

Merkblatt zum kirchlichen Datenschutz

Datenschutz ist Grundrechtsschutz

Die Datenschutzbestimmungen dienen dem Schutz personenbezogener Daten vor Missbrauch. Nach dem Urteil des Bundesverfassungsgerichts vom 15.12.1983 gehört der Schutz personenbezogener Daten zum allgemeinen Persönlichkeitsrecht jedes Menschen gemäß Art. 2 GG. Das Grundrecht auf informationelle Selbstbestimmung besagt, dass grundsätzlich jeder selbst darüber bestimmen kann, welche Daten über ihn erhoben werden können. In dieses Freiheitsrecht darf nur eingegriffen werden, wenn das gesetzlich erlaubt ist. Die europäische Datenschutzrichtlinie vom 24.10.1995 (ab 25.05.2018 die Europäische Datenschutzgrundverordnung) sichert das Grundrecht der informationellen Selbstbestimmung in allen Staaten der EU.

Kirchlicher Datenschutz

Der Umgang und Schutz von Daten der Kirchenmitglieder und der in den Einrichtungen der Kirche betreuten Personen unterliegt dem **kirchlichen Selbstbestimmungsrecht**.

Für kirchliche Einrichtungen in der Diözese Würzburg sind nicht das Bundesdatenschutzgesetz oder das bayerische Datenschutzgesetz, sondern die Ordnung über den kirchlichen Datenschutz (KDO) vom 1. Mai 2014 (WDBI 7/2014, S. 167,) und die Verordnung zur Durchführung der Ordnung über den kirchlichen Datenschutz (KDO-DVO) vom 12. Oktober 2015 (WDBI 19/2015, S.447) anwendbar. Außerdem sind unter Umständen die Datenschutzbestimmungen des Sozialgesetzbuches zu beachten. Die KDO gilt für die (Erz-)Bistümer und die Pfarreien, die Einrichtungen der Caritas sowie die sonstigen kirchlichen Einrichtungen. Für die Orden bischöflichen Rechts gilt die KDO unmittelbar. Die Orden päpstlichen Rechts wenden die KDO auf Grund der Beschlüsse der jeweiligen Ordensleitungen an.

Bei vom Staat zur Verfügung gestellten Daten, z. B. den Meldedaten, fordert der Staat, dass die Kirchen gleichwertige oder ausreichende Datenschutzmaßnahmen wie er selbst treffen. Deswegen sind die kirchlichen Datenschutzbestimmungen weitgehend inhaltsgleich mit den staatlichen Regelungen des Bundesdatenschutzgesetzes. Vorrangig sind die Regelungen von Spezialgesetzen, z. B. des Sozialgesetzbuches. Die Datenschutzbestimmungen des SGB 8 (Kinder- und Jugendhilfe) gelten ausdrücklich nur für die Träger der öffentlichen Jugendhilfe. Aber § 61 (3) SGB 8: Werden Einrichtungen und Dienste der freien Jugendhilfe in Anspruch genommen, so ist sicherzustellen, dass der Schutz der personenbezogenen Daten bei der Erhebung und Verwendung in entsprechender Weise gewährleistet ist. Dieser Gesetzesbefehl wurde umgesetzt mit der Anordnung über den Sozialdatenschutz in der freien Jugendhilfe in kirchlicher Trägerschaft (WDBI 6/2004, S. 71), die nichts anderes besagt, als dass die Sozialdatenschutzbestimmungen des SGB entsprechend gelten.

Zweck des Datenschutzes

Zweck der KDO ist es, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird. Der moderne Staat, die Kirchen und die Unternehmen benötigen aber in großem Umfang personenbezogene Daten, um ihre Aufgaben erfüllen zu können. Die Regelungen des Datenschutzes bringen das Recht von Einzelpersonen auf informationelle Selbstbestimmung mit dem Interesse kirchlicher Einrichtungen und anderer Personen an den Daten zum Ausgleich. Das Recht auf informationelle Selbstbestimmung kann nicht schrankenlos sein. Nach der Rechtsprechung des Bundesverfassungsgerichts sind Einschränkungen nur auf Grund eines Gesetzes zulässig. Das einschränkende Gesetz muss im überwiegenden Allgemeininteresse erforderlich sein, die Voraussetzungen für die Einschränkung und den Umfang des Grundrechtseingriffs für den Bürger erkennbar regeln und den Grundsatz der Verhältnismäßigkeit beachten. Es darf nur das erforderliche Minimum an Daten verarbeitet werden. Die Daten dürfen grundsätzlich nur

für den Zweck verwendet werden, für den sie erhoben oder erfasst wurden. Durch ergänzende Vorkehrungen muss dafür gesorgt werden, dass auch bei der Organisation und beim Verfahren des Umgangs mit personenbezogenen Daten auf die Rechte des Einzelnen Rücksicht genommen wird, z. B. durch Mitwirkungs- und Kontrollrechte.

