

Auftragsverarbeitung nach DSGVO-EKD und KDG: Microsoft, Systemhaus und Rechenzentrum vertraglich richtig einbinden

Es gibt einen Moment in fast jedem kirchlichen Microsoft-365-Projekt, der immer gleich abläuft. Irgendwer fragt, ob denn der Auftragsverarbeitungsvertrag vorliege. Es entsteht eine Pause. Dann sagt jemand aus der IT: „Wir haben doch den Vertrag mit Microsoft.“ Und jemand aus der Verwaltung sagt: „Wir haben doch das Systemhaus.“ Und beide meinen damit nicht denselben Vertrag, sondern gar keinen.

Das ist kein Vorwurf. Auftragsverarbeitung gehört zu den Themen, die man für erledigt hält, weil irgendwo eine PDF-Datei liegt. Der Haken: In Kirche, Diakonie und Caritas gilt nicht die Datenschutz-Grundverordnung, sondern eigenes Recht — das EKD-Datenschutzgesetz auf der evangelischen und das Gesetz über den Kirchlichen Datenschutz auf der katholischen Seite. Beide regeln die Auftragsverarbeitung eigenständig. Beide sind in den vergangenen anderthalb Jahren novelliert worden. Und beide haben ihre eigene Aufsicht, die im Zweifel nicht bei der Landesdatenschutzbehörde anruft, sondern selbst vor der Tür steht.

Dieser Beitrag gehört zur Reihe [Microsoft 365 in Kirche, Diakonie und Caritas](#) und nimmt sich das Vertragsgeflecht vor, das entsteht, sobald ein Träger einen Tenant betreibt: Microsoft als Anbieter der Onlinedienste, ein Systemhaus mit Administrationsrechten, häufig ein kirchliches Rechenzentrum, dazu ein CSP-Partner für die Lizenzen und eine Handvoll Fachverfahren. Vier bis sechs Vertragsverhältnisse, von denen in der Praxis zwei sauber dokumentiert sind, wenn es gut läuft.

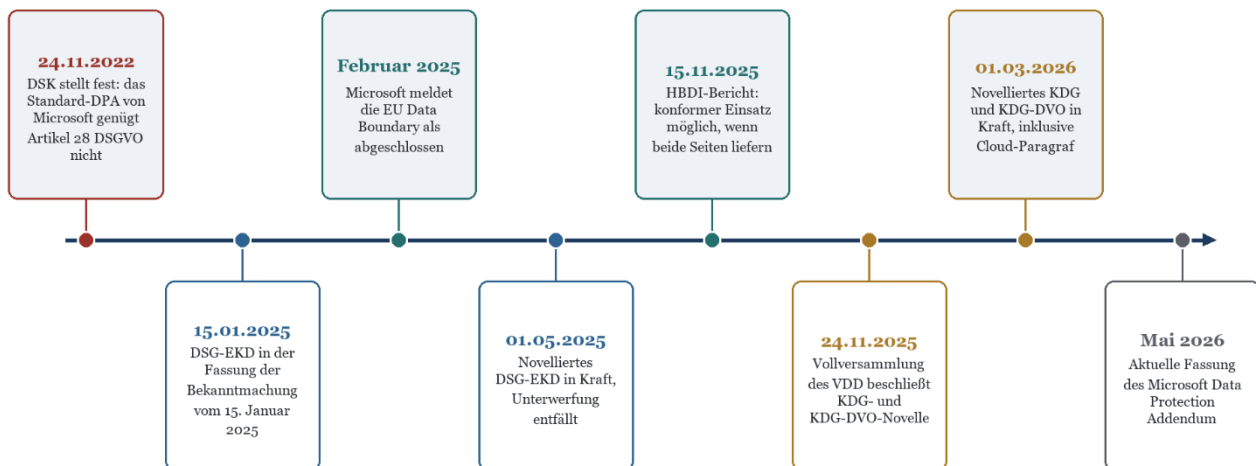
Die gute Nachricht vorweg: Vieles davon ist inzwischen einfacher geworden, weil beide Kirchen ihre Gesetze an die Realität angepasst haben. Die schlechte: Genau die Stelle, an der es in echten Projekten knallt — das Systemhaus mit Vollzugriff und ohne Vertrag — ist von keiner Novelle berührt worden. Die war schon immer heikel und ist es geblieben.

Was kirchliches Auftragsverarbeitungsrecht anders macht — und was nicht

Fangen wir mit der Entwarnung an: Die Auftragsverarbeitung nach kirchlichem Recht ist kein exotisches Parallelsystem. Wer Artikel 28 DSGVO kennt, erkennt in beiden kirchlichen Gesetzen fast alles wieder — sorgfältige Auswahl, Weisungsbindung, Vertraulichkeit, Unterstützung bei Betroffenenrechten, Löschung oder Rückgabe am Ende, Kontrollrechte. Die Unterschiede liegen nicht im Prinzip, sondern in Details, die ausgerechnet dann wichtig werden, wenn du einen fertigen Vertragstext eines Anbieters vor dir hast und entscheiden musst, ob er reicht.

Rechtsstand 2022 bis 2026

Was sich geändert hat, seit die Aufsichts das erste Mal Nein gesagt haben



Für Paragraphen und Fristen gilt: nur benennen, was in den Gesetzestexten selbst steht.

Skizze 1: Der Rechtsstand hat sich zwischen 2022 und 2026 an mehreren Stellen bewegt — auf kirchlicher und auf Anbieterseite gleichzeitig.

DSG-EKD: Textform, ein Zehn-Punkte-Katalog und eine klare Aufsichtszuständigkeit

Das EKD-Datenschutzgesetz regelt die Verarbeitung personenbezogener Daten im Auftrag in § 30 DSGVO-EKD. Maßgeblich ist die Fassung der Bekanntmachung vom 15. Januar 2025; die Novelle ist zum 1. Mai 2025 in Kraft getreten. Drei Punkte daraus solltest du kennen, auch wenn du sonst nichts aus dem Gesetz auswendig lernst.

Erstens: Die auftraggebende kirchliche Stelle bleibt verantwortlich, die Betroffenenrechte sind ihr gegenüber geltend zu machen, und zuständig für die Aufsicht ist die Aufsichtsbehörde der beauftragenden kirchlichen Stelle. Das klingt technisch, ist aber der Kern der ganzen Konstruktion: Nicht der Dienstleister zieht die Aufsicht an sich, sondern der Träger bringt sie mit. Wenn dein Kirchenkreis einen Dienstleister beauftragt, prüft im Ernstfall die Aufsicht des Kirchenkreises, nicht die des Dienstleisters.

Zweitens: Der Auftrag ist in Textform zu erteilen, und das Gesetz listet auf, was festzulegen ist — Gegenstand und Dauer, Umfang, Art und Zweck, die Art der Daten und der Kreis der Betroffenen, die technischen und organisatorischen Maßnahmen und ihre Kontrolle, Berichtigung und Löschung, die Verpflichtung der Beschäftigten des Auftragsverarbeiters auf das Datengeheimnis, gegebenenfalls die Berechtigung und die Bedingungen von Unterauftragsverhältnissen, die Kontrollrechte der beauftragenden Stelle samt Duldungs- und Mitwirkungspflichten, mitzuteilende Verstöße, den Umfang der Weisungsbefugnis sowie Rückgabe und Löschung am Ende. Zehn Punkte. Wer prüfen will, ob ein Vertragsentwurf trägt, hat damit eine brauchbare Checkliste, die keine Auslegung braucht.

Drittens — und das ist der Punkt, der in Projekten am häufigsten vergessen wird: Die Regelungen gelten entsprechend, wenn die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch andere Stellen im Auftrag vorgenommen wird und dabei ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. Übersetzt: Fernwartung ist Auftragsverarbeitung. Auch wenn der Dienstleister „nur administriert“ und „gar keine Daten

verarbeitet“. Wer Global Administrator ist, kann auf Postfächer, SharePoint-Bibliotheken und Teams-Inhalte zugreifen. Damit ist der Zugriff nicht ausgeschlossen, und damit ist die Sache entschieden.

