

DSG-EKD verständlich: Was das evangelische Datenschutzgesetz für Microsoft 365 konkret bedeutet

Es gibt eine Sorte Besprechung, die in kirchlichen Verwaltungen mit bemerkenswerter Zuverlässigkeit stattfindet. Jemand aus der IT hat Microsoft 365 vorgeschlagen, jemand aus der Verwaltung findet die Idee gut, und dann sagt eine einzige Person den einen Satz, der das Projekt für sechs Monate anhält: „Das geht bei uns nicht, wir haben ja das DSG-EKD.“ Danach schweigen alle ehrfürchtig, weil niemand im Raum das Gesetz je gelesen hat, aber alle ahnen, dass es irgendwo einen Absatz gibt, der genau das verbietet, was man gerade vorhatte.

Die gute Nachricht: Diesen Absatz gibt es nicht. Die weniger gute: Es gibt eine ganze Reihe anderer, und die verlangen von dir etwas, das deutlich unbequemer ist als ein Verbot. Sie verlangen, dass du weißt, was in deinem Tenant passiert, dass du es aufgeschrieben hast, und dass du es jemandem erklären kannst, der nicht gekommen ist, um sich beeindrucken zu lassen.

Dieser Beitrag übersetzt das evangelische Datenschutzrecht in die Sprache, in der ein Microsoft-365-Projekt tatsächlich geführt wird: Postfächer, Sites, Teams, Gruppen, Rollen, Richtlinien, Protokolle. Weil kirchliche Träger selten nur einer Konfession begegnen — spätestens im gemeinsamen Sozialraum, im Krankenhausverbund oder in der Kita-Kooperation sitzt die andere Seite mit am Tisch — steht neben dem DSG-EKD durchgehend das katholische Pendant, das KDG. Wo beide gleich ticken, sagen wir es. Wo sie es nicht tun, erst recht.

Fakten: Der Stand, von dem dieser Beitrag ausgeht

Die Synode der EKD hat am 13. November 2024 eine umfassende Reform des Kirchengesetzes über den Datenschutz der Evangelischen Kirche in Deutschland beschlossen. Die Neufassung wurde am 15. Januar 2025 im Amtsblatt der EKD veröffentlicht und gilt seit dem 1. Mai 2025.

Die Reform hat das kirchliche Recht näher an das europäische herangeführt: Informationspflichten und Betroffenenrechte wurden angeglichen, die Schwelle für die Bestellung örtlich Beauftragter wurde von zehn auf zwanzig Personen angehoben, die Pflicht zur vertraglichen Unterwerfung von Auftragsverarbeitern unter die kirchliche Aufsicht ist entfallen, und die Obergrenze für Geldbußen liegt nun bei sechs Millionen Euro.

Wenn du also ein Datenschutzkonzept aus dem Jahr 2021 im Schrank hast: Es ist nicht falsch, aber es ist an mehreren Stellen überholt. Das ist der häufigste Befund in Projekten dieses Jahres.

Eigenes Recht, eigene Aufsicht: warum das DSG-EKD kein Klon ist

Kirchen in Deutschland regeln ihren Datenschutz selbst. Das ist keine Trotzhaltung und keine historische Kuriosität, sondern eine ausdrückliche Öffnungsklausel des europäischen Datenschutzrechts: Wer als Religionsgemeinschaft beim Start der europäischen Regeln bereits eigene, umfassende Datenschutzregeln hatte, darf sie behalten — sofern sie mit dem europäischen Niveau in Einklang gebracht werden und eine unabhängige Aufsicht darüber wacht. Genau das haben beide großen Kirchen getan. Die evangelische Seite mit dem DSG-EKD, die katholische mit dem KDG.

Für dich als IT-Leitung, Verwaltungsleitung oder Geschäftsführung bedeutet das drei Dinge, die im Projektalltag deutlich mehr Wirkung entfalten als der Gesetzestext selbst: Du zitierst ein anderes

Gesetz, du sprichst mit einer anderen Aufsicht, und du klagst vor einem anderen Gericht. Inhaltlich sind die Anforderungen zu einem großen Teil deckungsgleich mit dem, was jedes andere Unternehmen auch erfüllen muss. Wer dir erzählt, kirchlicher Datenschutz sei ein völlig fremdes Universum, will dir entweder etwas verkaufen oder hat Angst vor der Cloud und sucht ein Argument.

Diesen Beitrag findest du eingebettet in eine größere Übersicht: Die Serie [Microsoft 365 in Kirche, Diakonie und Caritas](#) ordnet ein, was an kirchlichen Trägern wirklich anders ist — und was schlicht normales Microsoft 365 bleibt, auch wenn ein Kreuz am Briefkopf klebt.

Wer unter das DSGVO-EKD fällt — und wer nicht

Der Anwendungsbereich ist breiter, als viele denken. Erfasst sind die EKD selbst, die Gliedkirchen — also die Landeskirchen — und ihre Zusammenschlüsse, dazu die kirchlichen und diakonischen Dienste, Werke und Einrichtungen, die diesen Stellen zugeordnet sind. Übersetzt in die Organigramme, die auf deinem Schreibtisch liegen: das Landeskirchenamt, der Kirchenkreis, das Dekanat, die Kirchengemeinde mit ihrem Pfarramt und ihrem Presbyterium, das Diakonische Werk, der diakonische Träger mit seinen Krankenhäusern, Pflegeeinrichtungen, Kitas, Jugendhilfeangeboten, Beratungsstellen und Bildungswerken.

Das Gesetz gilt für automatisierte Verarbeitung ebenso wie für die Aktenordner im Regal — und ausdrücklich unabhängig davon, wo verarbeitet wird. Ein Rechenzentrum in Amsterdam macht die Sache nicht kirchenrechtsfrei. Ein Tenant, der auf dem Papier einem Dienstleister gehört, auch nicht.

Nicht erfasst ist alles, was außerhalb dieser Zuordnung liegt. Eine gemeinnützige GmbH, die zwar christlich gegründet wurde, aber weder der verfassten Kirche noch einem diakonischen Landesverband zugeordnet ist, fällt unter das allgemeine Recht. Bei Beteiligungen, Kooperationsgesellschaften und gemeinsamen Servicegesellschaften lohnt sich diese Frage vor der Tenant-Planung und nicht danach — sonst hängen in einem Verzeichnis der Verarbeitungstätigkeiten plötzlich zwei Rechtsordnungen nebeneinander, und niemand weiß, welche Aufsicht bei einer Panne anzurufen ist.

