. Die Grenze ist nicht immer leicht zu ziehen. Aber wenn der Pfarrer Talar trägt, tritt er auf jeden Fall in öffentlicher Funktion auf (Collarträger sind auch gut erkennbar).

Bei Personen, die als „**Beiwerk**“ abgebildet sind (der Klassiker: Foto vom Kölner Dom, das geht gar nicht ohne Personen als „Beiwerk“), dürfen Bilder veröffentlicht werden.

Bei **Gemeindeveranstaltungen** sollte bekannt sein (evtl. bekannt gegeben werden), wer Bilder für die Veröffentlichung im Gemeindebrief macht. Der- oder diejenige sollte dann bitte auch ganz offen und erkennbar fotografieren, je auffälliger, desto besser. Hilfreich kann es sein, auf einem Programmzettel entsprechende Hinweise abzudrucken.

Für die Aufnahme und Verwendung von **Fotos Minderjähriger** wird auf Ziffer 7 verwiesen.

- **Internet-Veröffentlichungen**

Internetausgaben von Veröffentlichungen jedweder Art (zum Beispiel eines Gemeindebriefs) sind grundsätzlich nicht anders zu bewerten als Print-Ausgaben. Denn die RDS-SELK differenziert bewusst nicht zwischen automatisierter und nicht-automatisierter Datenverarbeitung. Veröffentlichungen mit personenbezogenen Daten benötigen also in jeder Erscheinungsform zu ihrer Rechtmäßigkeit die strengen Voraussetzungen nach § 9 (Offenlegung an sonstige Stellen). Ohne Einwilligung der Betroffenen wird dies regelmäßig nicht der Fall sein.

- **Kinder, Schutz von**
(→ „Minderjährige, Schutz von“)

- **Kommunikantenbuch**
(→ „Abendmahl, Teilnehmerliste“)

- **Messenger-Dienste**

Messenger-Dienste wie „Telegram“ „WhatsApp“ und „Facebook“ stehen in einem negativen Ruf und unter dem Verdacht, Datenschutzrecht zu verletzen. Derartige Dienste müssen aber differenziert betrachtet werden. Die Übertragung an sich ist beispielsweise bei WhatsApp sicherer als etwa die Übertragung per E-Mail (siehe Stichwort: E-Mail), weil dort eine Ende-zu-Ende-Verschlüsselung erfolgt. Andererseits unterliegen die Betreiber (Facebook für WhatsApp und den Facebook-Messenger bzw. ein Entwicklerteam aus Dubai für Telegram“) nicht dem europäischen Datenschutzrecht und können daher das vom EuGH geforderte Datenschutzniveau nicht garantieren, das als rechtliche Voraussetzung für die Datenübermittlung an und in Drittländer vorausgesetzt wird (§ 10 RDS-SELK). Außerdem greifen die für die Nutzung eingesetzten Apps regelmäßig auf die Adressverzeichnisse in den Handys zu und stellen die dort abgelegten personenbezogenen Daten Dritten zur Verfügung. Diese Nutzung dieser Dienste sind daher datenschutzrechtlich unzulässig.

Europäische Alternativen sind beispielsweise die beiden Schweizer Instant-Messenger-Dienste „Wire“ und „Threema“ (die Schweiz gehört zwar nicht zur Europäischen Union, stellte aber ein angemessenes Datenschutzniveau im Sinne von § 10 RDS-SELK zur Verfügung).

- **Minderjährige, Schutz von**

Die RDS-SELK legt besonderen Wert auf den Schutz von Minderjährigen. Für die Verarbeitung derer Daten ist Einwilligung der Erziehungsberechtigten/Erziehungsberechtigten ist im Regelfall erforderlich. Eine Ausnahme macht § 12 RDS-SELK für besondere elektronische Angebote (etwa auch → Messenger-Dienste). Hier dürfen die Minderjährigen selbst einwilligen, sobald sie religionsmündig sind.

Auf die Veröffentlichung von Bildern, auf denen Minderjährige zu erkennen sind, sollte generell verzichtet werden, soweit nicht die **Einwilligung beider erziehungsberechtigten Eltern** vorliegt. Eine konkludente Einwilligung (→ Stichwort „Fotoaufnahmen“) kann ausreichend, ist allerdings nur unter strengen Voraussetzungen denkbar.