Ergänzend verlangt die Datenschutzverordnung der EKD in ihrem § 4, dass vor dem Abschluss von Verträgen zur Auftragsverarbeitung die oder der örtlich Beauftragte für den Datenschutz zu beteiligen ist. Vorher, nicht hinterher. Das ist keine Förmerei: Es ist die einzige Stelle im Prozess, an der jemand mit Datenschutzblick den Vertrag sieht, bevor er unterschrieben ist.

KDG: Schriftform, Genehmigung von Unterauftragnehmern und ein neuer Cloud-Paragraf

Auf katholischer Seite steht die Auftragsverarbeitung in § 29 KDG. Hier ist der Rechtsstand frischer, als viele Handreichungen vermuten lassen: Die Vollversammlung des Verbandes der Diözesen Deutschlands hat am 24. November 2025 eine Novelle des KDG und seiner Durchführungsverordnung beschlossen, die zum 1. März 2026 in Kraft getreten ist. Das Gesetz wird von den Diözesanbischöfen jeweils für ihr Bistum in Kraft gesetzt — wenn du wissen willst, was bei dir konkret gilt, führt der Weg über das Amtsblatt deines Bistums, nicht über eine allgemeine Zusammenfassung.

Inhaltlich folgt § 29 KDG eng der DSGVO-Systematik, mit drei praktisch relevanten Eigenheiten. Der Vertrag bedarf der Schriftform; für die Ersetzung der Schriftform durch die elektronische Form oder die Textform sind die jeweils geltenden staatlichen Regelungen maßgeblich. Der Auftragsverarbeiter darf keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen einsetzen, und bei einer allgemeinen Genehmigung muss er über jede beabsichtigte Änderung informieren, damit der Verantwortliche Einspruch erheben kann. Und der Vertrag muss ausdrücklich Überprüfungen einschließlich Inspektionen vorsehen, die vom Verantwortlichen oder einem von ihm beauftragten Prüfer durchgeführt werden.

Spannender ist für Cloud-Projekte allerdings die Durchführungsverordnung. Sie verlangt, dass der Verantwortliche die technischen und organisatorischen Maßnahmen eines Auftragsverarbeiters regelmäßig, mindestens jedoch alle zwei Jahre, auf ihre Wirksamkeit überprüft und dies dokumentiert — wobei bei Vorlage eines anerkannten Zertifikats auf die Prüfung verzichtet werden kann. Ein konkretes Intervall, schwarz auf weiß. Und sie enthält seit der Novelle einen eigenen Paragrafen zur Nutzung von Cloud-Diensten, der drei Dinge fordert: primär bereits geprüfte und freigegebene Dienste zu nutzen, andere Dienste anhand eines Katalogs von Risikoaspekten zu bewerten und vor der Nutzung eine Exit-Strategie zu definieren.

Faktenkasten: Der Risikokatalog des kirchlichen Cloud-Paragrafen

Die Durchführungsverordnung zum KDG nennt ausdrücklich als Aspekte, die ein erhöhtes Risiko darstellen können: ungeplante vorzeitige Vertragsbeendigung durch den Anbieter, unzureichend gesicherte administrative Zugänge, mangelnde Portabilität von Daten und IT-Systemen, generelle Abhängigkeit mangels Wechselmöglichkeit, Gefährdung der Integrität durch herstellereigenspezifische Datenformate, gemeinsame Nutzung der Infrastruktur durch mehrere Kunden, Unkenntnis über den Speicherort, hohe Mobilität der Informationen sowie unbefugter Zugriff durch das Administrationspersonal des Anbieters oder Dritte.

Bemerkenswert daran: Der Gesetzgeber nennt die unzureichend gesicherten administrativen Zugänge und den unbefugten Zugriff durch Administrationspersonal in einem Atemzug mit dem klassischen Drittlandthema. Genau das ist die Lücke, die in kirchlichen Tenants am häufigsten offensteht — und sie hat selten etwas mit Microsoft zu tun.

Die Unterwerfungsklausel ist Geschichte, und das ändert mehr, als es klingt

Bis 2025 gab es auf evangelischer Seite eine Hürde, an der jedes Cloud-Projekt zuverlässig hängen blieb: Ein Auftragsverarbeiter, für den kirchliches Datenschutzrecht nicht gilt, musste sich der kirchlichen Datenschutzaufsicht unterwerfen. Der Beauftragte für den Datenschutz der EKD hatte dafür eine Muster-Zusatzklärung veröffentlicht, zuletzt in einer überarbeiteten Fassung im November 2021. Inhaltlich ging es um Unterwerfung unter die kirchliche Aufsicht, Kontrollrechte und den Rechtsweg.

In der Praxis war dieses Papier ein Gesprächsbeender. Ein weltweit tätiger Cloud-Anbieter unterwirft sich nicht der Aufsicht einer Landeskirche, und zwar unabhängig davon, wie freundlich man fragt. Das Ergebnis war eine Rechtslage, die formal streng und praktisch unerfüllbar war – der schlechteste aller Zustände, weil er nicht zu besserem Datenschutz führt, sondern zu Schatten-IT und zu Verträgen, die man lieber nicht genau liest.

Mit der Novelle ist diese Anforderung ersatzlos entfallen. § 30 DSGVO-EKD bestimmt jetzt, dass sich die Vertragsinhalte an Artikel 28 DSGVO orientieren dürfen, sofern die kirchlichen Datenschutzbestimmungen auf den Auftragsverarbeiter keine Anwendung finden. Im KDG findet sich in seiner heutigen Fassung ohnehin keine entsprechende Unterwerfungspflicht. Damit ist für beide Konfessionen dasselbe erreicht: Ein Standard-Auftragsverarbeitungsvertrag nach europäischem Muster ist grundsätzlich anschlussfähig.

Wichtig: Entfallen ist die Unterwerfung, nicht die Prüfung

Dass der Vertragsinhalt sich an Artikel 28 DSGVO orientieren darf, heißt nicht, dass damit alles erledigt ist. Die Pflicht zur sorgfältigen Auswahl bleibt. Die Pflicht, sich vor Beginn der Verarbeitung und danach regelmäßig von der Wirksamkeit der Maßnahmen zu überzeugen und das Ergebnis zu dokumentieren, bleibt. Die Zuständigkeit der kirchlichen Aufsicht für den Träger bleibt ebenfalls – nach dem KDG verfügt die Datenschutzaufsicht über ihre Untersuchungs- und Abhilfebefugnisse ausdrücklich gegenüber Verantwortlichen und Auftragsverarbeitern, bis hin zum Zugang zu Räumlichkeiten und zur vorübergehenden oder endgültigen Beschränkung einer Verarbeitung.

Gestrichen wurde eine Unterschrift, die niemand leisten konnte. Nicht die Arbeit, die dahinter steht.

Thema	DSG-EKD (evangelisch)	KDG (katholisch)
Norm zur Auftragsverarbeitung	§ 30 DSGVO-EKD, Fassung der Bekanntmachung vom 15.01.2025, Novelle in Kraft seit 01.05.2025	§ 29 KDG, Novelle beschlossen am 24.11.2025, in Kraft seit 01.03.2026
Form des Vertrags	Textform	Schriftform; Ersetzung durch elektronische Form oder Textform nach staatlichen Regelungen
Nicht-kirchliche Dienstleister	Vertragsinhalte dürfen sich an Artikel 28 DSGVO orientieren	Vertrag nach kirchlichem, staatlichem oder europäischem Recht möglich
Unterwerfung unter kirchliche Aufsicht	mit der Novelle entfallen	im geltenden Gesetzestext nicht vorgesehen
Unterauftragsverarbeiter	Berechtigung und Bedingungen sind im Auftrag festzulegen	vorherige gesonderte oder allgemeine schriftliche Genehmigung, Information über jede Änderung, Einspruchsrecht
Kontrolle der Maßnahmen	vor Beginn und danach regelmäßig überzeugen, Ergebnis dokumentieren	Überprüfungen einschließlich Inspektionen vertraglich vorzusehen; Durchführungsverordnung: mindestens

		alle zwei Jahre, dokumentiert
Erleichterung bei kirchlichen Stellen	bei Beauftragung anderer kirchlicher Stellen kann auf einzelne Festlegungen verzichtet werden	keine vergleichbare pauschale Erleichterung im Gesetzestext
Beteiligung des Datenschutzes	örtlich Beauftragte vor Vertragsabschluss beteiligen (Datenschutzverordnung)	betriebliche Datenschutzbeauftragte beraten und überwachen; Einordnung in Datenschutzklassen unter Anhörung
Zertifikate als Nachweis	genehmigte Verhaltensregeln, zertifizierte und kirchlich geprüfte Informationstechnik	genehmigte Verhaltensregeln oder Zertifizierung als Faktor; bei anerkanntem Zertifikat Verzicht auf die Zwei-Jahres-Prüfung möglich

Tabelle 1: Auftragsverarbeitung im Vergleich. Die Systematik ist nahezu identisch, die Formvorschriften und die Prüfrhythmen sind es nicht.