Der BfD EKD: eine Aufsicht für Kirche und Diakonie

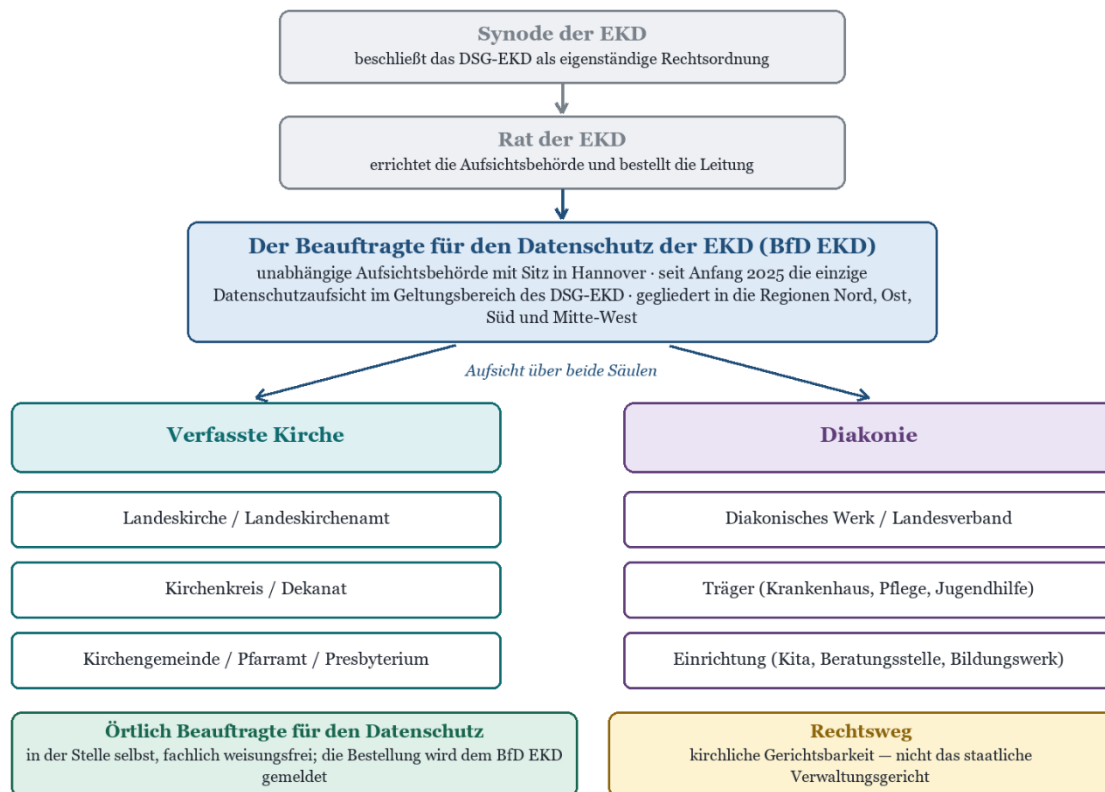
Der Rat der EKD errichtet die Aufsichtsbehörde und bestellt ihre Leitung. Der Beauftragte für den Datenschutz der EKD sitzt in Hannover, arbeitet völlig unabhängig und ist seit Anfang 2025 die einzige Datenschutzaufsicht im Geltungsbereich des DSGVO-EKD. Bis dahin gab es mehrere Stellen nebeneinander; einzelne Landeskirchen und ostdeutsche Gliedkirchen hatten eigene Aufsichten unterhalten, die inzwischen übergegangen sind. Organisiert ist die Behörde in vier Regionen: Nord, Ost, Süd und Mitte-West.

Praktisch heißt das: Wenn im diakonischen Pflegedienst ein Laptop verschwindet und im Landeskirchenamt eine Fehlkonfiguration auffällt, landen beide Vorgänge bei derselben Behörde. Das ist ein echter Vorteil gegenüber der Zersplitterung früherer Jahre — und ein Grund, warum sich landeskirchenweite Standards für Microsoft 365 lohnen. Wer in vier Kirchenkreisen vier verschiedene Antworten auf dieselbe Frage gibt, wird das genau einmal erklären müssen.

Der BfD EKD berät, bildet fort und beaufsichtigt. Er kann Anordnungen treffen, Verarbeitungen beschränken und Geldbußen verhängen — letztere allerdings nur für wirtschaftliche Tätigkeiten, was in der Diakonie mit ihren Betriebsteilen deutlich öfter zutrifft als im Pfarramt. Die Obergrenze liegt seit der Reform bei sechs Millionen Euro. Das ist eine Zahl, die man in einer

Presbyteriumssitzung besser nicht beiläufig erwähnt, wenn man den Abend noch entspannt beenden will.

Skizze 1: Wer beaufsichtigt wen — die evangelische Aufsichtsstruktur



Skizze 1: Die evangelische Aufsichtsstruktur — vom Kirchengesetz über die Aufsichtsbehörde bis zu den örtlich Beauftragten in der einzelnen Stelle.

Die örtlich Beauftragten — dein wichtigster Verbündeter

Innerhalb der Stelle sitzen die örtlich Beauftragten für den Datenschutz. Bestellt werden muss, wer in der Regel mindestens zwanzig Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten betraut hat — oder wessen Kerntätigkeit in der umfangreichen Verarbeitung besonderer Datenkategorien besteht. Der zweite Fall ist der eigentlich relevante: Ein Pflegedienst, eine Suchtberatung, eine Erziehungsberatungsstelle erfüllt ihn auch dann, wenn dort nur acht Personen arbeiten. Gesundheitsdaten und Sozialdaten sind kein Nebenschauplatz, sondern das Kerngeschäft.

Mehrere Stellen dürfen gemeinsame Beauftragte bestellen — die übliche Lösung, wenn ein Kirchenkreis fünfzig Gemeinden hat, von denen jede einzelne unter der Schwelle bleibt. Und wo gar keine Bestellungspflicht besteht, muss die Leitung die Aufgaben auf andere Weise sicherstellen. Das ist die Klausel, die gern überlesen wird: „Wir sind zu klein“ ist kein Freibrief, sondern nur eine andere Organisationsform derselben Pflicht.