Dass Konfirmandinnen und Konfirmanden im Gemeindebrief abgebildet werden, ist weiterhin üblich, unterliegt aber denselben Voraussetzungen. Erforderlich ist auch hierbei allerdings die Einwilligung der Eltern/Erziehungsberechtigten. In unseren allgemein überschaubaren Strukturen sollte das möglich sein.

- **postmortale Rechte**

(→ „Verstorbene“)

- **Spendenlisten**

(→ „Beitragserhebung“)

- **Soziale Medien**

Bei der Verwendung von personenbezogenen Daten in sog. „Sozialen Medien“ wie **Facebook, Instagram, YouTube, TikTok usw.** gibt es zahlreiche datenschutzrechtliche Probleme. Im Ergebnis muss von der Nutzung dieser Medien abgeraten werden. Zwar ist es sehr bequem, solche Internet-Dienste und vor allem deren Standardtools in Anspruch zu nehmen. Keines der Unternehmen, die diese Dienste betreiben, hat seinen Sitz aber in der EU. Die Dienste unterliegt damit regelmäßig auch nicht der DSGVO, sondern unterfallen dem Datenschutzrecht anderer Länder, die häufig nicht das gleiche Datenschutzniveau gewährleisten. So hat beispielsweise der EuGH das Datenschutzniveau in den USA als nicht ausreichend erachtet, als dass eine Übermittlung von Daten auf Server in Übersee generell zulässig wäre.

Tatsächlich gibt es Alternativen zu den genannten Diensten, die ihren Sitz in Europa haben und somit europäischen Datenschutzstandards genügen. „Geraspora“ und „Diaspora“ könnten zu einer Facebook-Alternative werden.

- **Verstorbene**

Die Persönlichkeitsrechte von Verstorbenen („postmortaler Achtungsanspruch“) werden von der RDS-SELK nicht geschützt. Denn § 2 Abs. 1 ist den Anwendungsbereich von Datenschutz auf die Verarbeitung von „personenbezogenen Daten“ beschränkt, die wiederum § 4 Ziff. 1 RDS-SELK als „alle Informationen, die sich auf eine natürliche Person (...) bezie-

hen“ definiert. Hierzu zählen nach allgemeiner Auffassung (übrigens auch zur DSGVO) nur lebende Personen.

- **Video- und Fotoaufnahmen**
(→ „Gottesdienst, Video-Übertragung“; → „Fotoaufnahmen“; → „Videoüberwachung öffentlich zugänglicher Räume“)
- **Videoüberwachung öffentlicher Räume**

Die RDS-SELK regelt für den Bereich der SELK erstmals die Videoüberwachung öffentlich zugänglicher Räume (§ 52). Für die Zulässigkeit müssen bestimmte Gründe (Ausübung des Hausrechts, Schutz von Personen und Sachen) vorliegen. Hierauf müssen alle (potenziell) betroffene Personen deutlich hingewiesen werden (und zwar spätestens beim Betreten des überwachten Bereichs).

Es gibt schutzwürdige Interessen der Betroffenen, die unbedingt zu beachten sind. Besonders schutzwürdig ist das Interesse an der nicht überwachten Teilnahme am Gottesdienst.

Die Beobachtung öffentlich zugänglicher Bereiche innerhalb und außerhalb von Dienstgebäuden mit optisch-elektronischen Einrichtungen ist im Grundsatz zulässig. Dies setzt aber voraus, dass die Videoüberwachung **in Ausübung des Hausrechts der kirchlichen Stelle oder zum Schutz von Personen und Sachen** erfolgt. Andere Überwachungszwecke sind ausgeschlossen. Außerdem ist eine Einzelfall-Abwägung des Verarbeitungszwecks gegen die schutzwürdigen Interessen der Betroffenen vorzunehmen, die nicht immer zugunsten des Verarbeitungszwecks ausfallen darf.

Außerdem bestimmt § 52 Abs. 1 S. 2 RDS-SELK, dass das Interesse an der nicht überwachten Teilnahme am Gottesdienst besonders schutzwürdig ist.

(Für die **Videoübertragung von Gottesdiensten** → „Gottesdienste, Videoübertragung von“)

(„to be continued“)