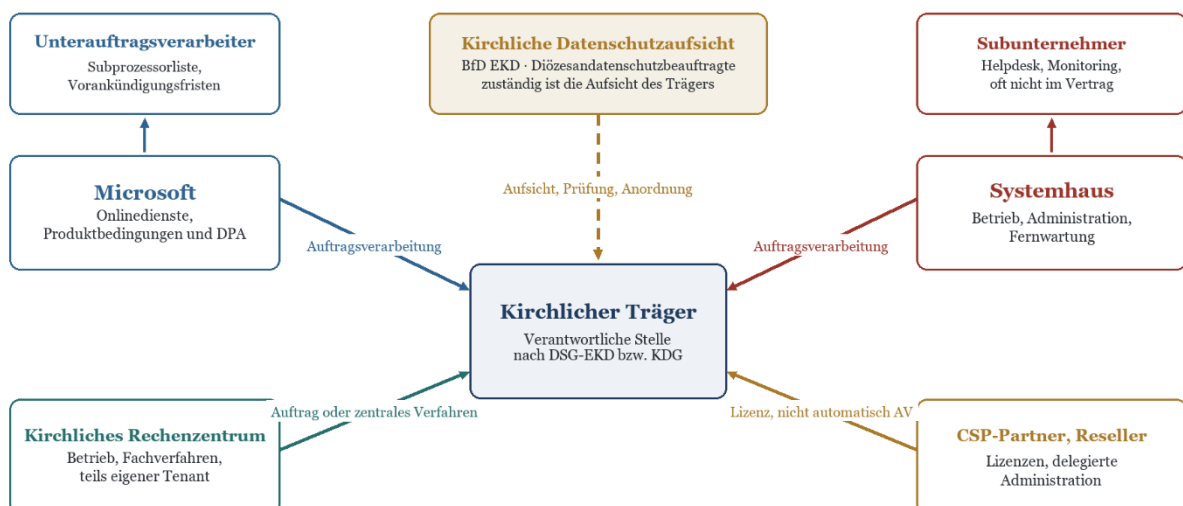
Wer sich die Grundlagen beider Gesetze im Zusammenhang ansehen will, findet sie ausführlich in [DSG-EKD verständlich: Was das evangelische Datenschutzgesetz für Microsoft 365 konkret bedeutet](#) und in [KDG verständlich: Microsoft 365 unter dem Kirchlichen Datenschutzgesetz der katholischen Kirche](#).

Das Vertragsgeflecht: Träger, Microsoft, Systemhaus, Rechenzentrum

In der Theorie ist Auftragsverarbeitung ein Zweiparteienverhältnis: Verantwortlicher hier, Auftragsverarbeiter dort, ein Vertrag dazwischen. In einem kirchlichen Microsoft-365-Projekt sitzen typischerweise vier bis sechs Parteien am Tisch, und mindestens eine davon hält sich für unbeteiligt.

Das Vertragsgeflecht

Träger, Microsoft, Systemhaus, kirchliches Rechenzentrum und die Aufsicht



Durchgezogen: Vertragsverhältnis. Gestrichelt: hoheitliche Aufsicht, kein Vertrag.

Skizze 2: Das typische Vertragsgeflecht eines kirchlichen Trägers. Der Träger steht in der Mitte, weil dort die Verantwortung bleibt — unabhängig davon, wer die Arbeit macht.

Microsoft: Was du bekommst, ohne zu verhandeln

Microsoft schließt keinen individuellen Auftragsverarbeitungsvertrag mit einer Kirchengemeinde, einem Kirchenkreis oder einem diakonischen Träger. Was du bekommst, ist das Products and Services Data Protection Addendum, kurz DPA, das über die Produktbedingungen Bestandteil deines Lizenzvertrags wird. Aktuell ist die Fassung vom Mai 2026; vorher galt die Fassung vom September 2025. Das ist ein Standarddokument für alle Kunden weltweit, und es ist kein Formular, in das du eigene Klauseln einträgst.

Das muss kein Nachteil sein. Ein Standarddokument, das von Aufsichtsbehörden über Jahre hinweg zerlegt und nachgebessert wurde, ist oft belastbarer als ein individuell ausgehandelter Text, den niemand außer den beiden Unterzeichnern je gesehen hat. Nur musst du wissen, was drinsteht — und was du deshalb selbst leisten musst.

Zu den Unterauftragsverarbeitern sagt Microsoft zu, über neue Subprozessoren, die Kundendaten verarbeiten, mindestens sechs Monate im Voraus zu informieren; die Bekanntgabe erfolgt über die veröffentlichte Subprozessorliste. Für Subprozessoren, die KI-Funktionalität unterstützen, beträgt die Vorankündigung mindestens 30 Tage, verbunden mit der Möglichkeit, deren Nutzung für mindestens sechs Monate nach der Ankündigung zu deaktivieren; für sonstige personenbezogene Daten gilt eine Frist von mindestens 30 Tagen. Das ist deutlich mehr als bei den meisten Systemhäusern — nur nutzt es nichts, wenn niemand bei dir im Haus die Liste jemals ansieht.

Beim Thema Kontrolle wird es interessant. Sowohl DSGVO-EKD als auch KDG kennen Kontrollrechte und, auf katholischer Seite, ausdrücklich Inspektionen. Microsoft weist die Einhaltung über unabhängige Prüfberichte und Zertifizierungen nach — ISO/IEC 27001, ISO/IEC 27018, ISO/IEC 27701 und SOC-Berichte, bereitgestellt über das Service Trust Portal. Eine Vor-Ort-Begehung im klassischen Sinn wirst du in einem Rechenzentrum in Irland nicht bekommen, und es wäre auch niemandem damit gedient. Beide Kirchengesetze sehen genau dafür einen Weg vor: Zertifizierungen und genehmigte Verhaltensregeln können zum Nachweis herangezogen werden, und nach der katholischen Durchführungsverordnung kann bei Vorlage eines anerkannten Zertifikats sogar auf die turnusmäßige Prüfung verzichtet werden.

Zum Datenstandort: Microsoft hat die EU Data Boundary im Februar 2025 als abgeschlossen gemeldet. Kundendaten, pseudonymisierte personenbezogene Daten und die bei Supportfällen anfallenden Professional Services Data bleiben danach für die Kerndienste in der EU und der EFTA. „Abgeschlossen“ heißt allerdings nicht „lückenlos“: Microsoft veröffentlicht selbst Listen von Diensten, die Teilmengen dauerhaft oder vorübergehend aus der Boundary heraus übertragen. Wer ehrlich dokumentieren will, nimmt diese Listen in die Bewertung auf, statt den Abschluss der Boundary als Freifahrtschein zu behandeln. Mehr dazu in [Die Cloud-Frage in der Kirche: Kirchliche Rechenzentren, Microsoft 365 und die Ehrlichkeit über Datenstandorte](#).