Tipp: Hol die örtlich Beauftragten früh in das Projekt

In fast jedem Projekt, das spät eskaliert, wurde die datenschutzbeauftragte Person erst zum Rollout eingeladen — mit der Bitte, doch bitte kurz zuzustimmen. Das ist ungefähr so klug, wie den Statiker erst nach dem Richtfest anzurufen.

Die örtlich Beauftragten sind fachlich weisungsfrei und dürfen wegen ihrer Tätigkeit nicht

benachteiligt werden. Sie sind damit die einzige Person im Haus, die „Nein“ sagen kann, ohne dass es Karriere kostet. Nutze das als Ressource, nicht als Risiko: Wer früh mitkonzipiert, muss später seltener bremsen.

Die katholische Seite: das KDG

Die katholische Kirche hat dieselbe Aufgabe anders gelöst. Das Gesetz über den Kirchlichen Datenschutz wurde von der Vollversammlung der Deutschen Bischofskonferenz beschlossen und dann in den einzelnen Bistümern in Kraft gesetzt. Es gilt für Bistümer, Generalvikariate, Pfarreien mit ihren Pfarrgemeinderäten und Kirchenverwaltungen sowie für die Caritas mit ihren Diözesan-, Kreis- und Ortsverbänden und deren Einrichtungen.

Der auffälligste Unterschied liegt in der Aufsichtsstruktur. Wo die evangelische Seite eine Behörde hat, teilen sich auf katholischer Seite fünf regionale Diözesandatschutzaufsichten die Zuständigkeit — darunter das Katholische Datenschutzzentrum in Dortmund für die nordrhein-westfälischen Bistümer und eine Stelle in Frankfurt am Main für eine weitere Gruppe. Für einen Caritasverband auf Kreisebene ist das sehr übersichtlich. Für einen katholischen Krankenhausverbund mit Standorten in mehreren Bistümern ist es eine Landkarte, die man in der Tenant-Planung kennen sollte.

Zweiter Unterschied: die Gerichtsbarkeit. Das KDG hat eine eigene Verwaltungsgerichtsbarkeit geschaffen — das Interdiözesane Datenschutzgericht in erster Instanz, den Datenschutzgerichtshof bei der Deutschen Bischofskonferenz in zweiter. Auf evangelischer Seite läuft der Rechtsweg über die kirchliche Gerichtsbarkeit der EKD. In beiden Fällen gilt: nicht das staatliche Verwaltungsgericht.

Skizze 2: Zwei Rechtsordnungen im Spiegel — evangelisch und katholisch

	Evangelisch	Katholisch
Gesetz	DSG-EKD — Kirchengesetz über den Datenschutz der EKD; Neufassung im Amtsblatt vom 15. Januar 2025, in Kraft seit 1. Mai 2025	KDG — Gesetz über den Kirchlichen Datenschutz, beschlossen von der Vollversammlung der Deutschen Bischofskonferenz, in den Bistümern in Kraft gesetzt
Aufsicht	ein BfD EKD für Kirche und Diakonie, gegliedert in vier Regionen	fünf regionale Diözesandatschutzaufsichten, darunter das Katholische Datenschutzzentrum in Dortmund und die Stelle in Frankfurt am Main
Gericht	kirchliche Gerichtsbarkeit der EKD	Interdiözesanes Datenschutzgericht, in zweiter Instanz der Datenschutzgerichtshof bei der Deutschen Bischofskonferenz
Mitarbeitervertretung	MVG-EKD — Mitarbeitervertretung, kein Personalrat, kein Betriebsrat	MAVO — Mitarbeitervertretungsordnung des jeweiligen Bistums
Gremium vor Ort	Presbyterium, Kirchenvorstand, Kirchengemeinderat	Pfarrgemeinderat, Kirchenverwaltung, Kirchenvorstand

Gemeinsam: beide Ordnungen fußen auf der Öffnungsklausel des europäischen Datenschutzrechts — die Grundbegriffe gleichen sich, die Zuständigkeiten nicht.

Frage	Evangelisch (DSG-EKD)	Katholisch (KDG)
Rechtsgrundlage	Kirchengesetz der EKD, Neufassung seit 1. Mai 2025 in Kraft	Gesetz der Deutschen Bischofskonferenz, in den Bistümern in Kraft gesetzt
Aufsicht	ein Beauftragter für den Datenschutz der EKD, vier Regionen	fünf regionale Diözesandatenschutzaufsichten
Rechtsweg	kirchliche Gerichtsbarkeit der EKD	Interdiözesanes Datenschutzgericht, dann Datenschutzgerichtshof
Meldung einer Datenpanne	unverzüglich; das Gesetz nennt keine feste Stundenzahl	unverzüglich; dauert es länger als 72 Stunden, ist die Verzögerung zu begründen
Datenschutzbeauftragte	örtlich Beauftragte; Schwelle seit der Reform zwanzig Personen	betriebliche Datenschutzbeauftragte nach den Regeln des KDG
Mitarbeitervertretung	MVG-EKD, Mitarbeitervertretung	MAVO des jeweiligen Bistums, Mitarbeitervertretung
Gremium in der Gemeinde	Presbyterium, Kirchenvorstand, Kirchengemeinderat	Pfarrgemeinderat, Kirchenverwaltung, Kirchenvorstand

