Merkblatt zum Datenschutz

in der

**Evangelischen Erwachsenenbildung in Bayern**

Stand: Januar 2018

**Vorbemerkung:**

Dieses Merkblatt wird mindestens einmal jährlich daraufhin gesichtet, ob es weiterhin die gängigsten Fragen zum Datenschutz in der evangelischen Erwachsenenbildung erfasst und ob es weiterhin die jeweils aktuelle Rechtslage wiedergibt. Zu diesem Zweck konsultiert die AEEB den zuständigen Regionalverantwortlichen für die Region Süd beim Datenschutzbeauftragten der EKD.

1. **Welche Datenschutzbestimmungen müssen die Mitgliedseinrichtungen der AEEB beachten?**

Die Mitgliedseinrichtungen der AEEB müssen das Datenschutzgesetz der Evangelischen Kirche in Deutschland (DSG-EKD) beachten (also nicht etwa das Bundesdatenschutzgesetz oder ein Landesdatenschutzgesetz). Alle Datenschutzgesetze sind als sog. „Auffanggesetze“ konzipiert, d.h. wenn eine bestimmte Verwendung von personenbezogenen oder personenbeziehbaren Daten in anderen kirchlichen oder teilweise auch staatlichen Gesetzen geregelt ist, gehen diese dem DSG-EKD vor. Beispielsweise sind auch bei kirchlichen Kindertagesstätten die Bestimmungen des Sozialgesetzbuches zu beachten.

Was das für eine bestimmte Datenverwendung innerhalb der AEEB konkret bedeutet, ist von der verantwortlichen Person in der jeweiligen Einrichtung zu klären. Dieses Merkblatt gibt dazu eine Hilfestellung.

1. **Worum geht es beim Datenschutz?**

Der Datenschutz schützt Persönlichkeitsrechte, d.h. die unantastbare Würde des Menschen und sein Recht auf freie Entfaltung. Daraus hat das Bundesverfassungsgericht das (Grund)Recht auf „Informationelle Selbstbestimmung“ abgeleitet: Bürgerinnen und Bürger und auch die Mitglieder der Evangelischen Kirche in Deutschland bestimmen selbst über die Verwendung ihrer Daten. Diese Selbstbestimmung tritt nur gegenüber parlamentarisch (bei kirchlichen Angelegenheiten synodal) - d. h. im Interesse der Allgemeinheit - beschlossenen Gesetzen zurück.

1. **Welche Sanktionen sind bei Nichteinhaltung der Vorschriften vorgesehen?**

Das DSG-EKD kennt z.Z. weder Straf- noch Bußgeldvorschriften. Im Mai 2018 tritt jedoch die EU-Datenschutzgrundverordnung (EU-DSGVO) in Kraft. Die Kirchen können „ihren“ Datenschutz nur behalten, wenn sie ihre Datenschutzbestimmungen an die EU-DSGVO angleichen. Gegen kirchliche Stellen, die als Unternehmen am Wettbewerb teilnehmen, also in Konkurrenz zu anderen Dienstleistungen oder Waren anbieten, kann die Aufsichtsbehörde Geldbußen verhängen.

Hält sich bis dahin eine dem DSG-EKD unterliegende Stelle nicht an die Datenschutzbestimmungen, kann dies der/die Datenschutzbeauftragte der Evangelischen Kirche in Deutschland beanstanden. Dieser Beanstandung muss unverzüglich abgeholfen werden. Geschieht dies nicht, wird es Aufgabe der Kirchenleitung, die Datenschutzkonformität herzustellen.

Viele kirchliche Stellen sind auf Datenübermittlungen vom Staat angewiesen. Der Staat darf nach seinen Datenschutzbestimmungen nur dann Daten in den kirchlichen Bereich übermitteln, wenn dort ein hinreichendes Datenschutzniveau gegeben ist.

Gegenüber kirchlichen Stellen ausgesprochene Beanstandungen wecken hieran regelmäßig Zweifel und gefährden die Übermittlung staatlicher Daten in den kirchlichen Bereich. Dies gilt erst recht, wenn Geldbußen verhängt werden.

1. **Welche Organisationen müssen eine/n Datenschutzbeauftragte/n bestellen?**

Alle Datenschutzgesetze adressieren (kirchliche oder staatliche)„Stellen“. Stellen müssen ihren Umgang mit personenbezogenen Daten entsprechend der Datenschutzgesetze organisieren. Verantwortlich dafür ist die Stellenleitung.