Das Systemhaus: der Auftragsverarbeiter, den alle vergessen

Jetzt zum unangenehmen Teil. In der überwiegenden Zahl der kirchlichen Tenants, die ich gesehen habe, existiert ein externes Konto mit der Rolle Global Administrator. Es gehört dem Systemhaus, das den Tenant eingerichtet hat. Es hat kein MFA-fähiges Verfahren, das irgendjemand beim Träger kontrolliert, es ist unbefristet, und der zugehörige Vertrag regelt Reaktionszeiten und Stundensätze, aber keine Auftragsverarbeitung.

Die Argumentation, warum das angeblich in Ordnung sei, ist immer dieselbe: Das Systemhaus verarbeite doch gar keine Daten, es administrierte nur. Diese Unterscheidung gibt es im kirchlichen Recht nicht. Das DSGVO-EKD erklärt die Regelungen zur Auftragsverarbeitung ausdrücklich für entsprechend anwendbar, wenn Prüfung oder Wartung durch andere Stellen im Auftrag erfolgt und ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. Ein Global

Administrator kann sich in Exchange Online, SharePoint und Teams Zugriff verschaffen. Der Zugriff ist also nicht ausgeschlossen. Ende der Diskussion.

Warnung: Systemhaus mit Global Admin und ohne Auftragsverarbeitungsvertrag

Die Konstellation ist der häufigste schwere Befund in kirchlichen Tenants — und der am leichtesten feststellbare. Eine Aufsicht braucht dafür keine forensische Analyse, sondern eine Liste der Rollenzuweisungen und die Frage nach dem Vertrag.

Was daran konkret schiefgeht:

- Rechtlich: eine Auftragsverarbeitung ohne Vertrag. Nach DSGVO-EKD fehlen Textform und Festlegungen, nach KDG die Schriftform. Nach dem KDG kommt hinzu, dass ein Auftragsverarbeiter, der über Zwecke und Mittel selbst entscheidet, als Verantwortlicher gilt — mit allen Folgen.
- Aufsichtsrechtlich: Die Datenschutzaufsicht kann nach dem KDG auch gegenüber dem Auftragsverarbeiter tätig werden, bis hin zu Anweisungen, Beschränkungen und Geldbußen. Der Träger haftet in jedem Fall — die Verantwortung wandert nicht mit dem Admin-Recht mit.
- Fachlich: Ein unbefristeter, hochprivilegierter externer Zugang ist genau das Risiko, das die katholische Durchführungsverordnung mit „unzureichend gesicherte administrative Zugänge“ und „unbefugter Zugriff durch Administrationspersonal“ beschreibt.
- Praktisch: Wenn dieses Konto kompromittiert wird, ist der Vorfall eine meldepflichtige Datenschutzverletzung des Trägers, nicht des Systemhauses. Und die Meldung geht an die kirchliche Aufsicht, nicht an die Landesbehörde.

Die Reihenfolge der Reparatur lautet: erst Vertrag, dann Rollen reduzieren, dann befristen, dann protokollieren. Nicht umgekehrt — und keinesfalls erst nach dem nächsten Audit.

Technisch ist die Lage inzwischen deutlich besser, als sie es 2019 war. Für Partner gibt es die granular delegierte Administration, die das alte Modell der pauschalen Delegation ablöst. Partner erhalten damit rollenbasierten, zeitlich befristeten Zugriff statt dauerhafter Vollrechte; die Befristung ist auf einen Zeitraum zwischen einem Tag und 730 Tagen einzustellen, und eine Beziehung mit der Rolle Global Administrator kann nicht automatisch verlängert werden. Wer das zusammen mit Privileged Identity Management und einem sauberen Notfallkonzept für Notfallzugänge aufsetzt, hat den administrativen Zugriff des Dienstleisters dort, wo ihn beide Kirchengesetze haben wollen.

Die Details zum Partnerzugriff beschreibt Microsoft in der Dokumentation zu [Granular delegated admin privileges \(GDAP\)](#). Für den Zugriff von Microsoft-Support auf Inhalte gibt es zusätzlich [Customer Lockbox](#): Ein Support-Ingenieur bekommt erst Zugriff, wenn eine benannte Person beim Träger die Anfrage freigibt; ohne Freigabe verfällt sie nach zwölf Stunden, und jede Entscheidung landet im Überwachungsprotokoll. Enthalten ist die Funktion in den E5-Plänen beziehungsweise über ein entsprechendes Add-on — ein Argument, das in kirchlichen Lizenzdiskussionen selten auftaucht und häufiger auftauchen sollte.

Das kirchliche Rechenzentrum: Auftragsverarbeiter, Verantwortlicher oder beides?

Kirchliche Rechenzentren sind der Sonderfall, für den beide Gesetze eigene Wege kennen. Das DSGVO-EKD erlaubt, bei der Beauftragung anderer kirchlicher Stellen auf einzelne Festlegungen zu verzichten — etwa auf die gesonderte Verpflichtung auf das Datengeheimnis, auf die Ausgestaltung der Kontrollrechte und auf die Festlegung des Umfangs der Weisungsbefugnis. Der Gedanke dahinter ist plausibel: Zwischen zwei kirchlichen Stellen gelten ohnehin dieselben Regeln und dieselbe Aufsicht. Zusätzlich kennt das Gesetz die Möglichkeit, für zentrale Verfahren mit mehreren beteiligten verantwortlichen Stellen die Verteilung von Aufgaben, Befugnissen und

Verantwortlichkeiten abweichend zu regeln — das ist der saubere Weg für landeskirchenweite Verfahren.

Die katholische Durchführungsverordnung wiederum definiert Rechenzentren eigens und verlangt für die Verarbeitung von Meldedaten aus den kommunalen Melderegistern in kirchlichen Rechenzentren eine Orientierung an den BSI-IT-Grundschutzkatalogen oder an vergleichbaren Regelungen mit entsprechendem Schutzstandard, insbesondere ISO 27001 auf Basis IT-Grundschutz. Wenn du dich gefragt hast, warum das kirchliche Meldewesen nie im Tenant landet: Das ist einer der Gründe. Mehr dazu steht in [Meldewesen und Gemeindegliederdaten: Warum Kirchenmitgliederdaten getrennt von Microsoft 365 bleiben](#).

Die eigentliche Frage bei kirchlichen Rechenzentren ist aber eine andere, und sie wird zu selten gestellt: In welcher Rolle handelt das Rechenzentrum eigentlich? Betreibt es den Tenant im Auftrag des Trägers, dann ist es Auftragsverarbeiter, und der Träger braucht einen Vertrag — auch wenn beide Seiten kirchlich sind. Betreibt es einen gemeinsamen Tenant für viele Träger und entscheidet selbst über Konfiguration, Sicherheitsbaseline und Datenhaltung, dann ist die Konstruktion eher ein zentrales Verfahren oder eine gemeinsame Verantwortlichkeit — und dann muss aufgeschrieben sein, wer welche Pflicht erfüllt. Ist es gleichzeitig CSP-Partner und beschafft die Lizenzen, kommen noch ein Lizenzvertrag und eine delegierte Administrationsbeziehung hinzu. Drei Rollen, ein Gegenüber, und in der Vertragsakte liegt ein einziges Blatt Papier.

Welche Tenant-Konstruktion überhaupt zu welcher kirchlichen Struktur passt, behandelt [Ein Tenant oder viele? Kirchengemeinde, Kirchenkreis, Landeskirche, Bistum und die Frage der Tenant-Architektur](#). Wer die Identitäten dahinter sortieren muss, findet den Faden in [Entra ID für kirchliche Träger: Identitäten zwischen Landeskirche, Verband, Träger und Einrichtung](#).