Grundsätze des Datenschutzes

Datenvermeidung und Datensparsamkeit (§ 2a KDO): Gestaltung und Auswahl von Datenverarbeitungssystemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere ist von den Möglichkeiten der Anonymisierung und Pseudonymisierung Gebrauch zu machen, soweit dies möglich ist und der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

Verbot mit Erlaubnisvorbehalt: Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten ist nur zulässig, soweit eine Rechtsvorschrift es erlaubt oder anordnet oder der Betroffene eingewilligt hat.

Besonders geschützte personenbezogene Daten: Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben sind besondere Arten personenbezogener Daten. Dazu gehört nicht die Zugehörigkeit zu einer Kirche oder sonstigen Religionsgemeinschaft. Die Einwilligung des Betroffenen in die Verarbeitung dieser Daten ist nur wirksam, wenn sich die Einwilligung ausdrücklich auf diese Daten bezieht. Das Erheben besonderer Arten personenbezogener Daten ist nur bei Vorliegen enger Voraussetzungen gemäß § 9 (5) KDO zulässig, z. B. bei einem überwiegendem wichtigem öffentlichen Interesse oder soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses erforderlich ist oder soweit dies zum Zwecke der Gesundheitsvorsorge geschieht.

Datengeheimnis: Den bei der Datenverarbeitung tätigen Personen ist untersagt, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Diese Personen sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis schriftlich zu verpflichten. Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.

Einwilligungsgrundsatz: Alle Rechtsnormen über den Datenschutz sehen vor, dass auch bei Fehlen einer gesetzlichen Grundlage die Datenverarbeitung jedenfalls zulässig ist, wenn der Betroffene einwilligt. Wird die Einwilligung bei dem Betroffenen eingeholt, ist er auf den Zweck der Erhebung, Verarbeitung oder Nutzung sowie, soweit nach den Umständen des Einzelfalls erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Sie bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist die datenschutzrechtliche Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung hervorzuheben.

Unabdingbare Rechte des Betroffenen: Die Rechte des Betroffenen auf Auskunft und auf Berichtigung, Löschung oder Sperrung können nicht durch Rechtsgeschäft ausgeschlossen werden.

Videoüberwachung ist nur zulässig, soweit sie zur Aufgabenerfüllung oder zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist, und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Die Überwachung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen. Die Daten sind unverzüglich zu löschen, wenn sie nicht mehr benötigt werden oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

Datensicherheit: Daten sind so zu erfassen und aufzubewahren, dass sie nicht verlorengehen und bei Bedarf wieder zur Verfügung stehen. Sie wird erreicht durch Zugangskontrolle, sichere Speicherung, regelmäßige Datensicherung auf Reservespeicher, Planung und Durchführung eines Backup-Konzeptes.

Schutz gegen unbefugte Kenntnisnahme: Nur die Berechtigten dürfen die Möglichkeit zur Kenntnisnahme der Daten haben. Dies wird erreicht durch Zugangskontrolle, Sicherung durch Passwörter und gegebenenfalls durch Verschlüsselung gespeicherter oder zu übermittelnder Daten.

Auskunftspflicht: Der Betroffene hat grundsätzlich ein Auskunftsrecht hinsichtlich der über ihn gespeicherten Daten und wohin die Daten übermittelt werden.

Im Rahmen von **Beschäftigungsverhältnissen** ist § 10a KDO zu beachten, der zum Zwecke der Aufnahme und Durchführung des Beschäftigungsverhältnisses und zur Aufdeckung von Straftaten den Datenschutz der Beschäftigten einschränkt und auf die Beteiligungsrechte der Mitarbeitervertretung hinweist.

Datenerhebung (§ 9 KDO)

- (1) Das Erheben personenbezogener Daten ist zulässig, wenn ihre Kenntnis zur Erfüllung der Aufgaben der verantwortlichen Stellen erforderlich ist.
- (2) Personenbezogene Daten sind beim Betroffenen zu erheben. Ohne seine Mitwirkung dürfen sie nur erhoben werden, wenn eine Rechtsvorschrift das zulässt, wenn die zu erfüllende Aufgabe ihrer Art nach eine Erhebung bei anderen Personen oder Stellen erforderlich macht oder die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde. Ist die Datenerhebung nicht auf Grund einer Rechtsvorschrift zulässig, ist sie jedenfalls dann ohne Mitwirkung des Betroffenen unzulässig, wenn Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden.