Kirchliche Stellen sind, ohne Rücksicht auf die Rechtsform, alle kirchlichen und diakonischen Werke und Einrichtungen, die der Evangelischen Kirche in Deutschland, den Gliedkirchen oder den gliedkirchlichen Zusammenschlüssen zugeordnet sind. Ebenso fallen rechtsfähige evangelische Stiftungen bürgerlichen Rechts darunter.

Bei kirchlichen Stellen, bei denen mehr als neun Personen nicht nur ausnahmsweise mit der Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu tun haben, müssen betriebliche oder örtliche Datenschutzbeauftragte bestellt werden. Datenschutzbeauftragte können von mehreren Stellen gemeinsam bestellt werden (örtliche Datenschutzbeauftragte).

Denkbar wäre beispielsweise, dass es auf Dekanatsebene oder auf Kirchenkreisebene eine/n örtlich Beauftragte/n für den Datenschutz gibt, der/die dann auch für die Einrichtungen der evangelischen Erwachsenenbildung im Dekanat oder Kirchenkreis zuständig ist. Denkbar wäre auch, dass mehrere Einrichtungen der Erwachsenenbildung eine/n Beauftragte/n bestellen. Diese Sachverhalte müssen noch geklärt werden (Stand Januar 2018).

Es können auch externe Datenschutzbeauftragte bestellt werden, die diese Aufgabe ehrenamtlich oder gegen Entgelt ausüben. Hier sollte darauf geachtet werden, dass diese tatsächlich eine Expertise im „Datenschutz“ haben und nicht unter dem Begriff „Datenschutz“ IT-Sicherheit oder Produkte zur IT-Sicherheit „verkaufen“.

1. **Bei wem liegt die Verantwortung, wenn kein/e Datenschutzbeauftragte/r bestellt wurde?**

Die Verantwortung liegt immer bei der Stellenleitung, auch wenn betriebliche oder örtliche Datenschutzbeauftragte bestellt sind, da letztere keine Anordnungsbefugnis haben. Die Verantwortung der betrieblichen oder örtlichen Datenschutzbeauftragten liegt darin, die Stellenleitung fachkundig zu beraten, Mitarbeitende zu schulen und eingesetzte Verfahren auf Rechtskonformität zu überwachen.

Besteht keine Pflicht, betriebliche oder örtliche Datenschutzbeauftragte zu bestellen, muss die Stellenleitung die erforderlichen Fachkenntnisse erwerben und die Einhaltung der Datenschutzbestimmungen besorgen.

Stellenleitungen können aber immer betriebliche oder örtliche Datenschutzbeauftragte bestellen; die Zahl neun ist so zu verstehen, dass es ab dann als begründungswürdig angesehen wird, wenn diese Aufgabe nicht delegiert wird; ab dann muss bestellt werden. Dies deshalb, weil die Tätigkeit als betrieblicher oder örtlicher Datenschutzbeauftragter Fachkunde erfordert. Nach dem Bundesdatenschutzgesetz ist es sogar ein Bußgeldtatbestand, wenn diese Fachkunde nicht vorhanden ist.

Eben wegen der erforderlichen Fachkunde ist es sehr häufig sehr sinnvoll ist, dass sich mehrere Stellen zusammentun und gemeinsam eine/n Datenschutzbeauftragte/n bestellen.

1. **Welche Aufgaben hat der/die Datenschutzbeauftragte?**

Betriebliche oder örtliche Datenschutzbeauftragte beraten a) fachkundig die Stellen-Leitung hinsichtlich der Verwendung personenbezogener Daten der Stelle, b) schulen die Beschäftigten und c) überwachen die eingesetzten „Verfahren“ auf Datenschutzkonformität.

Um diesem Aufgabenspektrum gerecht zu werden, sind Datenschutzbeauftragte zum Erwerb der Fachkunde und zur regelmäßigen Weiterbildung verpflichtet. Betriebliche oder örtliche Datenschutzbeauftragte sind darüber hinaus in ihrer Aufgabenerfüllung weisungsfrei.

Der Begriff „Verfahren“ hat sich etabliert, um klarzustellen, dass nicht nur bei Programmen, sondern beispielsweise auch bei Excel-Tabellen oder Ordnern mit Word-Dokumenten die Datenschutzbestimmungen beachtet werden müssen, wenn damit eine Speicherung personenbezogener Daten verbunden ist.

Betriebliche Datenschutzbeauftragte prüfen beispielsweise, ob bei Honorarverträgen und dem damit verbundenen Umgang mit personenbezogenen Daten die Datenschutzbestimmungen eingehalten werden. Sie können bei Reinigungsfirmen prüfen, ob die Firma die Reinigungskräfte auf die Wahrung des Datengeheimnisses (hier nach § 5 Bundesdatenschutzgesetz) verpflichtet hat. Sie können aber auch von den Stellen, für die sie zuständig sind, verlangen, dass dann, wenn Reinigungskräfte unbeaufsichtigt reinigen, Unterlagen mit personenbezogenen Daten weggeschlossen werden.