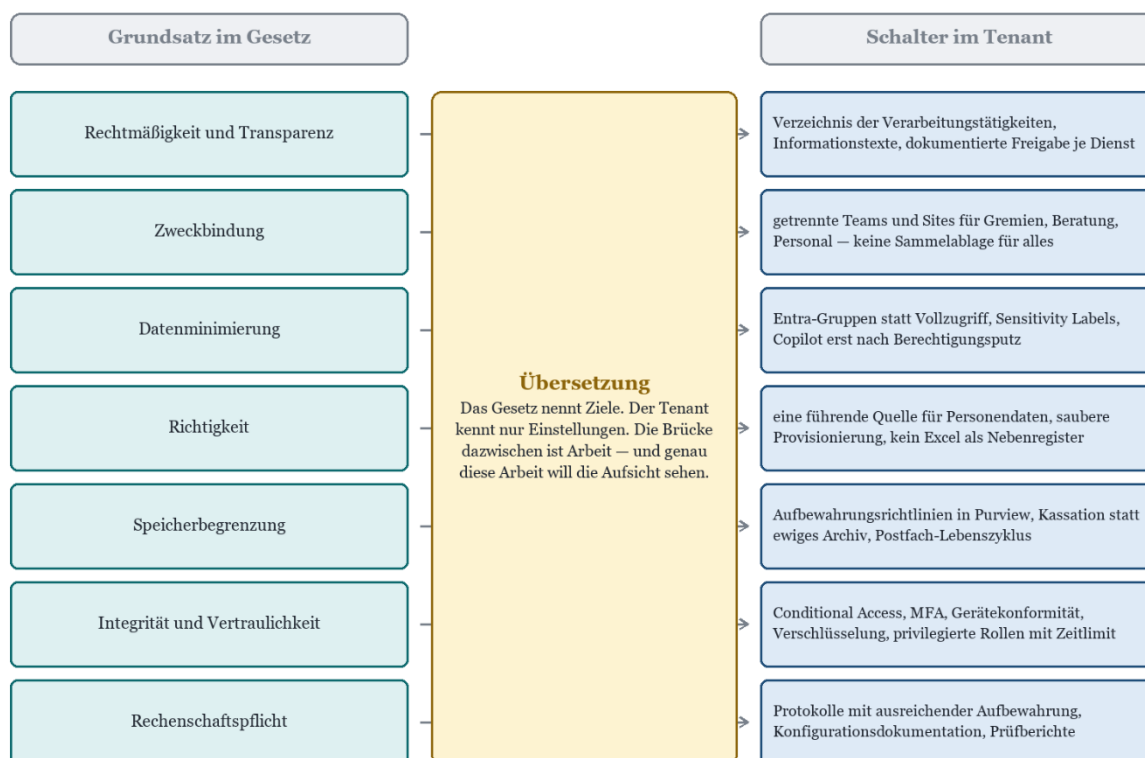
Wenn dich primär die katholische Perspektive interessiert, findest du sie ausführlich in [KDGV verständlich: Microsoft 365 unter dem Kirchlichen Datenschutzgesetz der katholischen Kirche](#). Wie beide Aufsichten in der Praxis prüfen — und was sie an einem Tenant zuerst anschauen — steht in [Kirchliche Datenschutzaufsicht in der Praxis: Was BfD EKD und Diözesandatenschutzbeauftragte von einem Microsoft-365-Tenant erwarten](#).

Die Grundsätze, übersetzt in Tenant-Einstellungen

Das DSGVO-EKD stellt sechs Grundsätze an den Anfang, die dir bekannt vorkommen werden: Rechtmäßigkeit und Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung sowie Integrität und Vertraulichkeit. Dazu kommt eine siebte Pflicht, die den meisten Projekten mehr Arbeit macht als alle anderen zusammen: Die verantwortliche Stelle muss die Einhaltung nachweisen können. Rechenschaftspflicht.

Der Charme dieser Grundsätze ist, dass sie abstrakt genug sind, um in jeder Diskussion zu gewinnen, und konkret genug, um jede Diskussion zu verlieren. „Zweckbindung“ klingt nach Seminar. In einem Tenant bedeutet es, dass die Personalakte nicht im selben Team liegt wie der Gemeindebrief, dass die Beratungsdokumentation nicht über die Suchfunktion in der ganzen Organisation auffindbar ist, und dass ein Kirchenkreis nicht ein einziges „Allgemein“-Team betreibt, in dem seit 2019 alles gelandet ist, was niemand einsortieren wollte.

Skizze 5: Vom Grundsatz zum Schalter – Recht wird Konfiguration



Skizze 5: Jeder Grundsatz hat eine technische Entsprechung. Die Übersetzung dazwischen ist die eigentliche Projektarbeit.

Die Übersetzungstabelle: Anforderung, Konsequenz, Werkzeug

Die folgende Tabelle ist der Kern dieses Beitrags. Sie nimmt die Anforderungen, die sich aus dem DSG-EKD ergeben, benennt die Konsequenz für deinen Tenant und nennt das Werkzeug, mit dem du sie umsetzt. Die katholische Entsprechung ist an jeder Stelle nahezu identisch – das KDG folgt in diesen Punkten derselben Systematik, mit anderen Paragraphennummern.

Anforderung aus dem DSG-EKD	Konsequenz für den Tenant	Microsoft-365-Werkzeug
Verzeichnis der Verarbeitungstätigkeiten führen	Jeder Dienst, der personenbezogene Daten verarbeitet, braucht einen Eintrag – auch Teams, auch OneDrive, auch die Power-Platform-Liste, die jemand „nur mal eben“ gebaut hat	Bestandsaufnahme über Admin Center, SharePoint-Nutzungsberichte, Power Platform Admin Center
Zweckbindung	Getrennte Arbeitsbereiche für Gremien, Personal, Beratung, Seelsorge; keine Sammelablage, keine organisationsweiten Standardberechtigungen	SharePoint-Site-Architektur, Teams-Vorlagen, Entra-Sicherheitsgruppen
Datenminimierung	Berechtigungen nach Bedarf statt nach Bequemlichkeit; „Jeder in der Organisation“ ist keine Berechtigung, sondern ein Verzicht darauf	Entra ID Gruppen, SharePoint-Freigabeeinstellungen, Sensitivity Labels
Speicherbegrenzung und Löschung	Aufbewahrung nach kirchlicher Kassationsordnung, nicht nach Speicherplatz; definierte Lebenszyklen	Microsoft Purview Aufbewahrungsrichtlinien und -bezeichnungen, Teams-

	für Postfächer, Teams, Sites	Ablaufrichtlinien
Integrität und Vertraulichkeit	Mehrstufige Anmeldung für alle, Gerätebedingungen, zeitlich begrenzte Administratorrollen, Verschlüsselung	Conditional Access, Entra ID Protection, Privileged Identity Management, Intune
Besondere Kategorien personenbezogener Daten	Gesundheits-, Sozial- und Religionsdaten brauchen eigene Schutzstufen und eigene Ablagen — nicht dieselbe Site mit einem anderen Ordernamen	Sensitivity Labels mit Verschlüsselung, Data Loss Prevention, Information Barriers
Auftragsverarbeitung dokumentieren	Für Microsoft, Systemhaus und Rechenzentrum je ein Auftrag in Textform, mit Unterauftragskette	Vertragsunterlagen, Microsoft-Produktbestimmungen, Liste der Unterauftragsverarbeiter
Datenschutz-Folgenabschätzung bei hohem Risiko	Vor dem Rollout, nicht danach; besonders bei Copilot, Auswertungen und Protokollierung	dokumentiertes Verfahren, Compliance Manager als Ablage
Meldung von Verletzungen	Ein geübter Ablauf mit Rufnummern, Zuständigkeiten und Beweisquellen — kein Absatz im Handbuch	Purview Audit, Entra-Anmeldeprotokolle, Defender-Vorfälle, eDiscovery
Rechenschaftspflicht	Alles, was oben steht, muss vorzeigbar sein — als Dokument, nicht als „das machen wir schon richtig“	Konfigurationsdokumentation, Protokollaufbewahrung, regelmäßige Überprüfung