Dienstleister	Vertragsgrundlage	Kirchliche Zusatzanforderung	Offene Frage
Microsoft (Onlinedienste)	Produktbedingungen und Data Protection Addendum; Standardvertragsklauseln für Drittlandbezüge; kein individuell verhandelter Vertrag	Dokumentierte Auswahlentscheidung, Einordnung in Datenschutzklasse bzw. Schutzniveau, Beteiligung der örtlich Beauftragten bzw. der betrieblichen Datenschutzbeauftragten, Exit-Strategie	Wie belegst du die wiederkehrende Wirksamkeitsprüfung, wenn du nicht vor Ort prüfen kannst? Welche Restübermittlungen bleiben trotz EU Data Boundary?
Systemhaus mit Administrationsrechten	Dienstleistungsvertrag plus eigener Auftragsverarbeitungsvertrag nach kirchlichem Recht; Fernwartung ausdrücklich einbeziehen	Textform nach DSGVO-EKD bzw. Schriftform nach KDG, Verpflichtung auf das Datengeheimnis, Kontroll- und Duldungspflichten, Regelung der Unterauftragsverhältnisse	Welche Rollen hat der Dienstleister wirklich? Sind sie befristet? Wer liest die Protokolle der privilegierten Zugriffe?
Kirchliches Rechenzentrum	Vertrag zwischen kirchlichen Stellen mit möglichen Erleichterungen, alternativ Regelung als zentrales Verfahren	BSI-Grundschutz oder vergleichbarer Standard bei Meldedaten; klare Zuordnung der Aufsichtszuständigkeit; Abgrenzung zur gemeinsamen Verantwortlichkeit	Auftragsverarbeiter, Verantwortlicher für ein zentrales Verfahren oder beides? Wer ist Vertragspartner von Microsoft?

CSP-Partner bzw. Reseller	Lizenzvertrag; ein Auftragsverarbeitungsvertrag nur, soweit Betriebsleistungen oder Zugriffe hinzukommen	Delegierte Administration befristen, Rolle Global Administrator vermeiden, Beziehungen regelmäßig überprüfen	Hat der Reseller tatsächlich keinen Datenzugriff — oder liegt eine Administrationsbeziehung aus der Einrichtungsphase noch aktiv im Tenant?
Fachanwendungen und Schnittstellen (Pflege, Kita, Fundraising, Meldewesen)	Jeweils eigener Auftragsverarbeitungsvertrag; bei Anbindung an den Tenant zusätzlich Regelung der Schnittstelle	Höhere Datenschutzklasse bei Klienten-, Beschäftigten- und Seelsorgedaten; Berufsgeheimnisse und Schweigepflicht bleiben unberührt	Welche Daten fließen über App-Registrierungen und Berechtigungen unbemerkt in den Tenant zurück?
Unterauftragsverarbeiter von Microsoft	Über das Data Protection Addendum mitvereinbart; Bekanntgabe über die Subprozessorliste	Aufnahme in die eigene Dokumentation; Bewertung der angekündigten Änderungen	Wer bei dir im Haus beobachtet die Liste und die Ankündigungsfristen — und was passiert, wenn du widersprechen willst?

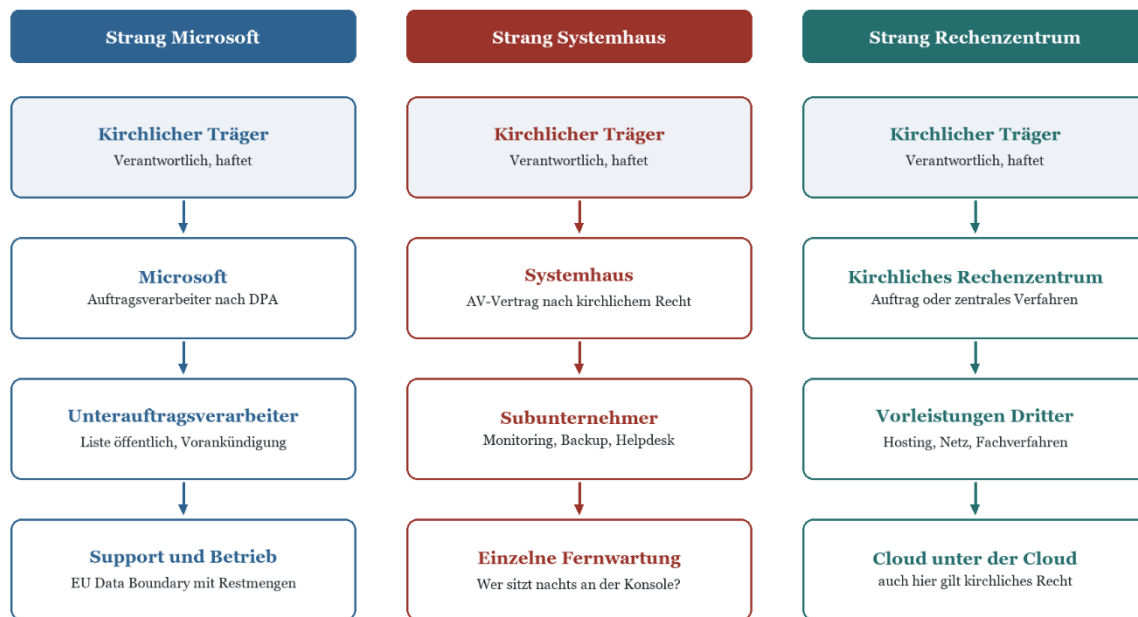
Tabelle 2: Wer ist was, worauf stützt sich das, was verlangt kirchliches Recht zusätzlich — und was bleibt offen. Die letzte Spalte ist die ehrlichste.

Unterauftragsverarbeiter: die Kette, die niemand zu Ende liest

Auftragsverarbeitung endet selten beim ersten Dienstleister. Sie setzt sich fort, und zwar in mehreren Strängen gleichzeitig. Das ist keine kirchliche Besonderheit, aber die kirchlichen Gesetze gehen damit unterschiedlich um, und das solltest du wissen, bevor du einen Vertragstext abzeichnest.

Die Kette, die niemand zu Ende liest

Drei Stränge, an deren Ende jemand sitzt, den dein Vertrag nie erwähnt hat



Die Haftung läuft die Kette nicht mit hinunter — sie bleibt oben, beim Träger.

Skizze 3: Drei Stränge, an deren Ende jeweils jemand sitzt, der auf Daten deiner Gemeindeglieder, Beschäftigten oder Klienten zugreifen kann.

Was das KDG verlangt und was das DSGVO-EKD offenlässt

Das KDG ist an dieser Stelle strenger formuliert. Ein Auftragsverarbeiter darf keinen weiteren Auftragsverarbeiter ohne vorherige gesonderte oder allgemeine schriftliche Genehmigung des Verantwortlichen einsetzen. Bei allgemeiner Genehmigung ist über jede beabsichtigte Hinzuziehung oder Ersetzung zu informieren, damit der Verantwortliche Einspruch erheben kann. Dem weiteren Auftragsverarbeiter sind dieselben Datenschutzpflichten aufzuerlegen, und kommt er ihnen nicht nach, haftet der erste Auftragsverarbeiter gegenüber dem Verantwortlichen.

Das DSGVO-EKD verlangt, gegebenenfalls die Berechtigung zur Begründung sowie die Bedingungen von Unterauftragsverhältnissen im Auftrag festzulegen. Das ist offener formuliert und räumt mehr Gestaltungsspielraum ein — aber es entbindet nicht davon, die Frage überhaupt zu regeln. Wenn im Vertrag nichts steht, ist das keine stillschweigende Erlaubnis, sondern eine Lücke.

Der Strang, der wirklich Ärger macht

In der Praxis ist nicht die Microsoft-Subprozessorliste das Problem. Die ist öffentlich, die Fristen sind lang, und man kann sie in einen Wiedervorlagetermin gießen. Das Problem ist der zweite Strang: das Systemhaus, das den Helpdesk an einen Partner ausgelagert hat, das Monitoring über einen Dienstleister fährt und die Rufbereitschaft nachts von einem dritten Unternehmen abdecken lässt. Keine dieser Konstruktionen ist per se unzulässig. Aber wenn ein diakonisches Werk in einer Großstadt in seiner Vertragsakte nur einen Rahmenvertrag über IT-Dienstleistungen hat, steht in diesem Vertrag exakt nichts über die drei Unternehmen, deren Beschäftigte nachts privilegierten Zugriff auf den Tenant haben.