1. **Wo können betriebliche oder örtliche Datenschutzbeauftragte die zur Erfüllung der Aufgaben notwendigen Kenntnisse erwerben?**

Der/die Datenschutzbeauftragte der EKD bzw. die Regionalverantwortlichen bieten dreitägige Grund- und Aufbauseminare an (siehe <https://datenschutz.ekd.de/veranstaltungen/> ). In den Regionen gibt es einmal jährlich einen Datenschutz-Infotag und zweimal jährlich Erfahrungsaustauschkreise (eintägig). Darüber hinaus werden bei Bedarf vom Regionalverantwortlichen und/oder seinem IT-Sachbearbeiter Vorträge oder ganztägige Inhouse-Schulungen angeboten.

1. **Welche Daten müssen geschützt werden?**

Die Datenschutzgesetze regeln den Umgang mit personenbezogenen oder personenbeziehbaren Daten. Der Begriff des personenbezogenen oder personenbeziehbaren Datums ist von den Gesetzgebern bewusst sehr umfassend angelegt: Alle(!) persönlichen und sachlichen Verhältnisse einer bestimmten oder bestimmbaren Person fallen darunter.

Das heißt nicht, dass alles verboten ist, aber ob zulässig oder nicht entscheidet sich nicht am Begriff des personenbezogenen Datums (es gibt keine belanglosen Daten), sondern daran, ob es eine gesetzliche Erlaubnisnorm gibt oder ob eine Einwilligung vorliegt.

1. **Was ist im Umgang mit Adressen von Teilnehmenden an Veranstaltungen zu beachten?**

Ein Gesetz, das die Erhebung von Teilnehmerdaten erlaubt, wird es i.d.R. nicht geben. Der einfachste Fall wäre dann, dass Teilnehmende einfach zur Veranstaltung hingehen können und dabei keine personenbezogenen Daten erhoben werden. Die Anzahl der Teilnehmende wäre kein personenbezogenes Datum.

Wenn die veranstaltende Stelle Teilnehmerdaten überhaupt erhebt, muss sie den „Erforderlichkeitsgrundsatz“ beachten: Sie darf nur solche Daten erheben, ohne die die Veranstaltung nicht oder nur mit unverhältnismäßigem zusätzlichen Aufwand durchgeführt werden könnte. Welche Daten dies sind ergibt sich aus der Art der Veranstaltung. Daraus ergibt sich auch der Zweck, zu dem die Daten der Teilnehmenden erhoben, verarbeitet und genutzt werden. An diesen Zweck bleiben die Daten gebunden, d.h. sie dürfen nur sehr eingeschränkt (siehe § 5 DSG-EKD) für andere Zwecke verwendet werden.

Beispiele:

1. Es wird eine schriftliche Anmeldung zu dem Zweck verlangt, einigermaßen zuverlässig abschätzen zu können, wie viele Teilnehmer/innen kommen werden. Dieser Bedarf muss aber tatsächlich vorhanden sein, beispielsweise, wenn frühere Veranstaltungen gezeigt haben, dass der Raum zu klein war. Diese Daten müssen nach der Veranstaltung wieder gelöscht werden, der Zweck ist ja erfüllt. Welche Daten zu diesem Zweck erhoben werden, ergibt sich aus Erfahrungswerten. Im Anmeldeformular muss der Zweck erläutert werden, z.B.: „Ihre Anmeldedaten (Name, Vorname, …) werden zu dem Zweck erhoben, einigermaßen zuverlässig die Zahl der Teilnehmenden abschätzen zu können. Ihre Daten werden nach der Durchführung der Veranstaltung unverzüglich gelöscht.“
2. Kostenerstattungen oder Zuschüsse erhält die veranstaltende Stelle nur, wenn sie Teilnehmerlisten zu Veranstaltungen führt. Dann ist dies der Zweck, und an diesen Zweck bleiben die Angaben gebunden. Welche Daten dazu erhoben werden, gibt der Zuschussgeber vor, der die Kosten teilweise oder ganz ersetzt. Die entsprechenden Daten müssen von der veranstaltenden Stelle (z. B. Bildungswerk) sicher verwahrt werden und dürfen ausschließlich dazu benutzt werden, im Falle einer Kontrolle durch den Kostenträger dort gemachte Angaben belegen zu können. Die Dauer der Aufbewahrung hängt dann davon ab, bis wann mit einer solchen Kontrolle zu rechnen ist, wohl maximal sieben Jahre. Für andere Zwecke dürfen diese Daten nicht verwendet werden. Auch darauf muss im Anmeldeformular hingewiesen werden. Eine Einwilligung braucht es in diesem Fall nicht und man kann eine ähnliche Formulierung wie unter a) verwenden, nur als Zweck ist die Kostenerstattung und als Aufbewahrungsdauer die festgestellte Frist zu nennen.
3. Es werden die Teilnehmerdaten auch dazu erhoben, um diese künftig über weitere Veranstaltungen informieren zu können. Dann müssen sie im Anmeldeformular auf diesen zusätzlichen Zweck hingewiesen werden. Ferner muss ihnen die Möglichkeit eingeräumt werden, der Speicherung ihrer Daten zu diesem Zweck zu widersprechen.