Rechenschaftspflicht: Der Screenshot ist kein Nachweis

Die Rechenschaftspflicht ist der Punkt, an dem sich technisch solide Projekte von prüfungsfesten unterscheiden. Ein Tenant kann vorbildlich konfiguriert sein und trotzdem bei einer Prüfung schlecht dastehen, weil niemand erklären kann, warum er so konfiguriert ist. „Das war schon so, als ich kam“ ist die häufigste und ehrlichste Antwort, die man in Bestandsanalysen hört — und die einzige, die garantiert zu einer Nachfrage führt.

Praktisch heißt Rechenschaft: Zu jeder relevanten Einstellung existiert eine Begründung, ein Datum und eine Person, die sie verantwortet. Zu jeder Ausnahme existiert eine befristete Freigabe. Und zu beidem existiert ein Termin, an dem nachgeschaut wird, ob es noch stimmt. Das ist weniger Aufwand, als es klingt, wenn man es von Anfang an mitschreibt — und deutlich mehr Aufwand, wenn man es drei Jahre später rekonstruieren muss.

Warnung: Der häufigste Befund: Protokolle, die zu kurz reichen

Rechenschaft braucht Protokolle, und Protokolle haben eine Haltbarkeit. In Microsoft Purview werden Audit-Einträge im Standardumfang seit Oktober 2023 für 180 Tage aufbewahrt. Die Anmeldeprotokolle in Entra ID reichen mit Entra ID P1 oder P2 dreissig Tage zurück, in der kostenfreien Stufe nur sieben.

Jetzt rechne das gegen die Realität: Ein unbemerkter Zugriff auf eine Beratungsdokumentation fällt oft erst auf, wenn eine betroffene Person nachfragt. Das kann Monate dauern. Wenn dann die Spuren abgelaufen sind, kannst du der Aufsicht weder sagen, was passiert ist, noch dass nichts passiert ist.

Wer länger aufbewahren will, braucht entweder die erweiterten Audit-Funktionen mit entsprechender Lizenzierung oder einen Export in einen eigenen Speicher. Das ist eine Entscheidung mit Preisschild — aber eine, die man einmal trifft und nicht im Krisenfall nachholen kann.

Besondere Kategorien: der kirchliche Sonderfall, der wirklich einer ist

An einer Stelle ist kirchliche IT tatsächlich anders als eine Stadtverwaltung oder ein Mittelständler — und zwar nicht wegen des Gesetzes, sondern wegen der Daten. In einer typischen Landeskirche mit Diakonie liegen in einem einzigen Tenant potenziell: Gesundheitsdaten aus der Pflege, Sozialdaten aus der Jugendhilfe, Schuldner- und Suchtberatungsakten, Kita-Entwicklungsdokumentationen, Personaldaten nach dem Dritten Weg, Religionszugehörigkeiten und im schlimmsten Fall Notizen aus einem Seelsorgegespräch.

Diese Mischung findest du sonst fast nirgends. Ein Krankenhaus hat Gesundheitsdaten, aber keine Kollektabrechnung. Eine Kommune hat Sozialdaten, aber keinen Beichtstuhl. Ein diakonisches Werk in einer Großstadt hat beides und obendrein eine Verwaltung, in der dieselben zwanzig Personen zwischen Gremienunterlagen und Klientenakten hin- und herwechseln. Genau deshalb ist die Trennung von Arbeitsbereichen in kirchlichen Tenants kein Luxus, sondern die tragende Konstruktion.

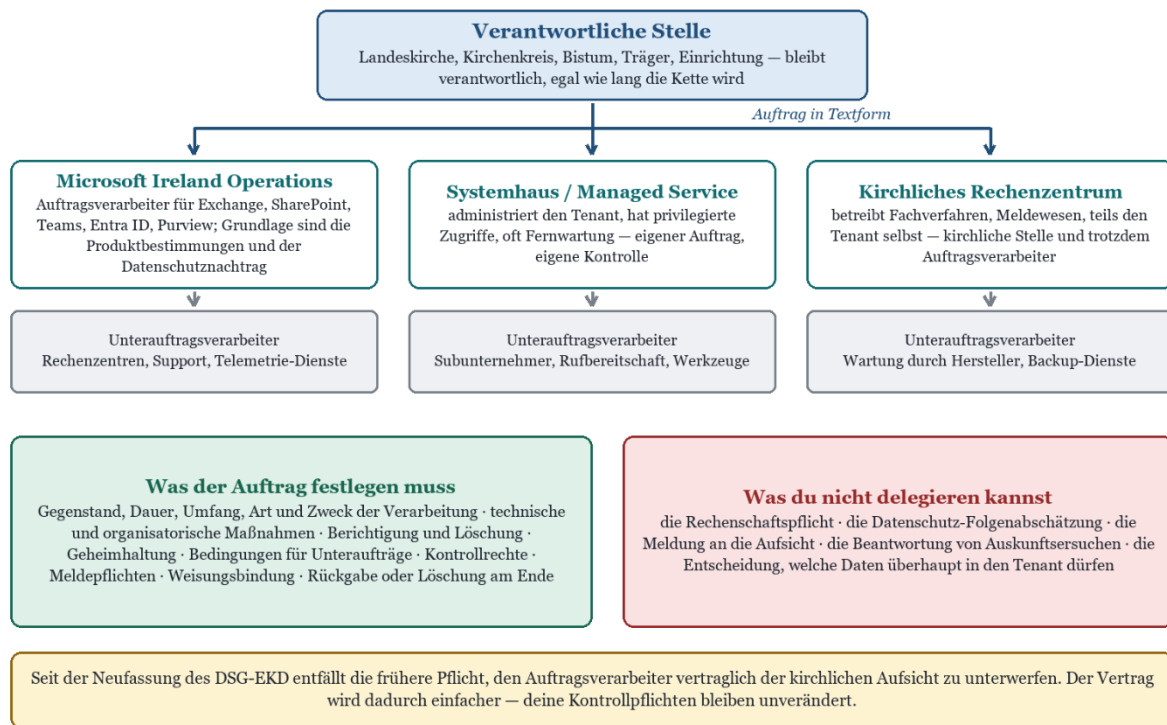
Zwei Themen verdienen dabei eine eigene Betrachtung, weil sie den Rest des Konzepts prägen: [Seelsorgegeheimnis und Beichtgeheimnis in Microsoft 365: Was nie in Teams, OneNote oder Copilot landen darf](#) und [Klientendaten in Diakonie und Caritas: Sozialdaten, Schweigepflicht und Schutz mit Microsoft Purview](#). Beim Seelsorgegeheimnis ist die Antwort übrigens erstaunlich oft: gar nicht in den Tenant. Das ist kein technisches Versagen, sondern eine bewusste Grenzziehung.