Der dritte Strang ist der stillste. Ein kirchliches Rechenzentrum bezieht seinerseits Vorleistungen — Hosting, Netz, einzelne Fachverfahren, gelegentlich auch Cloud-Dienste. Dass am Ende der

Kette wieder ein großer Hyperscaler steht, ist keine Unterstellung, sondern eine Frage, die du stellen darfst und solltest. Ein katholischer Krankenhausverbund mit mehreren Standorten, der seine Verwaltung bewusst in ein kirchliches Rechenzentrum gelegt hat, will wissen, ob die Backup-Ebene dieses Rechenzentrums in einer öffentlichen Cloud liegt. Nicht, weil das schlimm wäre, sondern weil es in der Dokumentation stehen muss.

Tip: Drei Fragen, die jedes Vertragsgespräch abkürzen

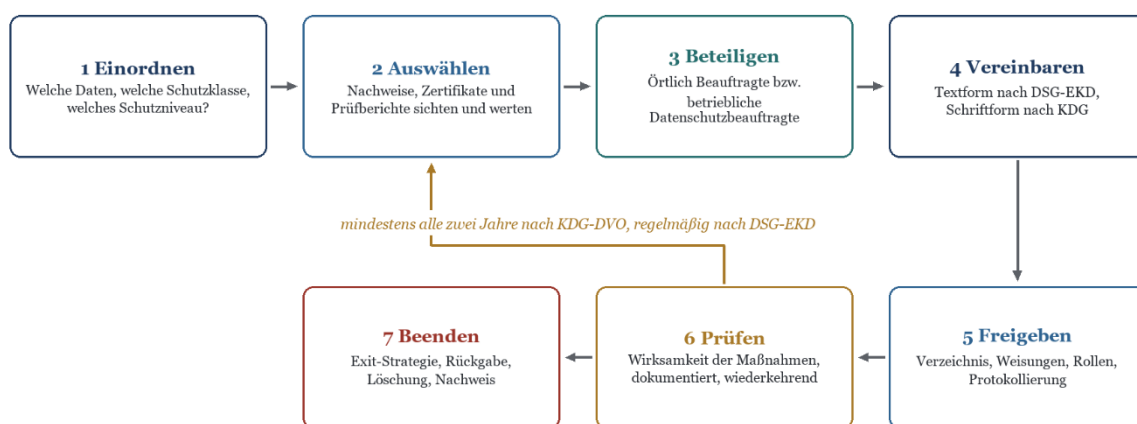
1. „Bitte nennen Sie uns alle Unternehmen, deren Beschäftigte auf unsere Systeme oder Daten zugreifen können – mit Rolle, Standort und Rechtsgrundlage.“ Ein Dienstleister, der das nicht in zwei Wochen liefern kann, hat seine eigene Lieferkette nicht im Griff.
2. „Wie und wo kündigen Sie uns Änderungen an Ihren Unterauftragnehmern an?“ Die richtige Antwort ist eine benannte Adresse und eine Frist, nicht „auf Anfrage“.
3. „Welchen Prüfbericht oder welches Zertifikat legen Sie uns vor, und wie alt ist er?“ Nach der katholischen Durchführungsverordnung ersetzt ein anerkanntes Zertifikat die turnusmäßige Prüfung; nach dem DSGVO-EKD kann zertifizierte und kirchlich geprüfte Informationstechnik zum Nachweis herangezogen werden. Beides funktioniert nur mit einem aktuellen Dokument in der Akte.

Vom Vertrag zum Nachweis: Kontrolle, Dokumentation, Aufsicht

Ein Auftragsverarbeitungsvertrag ist kein Ereignis, sondern ein Zustand. Beide Kirchengesetze verlangen nicht nur, dass du einen Vertrag schließt, sondern dass du dich vor Beginn der Verarbeitung und danach wiederkehrend davon überzeugst, dass die vereinbarten Maßnahmen tatsächlich wirken – und dass du das dokumentierst. Das ist die Pflicht, die am häufigsten verletzt wird, weil sie keinen Termin hat, an den jemand erinnert.

Der Lebenszyklus einer Auftragsverarbeitung

Von der Datenschutzklasse bis zur Exit-Strategie, und wieder von vorn



Der Kreis schließt sich bei Schritt zwei: Jede Prüfung ist auch eine neue Eignungsfrage.

Skizze 4: Der Lebenszyklus einer Auftragsverarbeitung. Die Rückkopplung von Schritt sechs zu Schritt zwei ist der Teil, den fast alle weglassen.

Die Prüfpflicht: einmal ist keinmal

Das DSGVO-EKD formuliert es so, dass die beauftragende kirchliche Stelle sich vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen hat und das Ergebnis

zu dokumentieren ist. Ein Intervall nennt das Gesetz nicht — was in der Praxis bedeutet, dass du es selbst festlegen und begründen musst. Die katholische Durchführungsverordnung ist konkreter und verlangt eine Überprüfung der Wirksamkeit regelmäßig, mindestens jedoch im Abstand von zwei Jahren, samt Dokumentation, mit der Erleichterung bei anerkannten Zertifikaten.

Für einen Microsoft-365-Tenant heißt das ganz praktisch: einmal jährlich oder alle zwei Jahre ein kurzer, geschriebener Vorgang, der die aktuellen Prüfberichte und Zertifikate des Anbieters aufnimmt, die eigene Konfiguration gegen die zugesagten Maßnahmen abgleicht und die Liste der Unterauftragsverarbeiter fortschreibt. Zwei Seiten reichen. Null Seiten reichen nicht.

Was die Aufsicht im Prüffall tatsächlich sehen will

Weder der Beauftragte für den Datenschutz der EKD noch eine Diözesandatenschutzbeauftragte wird dich bitten, das Data Protection Addendum vorzulesen. Gefragt wird nach Unterlagen, die zeigen, dass jemand nachgedacht und entschieden hat. Die folgende Tabelle ist die Kurzfassung dessen, was in einer Prüfkarte liegen sollte.

Nachweis	Was hineingehört	Wer liefert
Verzeichnis der Verarbeitungstätigkeiten	Die Verarbeitungen im Tenant, mit Empfängern, Drittlandbezug und Löschrufen; Auftragsverarbeiter führen ein eigenes Verzeichnis	Träger, unterstützt von IT und Datenschutz
Auswahl- und Eignungsdokumentation	Warum dieser Anbieter, welche Nachweise lagen vor, welche Alternativen wurden betrachtet	Projektleitung
Vertragsakte	Auftragsverarbeitungsvertrag je Dienstleister, Produktbedingungen und DPA in der geltenden Fassung, Regelung der Fernwartung	Verwaltungsleitung, Einkauf
Beteiligungsnachweis	Stellungnahme der örtlich Beauftragten bzw. der betrieblichen Datenschutzbeauftragten vor Vertragsabschluss	Datenschutz
Prüfbericht zur Wirksamkeit	Wiederkehrende Bewertung der Maßnahmen, mit Datum, Ergebnis und offenen Punkten	Datenschutz gemeinsam mit IT
Rollen- und Zugriffsübersicht	Wer hat privilegierte Rechte, befristet oder dauerhaft, intern oder extern; Notfallzugänge	IT-Leitung
Liste der Unterauftragsverarbeiter	Stand, Quelle, letzte Änderung, Bewertung angekündigter Änderungen	Datenschutz
Exit-Strategie	Rückgabe oder Löschung der Daten, Portabilität, Umgang mit anbieterspezifischen Formaten	IT-Leitung und Verwaltungsleitung

Tabelle 3: Die Prüfkarte. Acht Dokumente, von denen in der Praxis meist drei existieren — und selten die richtigen drei.

Der ehrliche Zwischenstand zur Bewertung von Microsoft 365

Zur Einordnung gehört, wie die Aufsichten selbst mit dem Thema umgehen, und da lohnt sich Genauigkeit statt Wunschdenken. Die Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder hat im November 2022 festgestellt, dass das damalige Standard-Auftragsverarbeitungspapier von Microsoft den Anforderungen von Artikel 28 DSGVO nicht genügt; sie benannte dafür mehrere Kritikpunkte. Der Beauftragte für den Datenschutz der EKD hat sich dem wenige Tage später öffentlich angeschlossen. Eine aktualisierte öffentliche Bewertung von Microsoft 365 hat der BfD EKD seither nicht veröffentlicht — der jüngste einschlägige Beitrag auf seiner Seite stammt aus dem November 2022.