Beispiel:

Ich bin damit einverstanden, dass meine Anschrift oder meine E-Mail-Adresse über den Zweck der Durchführung der Veranstaltung … *Name der Veranstaltung* … hinaus auch zum Zweck der Zustellung von Informationen (z.B. Programmheft) zu weiteren Veranstaltungen gespeichert und genutzt werden.

Mir ist bekannt, dass ich diese Einwilligung jederzeit widerrufen kann und dass ich das Recht auf vollständige Auskunft zu allen meinen bei … *veranstaltende Stelle* … gespeicherten Daten habe.

(Datum, Unterschrift)

1. **Dürfen Adressen von Teilnehmenden an andere Teilnehmende einer Veranstaltung ausgehändigt werden?**

Die Teilnehmenden bestimmen selbst über die Verwendung ihrer Daten. Ihre Daten dürfen nur dann an andere Teilnehmende weitergegeben werden, wenn sie eingewilligt haben. Eine solche Einwilligung kann beispielsweise bei der Anmeldung zu einer Veranstaltung abgefragt werden. In der Einwilligungserklärung muss genannt werden, welche Daten an andere Teilnehmenden zu welchem Zweck mitgeteilt werden dürfen. Zwecke wären etwa die Möglichkeit zur Bildung von Fahrgemeinschaften oder von Networking.

Eine einfache Möglichkeit, dies zu realisieren ist, bei der Veranstaltung einen Zettel herumgehen zu lassen, auf den Auskunftswillige diese Daten eintragen, die an andere Teilnehmende weitergegeben werden können.

Es ist aber beispielsweise nicht zulässig, dass Referent/innen oder Kursleiter/innen ohne Einwilligung Teilnehmerlisten kopieren und an die Teilnehmenden verteilen.

Damit Teilnehmende Fahrgemeinschaften bilden können, muss bereits bei der Anmeldung erfragt werden, ob man damit einverstanden ist, dass bestimmte Angaben, am besten eine Liste sinnvoller Angaben zum Anhaken, an andere Teilnehmende vorab zu eben diesem Zweck verschickt werden.

Entscheidend ist, dass die Teilnehmenden die volle Kontrolle darüber haben, welche Daten an andere Teilnehmer/innen weitergegeben werden.

1. **Unter welchen Voraussetzungen dürfen Personen in Verteiler (für den Programmversand und für Veranstaltungseinladungen) aufgenommen werden?**

Die Personen bestimmen selbst über die Verwendung ihrer Daten. Da keine gesetzliche Grundlage vorhanden ist, muss bei einer passenden Gelegenheit von ihnen die Einwilligung dafür eingeholt werden, ihre Kontaktdaten (Adresse, E-Mail) auch künftig für den Programmversand oder für die Einladung zu Veranstaltungen verwenden zu dürfen.

1. **Dürfen zum Nachweis der Anwesenheit Teilnehmerlisten geführt werden?**

Nur wenn dies erforderlich ist! Ein Erfordernis kann sich ergeben, wenn die Kostenträger Nachweise verlangen oder sich vorbehalten, stichprobenartige Kontrollen der Teilnehmerzahlen vorzunehmen. (Gemäß der ab 1.1.2017 geltenden Verwaltungsvorschrift sind bei Veranstaltungen mit vorheriger schriftlicher Anmeldung Teilnehmerlisten zu führen. Das Vorhandensein dieser Listen wird kontrolliert werden.)

Eine Verwaltungsvorschrift ist an sich kein Gesetz, das der „informationellen Selbstbestimmung“ vorrangig ist. Sie regelt lediglich, wie ein solches Gesetz auszuführen ist. Insofern steht hinter einer Verwaltungsvorschrift häufig eine Erlaubnisnorm. Es gehört zu den Aufgaben der betrieblichen oder örtlichen Datenschutzbeauftragten, die Sachlage zu klären.