Auftragsverarbeitung: Microsoft, Systemhaus, Rechenzentrum

Sobald jemand anderes personenbezogene Daten für dich verarbeitet, brauchst du einen Auftrag. Das DSG-EKD verlangt Textform — nicht zwingend Papier mit Unterschrift, aber auch nicht ein Nicken im Videocall. Und es verlangt, dass der Auftrag im Einzelnen festlegt, worum es geht: Gegenstand, Dauer, Umfang, Art und Zweck der Verarbeitung, die technischen und organisatorischen Maßnahmen, Berichtigung und Löschung, Geheimhaltung, die Bedingungen für Unteraufträge, deine Kontrollrechte, die Meldepflichten, die Weisungsbindung und was am Ende mit den Daten geschieht.

Der entscheidende Satz steht am Anfang der Regelung und wird gern überlesen: Die auftraggebende kirchliche Stelle bleibt für die Einhaltung des Gesetzes verantwortlich. Du kannst den Betrieb auslagern. Du kannst die Administration auslagern. Du kannst die Verantwortung nicht auslagern. Wenn ein Systemhaus eine Freigabe falsch setzt, steht am Ende dein Träger in der Meldung an den BfD EKD, nicht das Systemhaus.

Skizze 3: Die Verantwortungskette — wer verarbeitet was in wessen Auftrag



Skizze 3: Die Kette der Auftragsverarbeitung — und die Aufgaben, die an ihrem Anfang liegen bleiben.

Die gestrichene Unterwerfungsklausel — und was sie nicht bedeutet

Bis zur Reform verlangte das DSGVO-EKD eine Besonderheit, die viele Vertragsverhandlungen zäh gemacht hat: Der Auftragsverarbeiter musste sich vertraglich der kirchlichen Datenschutzaufsicht unterwerfen. Bei kleinen regionalen Dienstleistern war das eine Formalie. Bei einem global agierenden Cloud-Anbieter war es eine Verhandlung, die der BfD EKD ab 2019 geführt hat und für die es am Ende eine Musterzusatzvereinbarung gab.

Diese Regelung ist mit der Neufassung ersatzlos entfallen. Damit wird der Vertragsabschluss mit weltlichen Dienstleistern spürbar einfacher. Was daraus jedoch nicht folgt: dass die Prüfung entfällt. Deine Pflicht, nur mit Auftragsverarbeitern zu arbeiten, die hinreichende Garantien bieten, bleibt bestehen. Nur der Weg, das nachzuweisen, läuft jetzt über Zertifizierungen, Prüfberichte und Vertragsanlagen statt über eine kirchenrechtliche Sonderklausel.

Auf katholischer Seite ist die Konstruktion vergleichbar aufgebaut, aber nicht identisch formuliert. Wer für einen Träger arbeitet, der beiden Ordnungen begegnet — etwa in einer ökumenischen Beratungsstellenkooperation — führt die Vertragsunterlagen besser getrennt und prüft beide Seiten einzeln, statt eine Vorlage zu recyceln.

Fakten: Wo die Daten liegen — der Stand nach der EU-Datengrenze

Microsoft hat sein Programm zur europäischen Datengrenze in drei Stufen umgesetzt und im Februar 2025 für abgeschlossen erklärt. Seit Januar 2023 werden Kundendaten der Kerndienste in der EU gespeichert und verarbeitet, seit Januar 2024 auch pseudonymisierte personenbezogene Daten, seit Februar 2025 zusätzlich die Daten aus professionellen Dienstleistungen, etwa Supportprotokolle.

Wer noch enger binden will, kann Advanced Data Residency hinzubuchen — eine kostenpflichtige Erweiterung mit einer vertraglichen Zusage zur Speicherung ruhender Kundendaten in einer

bestimmten Länderregion, darunter Deutschland. Customer Lockbox verlangt darüber hinaus deine ausdrückliche Zustimmung, bevor Microsoft-Support im Rahmen eines Falles auf Inhalte zugreift. Das ist ein deutlich besseres Fundament als vor fünf Jahren. Es ersetzt aber keine eigene Bewertung — und es beantwortet nicht die Frage, welche Daten überhaupt in eine Cloud gehören. Diese Frage bleibt deine.

Wie die Verträge konkret aussehen, welche Anlagen dazugehören und wie man ein kirchliches Rechenzentrum sauber in die Kette einbindet, steht in [Auftragsverarbeitung nach DSG-EKD und KDG: Microsoft, Systemhaus und Rechenzentrum vertraglich richtig einbinden](#). Die grundsätzliche Standortfrage — kirchliches Rechenzentrum oder Microsoft-Cloud, und wie ehrlich man dabei über Abhängigkeiten redet — behandelt [Die Cloud-Frage in der Kirche: Kirchliche Rechenzentren, Microsoft 365 und die Ehrlichkeit über Datenstandorte](#).