Auf staatlicher Seite hat sich seither einiges bewegt. Der Hessische Beauftragte für Datenschutz und Informationsfreiheit hat nach Gesprächen mit Microsoft, die im Januar 2025 begannen, am 15. November 2025 einen Bericht vorgelegt, dem zufolge ein datenschutzkonformer Einsatz von Microsoft 365 möglich ist — unter zwei Bedingungen: Microsoft hält seine Zusagen ein, und die verantwortliche Stelle erfüllt ihre eigenen Pflichten, wozu ausdrücklich Dokumentation, Konfiguration, die Kontrolle der Dienstleister und ein sorgfältiges Löschkonzept gehören.

Faktenkasten: Was daraus für kirchliche Träger folgt — und was nicht

Staatliche Aufsichtsbewertungen binden die kirchlichen Aufsichten nicht. DSGVO-EKD und KDG sind eigenständiges Recht mit eigener Aufsicht; Beschlüsse der Datenschutzkonferenz oder Berichte einer Landesbehörde sind für BfD EKD und Diözesandatenschutzbeauftragte kein Maßstab, sondern Material.

In der Sache bewegen sie sich trotzdem in dieselbe Richtung: Die Prüfpunkte der kirchlichen Gesetze — Auswahl, Vertrag, Konfiguration, wiederkehrende Kontrolle, Löschung — sind deckungsgleich mit dem, was auch der staatliche Bericht dem Verantwortlichen abverlangt.

Die ehrliche Zusammenfassung lautet deshalb: Der Vertragsteil ist beherrschbar geworden. Was über Zulässigkeit entscheidet, ist inzwischen weniger die Frage, welches Papier Microsoft unterschreibt, sondern was du in deinem eigenen Tenant konfigurierst und dokumentierst.

Wie eine kirchliche Aufsicht im Prüffall konkret vorgeht und welche Unterlagen sie zuerst anfordert, steht in [Kirchliche Datenschutzaufsicht in der Praxis: Was BfD EKD und Diözesandatenschutzbeauftragte von einem Microsoft-365-Tenant erwarten](#). Die vorgelagerte Bewertung des Gesamtverfahrens gehört in die [Datenschutz-Folgenabschätzung für Microsoft 365 nach DSGVO-EKD und KDG](#), und wenn es doch einmal schiefgeht, hilft [Datenpannen bei kirchlichen Trägern: Meldung an BfD EKD oder Diözesandatenschutzbeauftragten, Fristen, Ablauf und Übung](#).

Die Fälle, in denen kirchliches Recht wirklich mehr verlangt

Bei aller Entspannung: Es gibt Konstellationen, in denen die Abgrenzung zur Kommune und zum Mittelstand real ist und nicht nur gefühlt. Sie hängen nicht am Vertragstext, sondern an der Art der Daten.

Klientendaten, Schweigepflicht und die Datenschutzklassen

Die katholische Durchführungsverordnung ordnet personenbezogene Daten in drei Datenschutzklassen ein und knüpft daran Schutzniveaus. In die höchste Klasse fallen insbesondere die besonderen Kategorien personenbezogener Daten sowie Daten über strafbare Handlungen, arbeitsrechtliche Rechtsverhältnisse, Disziplinarentscheidungen und Namens- und Adressangaben mit Sperrvermerken. Für Beratungsstellen, Jugendhilfe, Pflege und Personalverwaltung heißt das: Der Regelfall ist die höchste Klasse, nicht die Ausnahme. Erfolgt keine Einordnung, gilt automatisch die höchste Datenschutzklasse — eine bemerkenswert wirksame Regelung gegen das Verschieben unbequemer Entscheidungen.

Schon das unterste Schutzniveau verlangt bei der Nutzung ungesicherter Netze ausdrücklich Mehr-Faktor-Authentifizierung. Für ein Cloud-Produkt, das per Definition über das offene Internet genutzt wird, ist das keine Kür. Und die Verpflichtung der Beschäftigten des Auftragsverarbeiters auf das Datengeheimnis, die das DSGVO-EKD ausdrücklich in den Vertragskatalog aufnimmt, trifft genau die Personen, die beim Systemhaus nachts Störungen beheben.

Wie sich Klienten- und Sozialdaten im Tenant technisch schützen lassen, behandelt [Klientendaten in Diakonie und Caritas: Sozialdaten, Schweigepflicht und Schutz mit Microsoft Purview](#).

Seelsorgegeheimnis: die Grenze, die kein Vertrag verschiebt

Hier endet die Vertragsgestaltung. Beide Kirchen halten die Verpflichtung zur Wahrung des Beicht- und Seelsorgegeheimnisses sowie anderer Berufs- und Amtsgeheimnisse ausdrücklich unberührt vom Datenschutzrecht. Die katholische Durchführungsverordnung ist an dieser Stelle unmissverständlich: Daten, die dem Beichtgeheimnis unterliegen, dürfen nicht verarbeitet werden. Daten, die dem Seelsorgegeheimnis unterliegen, dürfen nur verarbeitet werden, wenn dem besonderen Schutzniveau angepasste Maßnahmen ergriffen werden, die erforderlichenfalls über das höchste Schutzniveau hinausgehen.

Kein Auftragsverarbeitungsvertrag der Welt macht ein Seelsorgeprotokoll in OneNote zulässig. Das ist kein Vertrags-, sondern ein Architekturthema — nachzulesen in [Seelsorgegeheimnis und Beichtgeheimnis in Microsoft 365: Was nie in Teams, OneNote oder Copilot landen darf](#).

Mitarbeitervertretung: der Vertrag ersetzt die Beteiligung nicht

Ein Punkt, der in Vertragsverhandlungen regelmäßig untergeht: Der Auftragsverarbeitungsvertrag ist ein datenschutzrechtliches Instrument. Er sagt nichts über die Mitbestimmung. Wenn dein Systemhaus künftig zentrale Protokolle auswertet oder ein neues Monitoring einführt, das Rückschlüsse auf das Verhalten von Beschäftigten zulässt, ist das ein Thema für die Mitarbeitervertretung nach dem Mitarbeitervertretungsgesetz der EKD beziehungsweise nach der Mitarbeitervertretungsordnung — unabhängig davon, wie gut der Vertrag mit dem Dienstleister ist. Der Dritte Weg ist an dieser Stelle nicht weniger verbindlich als das Betriebsverfassungsgesetz, nur anders organisiert.

Praktisch heißt das: Vertragsabschluss und Dienstvereinbarung gehören in dieselbe Projektplanung. Ein Träger, der im Frühjahr den Vertrag unterschreibt und im Herbst feststellt, dass die MAV der Protokollierung noch nicht zugestimmt hat, hat nicht schneller gearbeitet, sondern zweimal.

Häufige Fragen

Reicht das Data Protection Addendum von Microsoft als Auftragsverarbeitungsvertrag nach kirchlichem Recht?

Als Vertragsdokument ist es der Anknüpfungspunkt, ja. Das DSGVO-EKD lässt seit der Novelle ausdrücklich zu, dass sich die Vertragsinhalte an Artikel 28 DSGVO orientieren, wenn kirchliches Datenschutzrecht auf den Auftragsverarbeiter keine Anwendung findet; das KDG erlaubt Verträge nach kirchlichem, staatlichem oder europäischem Recht. Was das Addendum nicht ersetzt, sind deine eigenen Pflichten: die dokumentierte Auswahlentscheidung, die Beteiligung des Datenschutzes vor Vertragsabschluss, die wiederkehrende Wirksamkeitsprüfung und die Exit-Strategie.

Brauchen wir noch die Zusatzerklärung zur Unterwerfung unter die kirchliche Aufsicht?

Auf evangelischer Seite nicht mehr. Die Anforderung ist mit der Novelle des DSGVO-EKD entfallen, die zum 1. Mai 2025 in Kraft getreten ist. Im KDG ist eine entsprechende Pflicht im geltenden Text nicht vorgesehen. Wenn in einem alten Vertrag oder einer alten Handreichung bei dir im Haus noch danach gefragt wird, ist das ein Hinweis darauf, dass das Dokument aus der Zeit vor 2025 stammt und ohnehin eine Durchsicht verdient hat.