1. **Dürfen Unterschriften von Teilnehmenden verlangt werden?**

Hier muss unbedingt der Zweck geklärt werden. Ohne dass der Zweck konkret benannt ist, lässt sich nicht entscheiden, ob es datenschutzkonform ist, von den Teilnehmenden Unterschriften zu verlangen. Ist der Zweck benannt, muss die Erforderlichkeit geprüft werden; d.h. es ist zu prüfen, ob der Zweck tatsächlich nur dadurch erreicht werden kann, dass die Teilnehmenden eine Unterschrift leisten.

Einwilligungserklärungen für bestimmte Datenverwendungen müssen unterschrieben werden, um rechtswirksam zu sein. An sich ist auch eine mündlich gegebene Zustimmung rechtswirksam, lässt sich im Streitfall aber unter Umständen nicht beweisen.

1. **Dürfen während der jeweiligen Veranstaltung Listen durchgereicht werden, um von den Teilnehmenden bestimmte Angaben zu erheben?**

Der eine Aspekt ist das Erheben von Daten, der andere die Art und Weise, wie diese Daten erhoben werden.

Erhebung:

Bei einer Erhebung von Daten muss deutlich werden, welche Stelle die Daten „haben“ möchte und zu welchem Zweck. Insbesondere muss deutlich werden, ob die veranstaltende Stelle die Daten mit Hilfe der Referentin/des Referenten bzw. Kursleiter/in erhebt oder die letztgenannten für eigene Zwecke. Die Betroffenen müssen wissen, welches die verantwortliche Stelle ist. Im Falle der Referentin/des Referenten bzw. Kursleiter/in kann es sein, dass diese die verantwortliche „Stellen“ sind (siehe Ziffer 17).

Art der Erhebung:

Das Durchreichen von Listen bedeutet, dass Teilnehmende Daten anderer Teilnehmenden einsehen können. Zumindest bei thematisch sensiblen Veranstaltungen muss davon Abstand genommen werden.

Erfahrungsgemäß haben Teilnehmende nichts gegen diese gängige Praxis einzuwenden. Beschwert sich aber ein/e Teilnehmer/in beim/bei der Datenschutzbeauftragten, muss ihm/ihr Recht gegeben werden und die betreffende „Stelle“ muss künftig von dieser Methode der Datenerhebung Abstand nehmen.

Es ist ratsam, dass betriebliche oder örtliche Datenschutzbeauftragte anhand typischer Konstellationen nach praktischen Möglichkeiten suchen, die benötigten Angaben so zu erheben, dass nicht ein/e Teilnehmer/in die Angaben eines/einer anderen einsehen kann (z.B. das Auslegen kleiner Erhebungs-Formulare, die dann in eine Box eingeworfen werden können).

1. **Welche Datenschutzbestimmungen gelten für Referent/innen und Kursleitende?**

Die nachfolgenden Ausführungen sind etwas trocken, es ist aber unverzichtbar, sich damit vertraut zu machen, soll datenschutzkonform gehandelt werden. Auch Referent/innen und Kursleitende sollten damit vertraut sein:

Eine datenverarbeitende Stelle *übermittelt* (§ 2 Abs. 4 Ziffer 3 i.V.m § 12 u. 13 DSG-EKD) Daten an Dritte, oder sie zieht im Rahmen einer sog. *Datenverarbeitung im Auftrag* (§ 11 DSG-EKD) die „Dritten“ in die eigene Stelle hinein. Dritte können Personen oder Stellen sein. Betroffene sind keine Dritten.

Das heißt, dass hinsichtlich der Referent/innen oder Kursleiter/innen als erstes festgelegt werden *muss*, ob man ihnen Daten übermittelt oder ob man mit ihnen einen Vertrag über eine Datenverarbeitung im Auftrag schließt.

Ein Beispiel für eine Datenverarbeitung im Auftrag ist die Tätigkeit eines EDV-Dienstleisters, der die Funktionsfähigkeit der eigenen Stelle sicherstellt. Dieser wird dabei unvermeidlich die Möglichkeit der Einblicknahme eigener Daten bekommen. In einem solchen Fall macht man einen Vertrag über eine Datenverarbeitung im Auftrag.

Die Tätigkeit von Referent/innen oder Kursleiter/innen wird wohl eher selten mit einer unvermeidlichen Kenntnisnahme eigener Daten einhergehen oder anderweitig mit der Tätigkeit eines EDV-Dienstleisters vergleichbar sein.