Zentrale Verfahren: die unterschätzte Neuerung

Eine Regelung der Neufassung verdient in Tenant-Projekten mehr Aufmerksamkeit, als sie üblicherweise bekommt: Das Recht der EKD, der Gliedkirchen oder ihrer Zusammenschlüsse kann für zentrale Verfahren festlegen, wie sich datenschutzrechtliche Aufgaben, Befugnisse und Verantwortlichkeiten auf die beteiligten Stellen verteilen. Übersetzt: Wenn eine Landeskirche einen gemeinsamen Tenant für ihre Kirchenkreise und Gemeinden betreibt, lässt sich die Verantwortungsverteilung rechtlich sauber abbilden, statt sie in einem Konvolut bilateraler Vereinbarungen zu simulieren.

Das ist der Unterschied zwischen einer Tenant-Architektur, die man erklären kann, und einer, die man verteidigen muss. Wer gerade vor der Frage steht, ob Kirchengemeinde, Kirchenkreis und Landeskirche einen gemeinsamen oder je eigene Tenants bekommen, sollte diese Regelung kennen, bevor die Entscheidung fällt.

Die Architekturfrage selbst — mit allen Konsequenzen für Identitäten, Lizenzen und Administration — behandelt [Ein Tenant oder viele? Kirchengemeinde, Kirchenkreis, Landeskirche, Bistum und die Frage der Tenant-Architektur](#).

Folgenabschätzung, Meldepflichten und der Ernstfall

Wann eine Datenschutz-Folgenabschätzung fällig ist

Wenn eine Form der Verarbeitung — insbesondere bei Einsatz neuer Technologien — voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen bedeutet, ist vorab eine Folgenabschätzung durchzuführen. Das Gesetz nennt drei Regelfälle: automatisierte Entscheidungsfindung mit Profilbildung, umfangreiche Verarbeitung besonderer Datenkategorien und systematische Überwachung öffentlich zugänglicher Bereiche.

Das Wort „vorab“ ist der Punkt, an dem die meisten Projekte stolpern. Eine Folgenabschätzung, die nach dem Rollout entsteht, ist keine Folgenabschätzung, sondern ein Protokoll. Sie soll die Entscheidung beeinflussen, nicht sie dokumentieren.

Für Microsoft 365 heißt das konkret: Eine reine Umstellung von Dateiserver auf SharePoint mit unveränderten Berechtigungen ist in vielen Fällen keine Verarbeitung mit hohem Risiko. Sobald aber Klientendokumentation aus der Beratung, Pflegedokumentation oder Personalauswertungen betroffen sind, sieht das anders aus. Und bei Copilot sieht es grundsätzlich anders aus — nicht weil

der Dienst gefährlich wäre, sondern weil er vorhandene Berechtigungsfehler mit einer Effizienz sichtbar macht, die man vorher nicht für möglich gehalten hätte.

Warnung: Copilot ist kein Datenschutzproblem — er ist ein Aufdeckungswerkzeug

Ein Sprachmodell, das über alle Inhalte suchen darf, auf die eine Person Zugriff hat, findet auch die Inhalte, auf die sie eigentlich keinen Zugriff haben sollte. In kirchlichen Tenants ist das selten Absicht und fast immer Geschichte: Ein Team, das 2020 „nur kurz“ für alle geöffnet wurde. Eine Site, deren Berechtigungsvererbung jemand aufgebrochen und nie wieder zusammengesetzt hat. Ein Freigabelink ohne Ablaufdatum.

Wenn in demselben Tenant Beratungsakten, Pflegedokumentation oder Personalvorgänge liegen, ist das kein akademisches Risiko. Die Folgenabschätzung für Copilot beginnt deshalb nicht beim Sprachmodell, sondern bei einer ehrlichen Berechtigungsanalyse. Wer diesen Schritt überspringt, hat kein Copilot-Projekt, sondern eine gut getarnte Datenpanne mit Rollout-Termin.

Wie eine Folgenabschätzung für einen Microsoft-365-Tenant methodisch aufgebaut wird und welche Befunde regelmäßig auftauchen, steht in [Datenschutz-Folgenabschätzung für Microsoft 365 nach DSG-EKD und KDG: Vorgehen, Muster und typische Befunde](#). Speziell zu Copilot — Nutzen, Grenzen und die Überprüfung vor dem Rollout — gibt es [Copilot in Kirche und Diakonie: Nutzen, Grenzen, Oversharing und die Copilot-Überprüfung vor dem Rollout](#).

Wenn es knallt: die Meldung an die Aufsicht

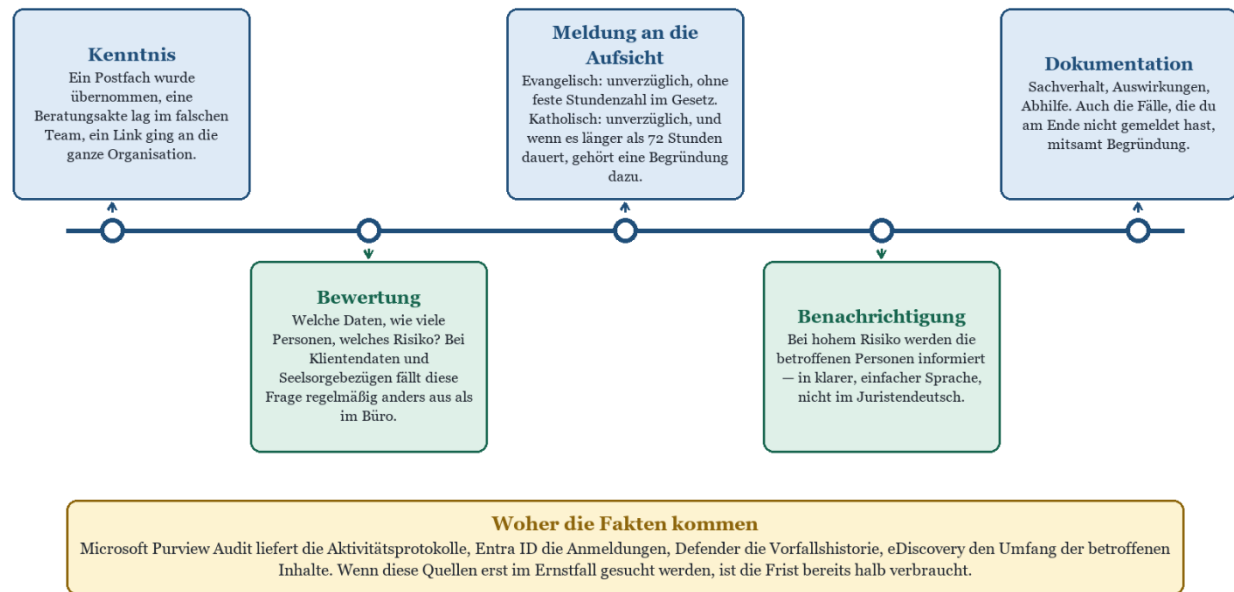
Hier liegt einer der wenigen wirklich harten Unterschiede zwischen den beiden Ordnungen — und einer, den man kennen muss, bevor man ihn braucht.