Datenspeicherung, -veränderung und -nutzung (Zweckbindungsgrundsatz) (§ 10 KDO)

- (1) Das Speichern, Verändern oder Nutzen personenbezogener Daten ist zulässig, wenn es zur Erfüllung der in der Zuständigkeit der verantwortlichen Stelle liegenden Aufgaben erforderlich ist und es für die Zwecke erfolgt, für die die Daten erhoben worden sind.
- (2) Das Speichern, Verändern oder Nutzen für andere Zwecke ist nur zulässig, wenn
 1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt und kirchliche Interessen nicht entgegenstehen,
 2. der Betroffene eingewilligt hat,
 3. offensichtlich ist, dass es im Interesse des Betroffenen liegt, und kein Grund zu der Annahme besteht, dass er in Kenntnis des anderen Zwecks seine Einwilligung verweigern würde,
 4. Angaben des Betroffenen überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen,
 5. die Daten allgemein zugänglich sind,
 6. es zur Abwehr einer Gefahr für die öffentliche Sicherheit oder erheblicher Nachteile für das Gemeinwohl oder zur Wahrung erheblicher Belange des Gemeinwohls erforderlich ist,
 7. Straftaten und Ordnungswidrigkeiten vorliegen,
 8. es zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist,
 9. der Auftrag der Kirche oder die Glaubwürdigkeit ihres Dienstes dies erfordert.

Datenübermittlung an kirchliche und öffentliche Stellen (§ 11 KDO)

- (1) Die Übermittlung personenbezogener Daten an kirchliche und öffentliche Stellen ist zulässig, wenn
1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder der empfangenden kirchlichen Stelle liegenden Aufgaben erforderlich ist und
 2. eine Nutzung für einen anderen Zweck als den der Datenerhebung möglich wäre.
- (2) Die Verantwortung für die Zulässigkeit der Datenübermittlung trägt grundsätzlich die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen der empfangenden Stelle, trägt diese die Verantwortung.

Datenübermittlung an nicht kirchliche und nicht öffentliche Stellen (§ 12 KDO)

Die Datenübermittlung an nicht kirchliche und nicht öffentliche Stellen ist zulässig, wenn

- sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und eine Nutzung für einen anderen Zweck als den der Datenerhebung möglich wäre, oder
- der Dritte ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und der Betroffene kein schutzwürdiges Interesse an dem Ausschluss der Datenübermittlung hat.

Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle.

Löschung von Daten

Die Löschung von Daten ist sofort notwendig, wenn sich herausstellt, dass die Speicherung der Daten unzulässig war. Die Daten müssen auch dann gelöscht werden, wenn die speichernde Stelle sie zur Erfüllung ihrer Aufgaben nicht mehr benötigt. Ist der Inhalt von Dateien unrichtig, so wird er berichtigt. Kann die Richtigkeit der gespeicherten Daten nicht mehr geklärt werden, sind die Daten zu sperren.

Datenschutzbeauftragte

Der Diözesandatenschutzbeauftragte gemäß § 16 KDO ist Herr Joachimski für alle bayerischen Diözesen. Er wird von den Bischöfen ernannt, ist unabhängig, wacht über die Einhaltung der Bestimmungen des Datenschutzes, berät die kirchlichen Stellen und beanstandet gegebenenfalls Verstöße gegen den Datenschutz. Alle kirchlichen Dienststellen müssen ihn unterstützen. Jedermann kann sich an ihn wenden, wenn er meint in seinem informationellen Selbstbestimmungsrecht verletzt worden zu sein.

Jupp Joachimski, Datenschutzbeauftragter der bayerischen (Erz-)Diözesen, Rochusstraße 5
80333 München, Tel.: 0 89/21 37-17 96 (Bürozeit Di./Mi. 9:00 – 12:00), Fax: 0 89/21 37-15
85, E-Mail: jjoachimski@ordinariat-muenchen.de

Betrieblicher Datenschutzbeauftragter der Diözese Würzburg und der dazu gehörenden Kirchenstiftungen ist Justitiar Roland Huth, Bischöfliches Ordinariat Würzburg, Domerschulstr. 2, 97070 Würzburg, Tel: 0931/386- 73 050, Fax: 0931/386- 73 099, E-Mail: roland.huth@bistum-wuerzburg.de

Dr. Johannes Siedler
Betrieblicher Datenschutzbeauftragter der Erzdiözese Bamberg

Roland Huth
Betrieblicher Datenschutzbeauftragter der Diözese Würzburg