Insofern sollte zunächst von folgender Sachlage ausgegangen werden:

*Referent/innen und Kursleitende sind gegenüber der eigenen Stelle Dritte.*

*Die eigene Stelle übermittelt ihnen zum Zweck der Durchführung oder Vorträgen eigene Daten.*

*Referent/innen oder Kursleitende sind keine kirchlichen Stellen.*

Bestehen Zweifel, ob diese Sachlage zutrifft, muss sie zusammen mit der/dem zuständigen Datenschutzbeauftragten geklärt werden.

Ist die genannte Sachlage gegeben, gilt folgendes:

Für Referent/innen oder Kursleitende gilt das Bundesdatenschutzgesetz (BDSG). Sie unterliegen damit der Aufsicht des Landesdatenschutzbeauftragten, in dessen Bundesland sie tätig sind. Daraus sollten die Referent/innen und Kursleitenden an geeigneter Stelle hingewiesen werden (z.B. im Honorarvertrag). Für eine kirchliche Stelle ergibt sich die Zulässigkeit, ihnen eigene Daten zu übermitteln, aus § 12 DSG-EKD.

Die Verantwortung für die Zulässigkeit der Übermittlung trägt die kirchliche Stelle. Fühlen sich Teilnehmer/innen in ihren Persönlichkeitsrechten beeinträchtigt, werden sie sich u.U. auch an die veranstaltende Stelle (den Veranstalter) und nicht an den/die Referent/in oder Kursleiter/in wenden. Die veranstaltende Stelle muss sich dann klar und deutlich entlasten können.

Dazu dient auch die Bestimmung in § 12 DSG-EKD, wonach die Referent/innen oder Kursleitenden darauf hingewiesen werden müssen, dass die ihnen übermittelten Daten nur zu dem Zweck verwendet werden dürfen, zu dem sie übermittelt wurden. Ein solcher Hinweis muss in den Honorarverträgen enthalten sein.

Weiterhin *muss* in den Honorarverträgen geregelt werden, ob im Rahmen der Veranstaltung Teilnehmerdaten erhoben werden dürfen und wenn ja, auf der Basis welcher Erhebungsformulare oder welcher Einwilligungserklärungen und wie mit diesen Daten verfahren wird. Geregelt werden muss auch der Verbleib der Daten nach der Veranstaltung. Die eingesetzten Formulare sollten von der/vom zuständigen Datenschutzbeauftragte/n überprüft werden.

Es ist ferner ganz wichtig zu klären, inwieweit Referent/innen ihrerseits bei staatlichen oder kirchlichen Stellen beschäftigt sind und seitens dieser Stellen Ansprüche auf erhobene Daten geltend gemacht werden.

Die Übermittlung sog. besonderer Arten von Daten, d.h. Angaben über rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit (Mitarbeitervertretungszugehörigkeit), Gesundheit oder Sexualleben, ist unzulässig.

Anmerkung:

Die vorstehenden Ausführungen erscheinen umfangreich, es genügt aber, dies einmal zu klären und die entsprechenden Formulare zu entwickeln bzw. bestehende Formulare anzupassen bzw. zu ergänzen. Dann muss nur noch reagiert werden, wenn eine Veranstaltung nicht wie üblich abgewickelt werden soll.

1. **Dürfen Daten der Teilnehmenden an Referent/innen und Kursleiter/innen weitergegeben werden?**

Für eine Orientierung im Alltag helfen bei Fragen nach der Zulässigkeit der *Zweckbindungsgrundsatz* und der *Erforderlichkeitsgrundsatz*.

Jede Frage nach der Zulässigkeit einer Datenverwendung kann nur beantwortet werden, wenn der Zweck dargelegt wird. Ist dieser Punkt geklärt, wird geprüft, ob es für die Erreichung dieses Zwecks *erforderlich* ist, die in Frage stehenden Daten zu verwenden, d.h. ob ohne die Verwendung dieser Daten der Zweck nicht oder nur mit unverhältnismäßigem zusätzlichen Aufwand erreicht werden kann.

Die Grundsätze der Datensparsamkeit und Datenvermeidung (§ 2a DSG-EKD) müssen bei angemessen berücksichtigt werden.

Ein vertretbarer Zweck könnte sein, dass Referent/innen und Kursleiter/innen eine grobe Vorstellung davon bekommen, mit welchem Spektrum an Teilnehmer/innen sie zu rechnen haben. Dieser Zweck muss sich dann aber plausibel aus der Art der Veranstaltung ergeben. Dazu würde es aber reichen, Berufe oder ehrenamtliche Tätigkeiten ohne Personenbezug zu übermitteln (Datensparsamkeit und Datenvermeidung).