Unser Systemhaus sagt, es verarbeite keine Daten, sondern administrierte nur. Stimmt das?

Nein. Das DSGVO-EKD erklärt die Regelungen zur Auftragsverarbeitung ausdrücklich für entsprechend anwendbar, wenn Prüfung oder Wartung im Auftrag erfolgt und ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann. Bei einem Global Administrator in einem Microsoft-365-Tenant ist er nicht ausgeschlossen. Die saubere Lösung ist ein Auftragsverarbeitungsvertrag plus ein Rollenmodell, das dem Dienstleister nur gibt, was er wirklich braucht — befristet und protokolliert.

Müssen wir einen Vertrag mit dem kirchlichen Rechenzentrum schließen, obwohl beide Seiten kirchlich sind?

In aller Regel ja. Das DSGVO-EKD lässt bei der Beauftragung anderer kirchlicher Stellen lediglich zu, auf einzelne Festlegungen zu verzichten — etwa die gesonderte Verpflichtung auf das Datengeheimnis oder die ausdrückliche Ausgestaltung der Kontrollrechte. Der Auftrag selbst bleibt zu erteilen. Alternativ kann das Konstrukt als zentrales Verfahren geregelt werden, in dem die Verteilung von Aufgaben und Verantwortlichkeiten ausdrücklich festgelegt wird. Was nicht funktioniert, ist die stille Annahme, unter kirchlichen Stellen brauche es nichts.

Wie oft müssen wir den Auftragsverarbeiter prüfen?

Nach dem DSGVO-EKD vor Beginn der Verarbeitung und danach regelmäßig, mit dokumentiertem Ergebnis; ein festes Intervall nennt das Gesetz nicht, du musst es also selbst festlegen und begründen. Die Durchführungsverordnung zum KDG verlangt eine Wirksamkeitsprüfung regelmäßig, mindestens jedoch alle zwei Jahre, mit Dokumentation — bei Vorlage eines anerkannten Zertifikats kann auf die Prüfung verzichtet werden. Für gemischte Landschaften empfiehlt sich schlicht der strengere Rhythmus, dann musst du nicht zweimal nachdenken.

Was ist mit Unterauftragsverarbeitern, die wir nicht kennen?

Bei Microsoft ist die Lage vergleichsweise komfortabel: Es gibt eine veröffentlichte Subprozessorliste, und für neue Subprozessoren mit Zugriff auf Kundendaten sagt Microsoft eine Vorankündigung von mindestens sechs Monaten zu. Deine Aufgabe ist, diese Liste tatsächlich zu beobachten und die Ankündigungen zu bewerten. Bei Systemhäusern und Rechenzentren musst du aktiv fragen — das KDG verlangt hier eine Genehmigung und die Information über jede beabsichtigte Änderung, das DSGVO-EKD die Regelung von Berechtigung und Bedingungen im Auftrag.

Darf ein CSP-Partner Global Administrator in unserem Tenant sein?

Dürfen und sollen sind zwei verschiedene Dinge. Microsoft hat das alte Modell der pauschalen delegierten Administration durch die granulare, zeitlich befristete Delegation abgelöst; die Befristung liegt zwischen einem und 730 Tagen, und eine Beziehung mit der Rolle Global Administrator lässt sich nicht automatisch verlängern. Nimm das als das, was es ist: eine Empfehlung des Herstellers, die sich mit dem deckt, was die kirchlichen Regelwerke unter angemessenen technischen und organisatorischen Maßnahmen verstehen.

Gilt für uns eigentlich das Bundesdatenschutzgesetz oder die DSGVO?

Für kirchliche Stellen im Geltungsbereich der beiden Kirchengesetze gilt kirchliches Datenschutzrecht — DSGVO-EKD beziehungsweise KDG, jeweils mit ihren Durchführungsbestimmungen und mit eigener Aufsicht. Beide Gesetze nehmen ausdrücklich Bezug auf die DSGVO und stellen den Einklang mit ihr her, sind aber eigenständig. Spezielle

staatliche Vorschriften — etwa im Sozial-, Kranken- oder Arbeitsrecht — bleiben daneben anwendbar, soweit sie das kirchliche Schutzniveau nicht unterschreiten. Genau deshalb funktioniert ein Vertragsmuster aus der Kommunalverwaltung nicht ungeprüft eins zu eins.

Wir haben seit Jahren einen Tenant und keinen einzigen dieser Verträge. Wo fangen wir an?

Bei der Rollenliste, nicht beim Vertrag. Zieh dir die Übersicht aller privilegierten Rollen im Tenant und markiere jede Zuweisung, die nicht zu einer Person deiner eigenen Organisation gehört. Das ist in aller Regel eine kurze Liste und gleichzeitig die vollständige Liste der Dienstleister, mit denen du einen Vertrag brauchst. Danach kommen Verzeichnis, Beteiligungsnachweis und Prüfbericht. In dieser Reihenfolge, weil sie mit dem größten Risiko beginnt.

Fazit

Die Auftragsverarbeitung in Kirche, Diakonie und Caritas ist in den letzten anderthalb Jahren deutlich praktikabler geworden. Das novellierte DSGVO-EKD gilt seit dem 1. Mai 2025, das novellierte KDG samt Durchführungsverordnung seit dem 1. März 2026. Die Klausel, an der früher jedes Cloud-Projekt scheiterte — die Unterwerfung des Dienstleisters unter die kirchliche Aufsicht — ist auf evangelischer Seite gestrichen, und auf katholischer Seite hat es sie in dieser Form nicht gegeben. Ein Standardvertrag nach europäischem Muster ist damit anschlussfähig.

Was geblieben ist, ist die Arbeit dahinter: sorgfältig auswählen, den Datenschutz vor Vertragsabschluss beteiligen, Form wahren — Textform nach DSGVO-EKD, Schriftform nach KDG —, Unterauftragsverhältnisse regeln, wiederkehrend prüfen und das Ergebnis aufschreiben. Dazu kommt auf katholischer Seite der neue Cloud-Paragraf mit Risikoprüfung und Exit-Strategie, und auf beiden Seiten die Einsicht, dass Fernwartung Auftragsverarbeitung ist.

Der eigentliche Befund dieses Artikels ist aber ein anderer, und er ist unbequem: Das vertragliche Risiko liegt nicht bei Microsoft. Es liegt bei dem Dienstleister, der seit vier Jahren einen unbefristeten Vollzugriff auf deinen Tenant hat, weil das bei der Einrichtung mal praktisch war. Diesen Zugang zu ordnen kostet weniger als einen Projekttag, verbessert die Sicherheitslage sofort und beantwortet gleichzeitig die erste Frage, die dir eine kirchliche Aufsicht stellen wird.

Weiter im Thema

[Microsoft 365 für kirchliche Träger: DSGVO-EKD und KDG](#) › der Überblick über beide Rechtskreise

[Kirchliche Datenschutzaufsicht in der Praxis: Was BfD EKD und](#)

[Diözesandatenschutzbeauftragte von einem Microsoft-365-Tenant erwarten](#) › was im Prüffall angefordert wird

[Die Cloud-Frage in der Kirche: Kirchliche Rechenzentren, Microsoft 365 und die Ehrlichkeit über Datenstandorte](#) › Datenstandorte und die Rolle kirchlicher Rechenzentren

[Datenschutz-Folgenabschätzung für Microsoft 365 nach DSGVO-EKD und KDG: Vorgehen, Muster und typische Befunde](#) › die Bewertung des Gesamtverfahrens

[Notfall- und Red-Team-Übung für kirchliche Träger: Wenn die Diakonie-Verwaltung verschlüsselt ist und das Pflegeheim weitermachen muss](#) › wenn der privilegierte Zugang doch missbraucht wird

Wenn du dein Vertragsgeflecht einmal geordnet auf den Tisch legen willst, statt es im nächsten Prüftermin zu sortieren: Dabei hilft die [Microsoft-365-Beratung für kirchliche Träger](#).