Aus der Art einer Veranstaltung könnte sich auch der Zweck ergeben, Namensschilder zu erstellen und den Referent/innen und Kursleiter/innen zur Verfügung zu stellen. Es könnte aber auch genügen, leere Namensschilder auszugeben, auf denen die Teilnehmer/innen ihre Namen am Anfang des Kurses schreiben.

Die veranstaltende Stelle hat hier einen Ermessensspielraum. Entscheidend ist, dass der Zweck schlüssig genannt und begründet wird und dass nur die Daten weitergegeben werden, die diesem Zweck entsprechen.

Sind Zweck und Erforderlichkeit geklärt, müssen im Honorarvertrag entsprechende Vereinbarungen getroffen werden (siehe Ziffer 15). Um die Übermittlung sicher zu machen, muss Ziffer 20 zu beachtet werden.

1. **Dürfen Referent/innen und Kursleiter/innen Teilnehmerdaten über die Veranstaltung hinaus aufbewahren?**

Im Normalfall geben Referent/innen und Kursleiter/innen die personenbezogenen Daten, die sie von der veranstaltenden Stelle zur Durchführung der Veranstaltung erhalten haben, unverzüglich wieder zurück oder löschen bzw. vernichten sie.

Das muss im Honorarvertag geregelt sein.

Die Löschung oder Vernichtung muss datenschutzkonform erfolgen (z.B. DIN 66399 bei der Vernichtung von Papierunterlagen).

Alles andere setzt die informierte Einwilligung der Teilnehmenden voraus. Das dafür verwendete Formular muss mit der/dem für die veranstaltende Stelle zuständigen Datenschutzbeauftragten abgesprochen werden. Die Verwendung genau dieses Formulars muss auch Gegenstand des Honorarvertrages sein.

1. **Was ist bei der Veröffentlichung bzw. bei der Weitergabe von Referentenlisten (in Papierform und im Internet) zu beachten?**

Eine Rechtsgrundlage dazu gibt es nicht, insofern muss von den Referent/innen die Einwilligung dafür eingeholt werden.

Es wird empfohlen, die Einverständniserklärung von Referent/innen für beide Veröffentlichungsformen einzuholen. Nur mit der Veröffentlichung in Papierform einverstanden zu sein, muss dabei ermöglicht werden.

Die Einwilligungserklärung muss darauf hinweisen, dass im Internet veröffentlichte personenbezogene Angaben kaum mehr gelöscht und in anderen ggf. unerwünschten Zusammenhängen verwendet werden können.

1. **Welche Standards sind in Bezug auf die IT-Sicherheit einzuhalten?**

Die folgenden Ausführungen gelten für jede kirchliche Stelle, auch ohne irgendeinen Bezug zur Erwachsenenbildung:

Nach dem Datenschutzgesetz muss die IT-Sicherheit gewährleistet werden. Dazu wurde von der EKD die IT-Sicherheitsverordnung erlassen. Diese verlangt, dass ein IT-Sicherheitskonzept erstellt wird. Dieses muss sich an den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) oder vergleichbaren Standards orientieren.

Auf der Homepage des/der Datenschutzbeauftragten der EKD (siehe <https://datenschutz.ekd.de/infothek-items/rat-der-ekd-erlaesst-it-sicherheitsverordnung> ) gibt es zwei Muster-IT-Sicherheitskonzepte: eines für große „Stellen“ und eines für mittlere und kleinere „Stellen“.

Ein solches Konzept muss seit Anfang 2016 in den Grundzügen, seit Ende 2017 fertig vorgelegt werden können.

Dass die Anforderungen des IT-Sicherheitskonzept für kleinere Stellen erfüllt werden, ist beim Stand der Technik das allermindeste.

Stellen, für die das kleine IT-Sicherheitskonzept nicht genügt, müssen zeitnahe die Anforderungen des IT-Sicherheitskonzeptes für größere Stellen umsetzen.

1. **Was ist hinsichtlich der IT-Sicherheit bei Datenübermittlungen zu beachten?**

Personenbezogene Daten *müssen* verschlüsselt an die Referent/innen und Kursleitenden übermittelt werden. Bei den besonderen Arten personenbezogener Daten (siehe Ziffer 15) ist die Verschlüsselung ein sehr hartes Muss. Jede andere Art der Übermittlung muss mit der/dem zuständigen Datenschutzbeauftragten abgesprochen werden. Die Weitergabe muss auf alle Fälle so erfolgen, dass Unbefugte keinen Einblick nehmen können.

EDV-technisch steht eine ganze Palette an Möglichkeiten zur Verfügung. Textverarbeitungssysteme (z.B. Microsoft Office) oder Tabellenkalkulationsprogramme (z.B. Libre Office bzw. Open Office) erlauben z.B. den Export eines Dokuments als verschlüsselte PDF-Datei.

Sog. Zip-Programme (z.B. 7-Zip) sind fast auf jedem PC installiert oder können kostenlos heruntergeladen werden. 7-Zip kann z.B. ohne Administrationsrechte betrieben werden. Damit können auch mehrere Dateien oder größere Tabellen, die sich nicht in das PDF-Format konvertieren lassen, verschlüsselte versandt werden.

Allen genannten Verfahren ist gemeinsam, dass mit dem Empfänger ein Kennwort vereinbart werden muss, z.B. telefonisch oder bei einem Treffen. Das Kennwort darf nicht auf demselben Weg übermittelt werden wie die Daten.

Dazu können auch Angaben verwendet werden, die nur der sendenden und der empfangenden Person oder Stelle bekannt sind, z.B. eine Kundennummer. Der Hinweis, was als Kennwort dient, (nicht das Kennwort selbst), darf zusammen mit den verschlüsselten Daten übermittelt werden.

Es gibt auch (komplexere) Programme, bei denen eine solche Absprache über das Kennwort nicht erforderlich ist. Solche Programme benötigen zentrale und lokale Installationen und sollten mit der/dem zuständigen Datenschutzbeauftragten abgesprochen werden.

1. **Worauf ist bei Versand von Emails zu achten?**

Was vertrauliche Inhalte von E-Mails anbelangt, siehe die Ausführungen zur IT-Sicherheit bei Datenübermittlungen (Ziffer 20).

Dazu kann es erforderlich sein, einen vertraulichen Text nicht als Inhalt einer E-Mail zu versenden, sondern ein separates verschlüsseltes Textdokument zu erstellen und dieses wie in Ziffer 20 beschrieben zu übermitteln.

Konkret bezogen auf den Versand von E-Mails muss beachtet werden, dass auch E-Mail-Adressen sehr häufig personenbezogene Daten sind, etwa, wenn sie den Vornamen und den Nachnamen enthalten.

Die Datenschutzbestimmungen gelten auch für personenbeziehbare Daten. Insofern ist eine E-Mail-Adresse auch dann als personenbezogenes Daten zu behandeln, wenn zwar der Name darin nicht vorkommt, es sich aber aus anderen Umständen heraus ergibt, wer der Empfänger dieser E-Mails ist.

Insofern gelten auch für E-Mail-Adressen die Bestimmungen der Datenschutzgesetze, d.h. man darf sie nur auf der Basis einer Rechtsgrundlage, im Rahmen eines Vertragsverhältnisses oder mit Einwilligung der Betroffenen verwenden.

Eine Rechtsgrundlage, diese Daten an andere weitergeben zu dürfen, ist nicht immer vorhanden. Bei der Verwendung von Sammlungen von E-Mail-Adressen (Verteiler) ist deshalb Vorsicht geboten, hier kann es ein Datenschutzverstoß sein, wenn nicht die Blind-Carbon-Copy-Funktion (BBC) des E-Mail-Clients verwendet wird (siehe <https://datenschutz.ekd.de/wp-content/uploads/2016/09/E-Mailverteiler_mit_-BCC.pdf>).

Mehrere Internetdienstanbieter haben sich zu der Initiative E-Mail Made in Germany (siehe <https://de.wikipedia.org/wiki/E-Mail_made_in_Germany>) zusammengeschlossen, um eine sichere Übertragung von E-Mails zu gewährleisten. Insofern sollten so weitgehend wie möglich von der Landeskirche bereitgestellte E-Mail-Adressen verwendet werden. Wenn das nicht möglich ist, sollten E-Mail-Adressen der Internetdienstanbieter der genannten Initiative verwendet werden.

Gelegentlich haben Einrichtungen, Institutionen oder Organisationen eigene Internetauftritte und mit dem entsprechenden Domain-Namen verbundene E-Mail-Adressen. Diese sollten bei ihren Internetprovidern nachfragen, ob deren Mailserver Daten verschlüsselt mit anderen Mailservern austauschen, wenn letztere das anbieten. Wenn dem so ist, ist ebenfalls das Sicherheitsniveau von E-Mail Made in Germany gegeben.

Bei einer Kommunikation mit anderen als den vorstehend genannten E-Mail-Adressen ist Vorsicht geboten, ggf. sollten Empfänger aufgefordert werden, sich eine entsprechende E-Mail-Adresse zu besorgen.

**München, den 11.01. 2018**

**Arbeitsgemeinschaft für Evang. Erwachsenenbildung in Bayern e.V. (AEEB)**

Herzog-Wilhelm-Straße 24

80331 München