Das DSG-EKD verlangt, dass die verantwortliche Stelle eine Verletzung des Schutzes personenbezogener Daten unverzüglich der Aufsichtsbehörde meldet, wenn damit ein nicht unerhebliches Risiko verbunden ist. Eine feste Stundenzahl nennt das Gesetz nicht. „Unverzüglich“ bedeutet im deutschen Rechtsverständnis „ohne schuldhaftes Zögern“ — was in der Praxis nicht großzügiger ist als eine Frist, sondern nur schlechter planbar.

Das KDG formuliert es anders: unverzüglich, und wenn die Meldung nicht binnen 72 Stunden nach Bekanntwerden erfolgt, ist eine Begründung für die Verzögerung beizufügen. Diese 72 Stunden sind keine Schonfrist, sondern der Punkt, ab dem du dich erklären musst.

Der Auftragsverarbeiter meldet in beiden Ordnungen nicht der Aufsicht, sondern dir. Das ist ein Punkt, den man in Verträgen mit Systemhäusern prüfen sollte: Wie schnell erfährst du von einem Vorfall, den dein Dienstleister bemerkt? Wenn dort „unverzüglich“ steht und der Dienstleister das als „im nächsten Jour fixe“ versteht, hast du ein Problem, das keine Technik löst.

Skizze 4: Von der Kenntnis zur Meldung – der Ablauf bei einer Datenpanne



Skizze 4: Der Ablauf vom ersten Verdacht bis zur Dokumentation – mit den Unterschieden zwischen beiden Ordnungen.

Schritt	Was zu tun ist	Woher die Fakten kommen
Kenntnis	Zeitpunkt festhalten – ab hier läuft die Bewertung, nicht ab der ersten Krisensitzung	Ticketsystem, Defender-Vorfall, Meldung durch das Team
Eingrenzung	Welche Postfächer, Sites, Teams, Konten sind betroffen?	Purview Audit, Entra-Anmeldeprotokolle, SharePoint-Freigabeberichte
Risikobewertung	Welche Datenkategorien, wie viele Personen, welche Folgen? Klientendaten und Seelsorgebezüge ändern das Ergebnis	Verzeichnis der Verarbeitungstätigkeiten, Sensitivity Labels, eDiscovery-Suche
Meldung	Evangelisch an den BfD EKD, katholisch an die zuständige Diözesandatschutzaufsicht – beide bieten Online-Formulare	vorbereitete Meldevorlage mit Kontaktdaten der Beauftragten
Benachrichtigung	Bei hohem Risiko die betroffenen Personen informieren, in klarer, einfacher Sprache	Adressbestände, Textbausteine, abgestimmter Kommunikationsweg
Dokumentation	Sachverhalt, Auswirkungen, Abhilfe – auch bei Fällen, die du nicht gemeldet hast	Vorfallsakte, Abschlussbericht, Maßnahmenverfolgung

Der komplette Meldeablauf inklusive Formularen, Zuständigkeiten und einer Übung, die man tatsächlich durchspielen kann, steht in [Datenpannen bei kirchlichen Trägern: Meldung an BfD EKD oder Diözesandatschutzbeauftragten, Fristen, Ablauf und Übung](#).

Was die Aufsicht bei einer Prüfung sehen will

Prüfungen kommen selten überraschend und fast nie ohne Anlass – meist steht eine Beschwerde, eine gemeldete Panne oder eine turnusmäßige Befragung dahinter. Die Unterlagen, nach denen dann gefragt wird, sind erstaunlich vorhersehbar. Deshalb lohnt es sich, sie vorher zu haben.

Tipp: Der Ordner, den du vor der Prüfung haben solltest

Lege ihn heute an, nicht wenn der Brief kommt. Zwei Tage Arbeit jetzt sparen dir zwei Wochen Panik

später. Diese Unterlagen werden typischerweise verlangt:

- Das Verzeichnis der Verarbeitungstätigkeiten — aktuell, mit Datum, und mit einem Eintrag je Microsoft-365-Dienst statt einer Sammelzeile „Microsoft 365“.
- Die Bestellungsurkunde der örtlich Beauftragten und der Nachweis, dass die Bestellung der Aufsicht gemeldet wurde.
- Die Aufträge zur Verarbeitung im Auftrag: Microsoft, Systemhaus, kirchliches Rechenzentrum, Fachverfahrenshersteller — samt Liste der Unterauftragsverarbeiter.
- Die Datenschutz-Folgenabschätzung für die risikoreichen Verarbeitungen, mit Datum vor dem Rollout.
- Das IT-Sicherheitskonzept nach der IT-Sicherheitsverordnung der EKD, auf dem aktuellen Stand — nicht die Fassung, die vor zwei Migrationen galt.
- Das Berechtigungskonzept: Wer darf was, wie werden Rollen vergeben, wie werden sie entzogen, wann wurde zuletzt geprüft.
- Die technischen und organisatorischen Maßnahmen als Dokument — inklusive Conditional-Access-Regelwerk, Protokollierung und Aufbewahrungsdauer.
- Das Lösch- und Aufbewahrungskonzept mit Bezug auf die kirchliche Kassationsordnung und die Archivregelungen.
- Die Dokumentation der Schulungen und Verpflichtungen auf das Datengeheimnis — mit Teilnahmenachweis, nicht mit Einladungsverteiler.
- Die Vorfallsdokumentation der letzten Jahre, auch für die Fälle, die am Ende nicht meldepflichtig waren.
- Die Dienstvereinbarungen mit der Mitarbeitervertretung, soweit sie Microsoft 365, Protokollierung oder Auswertungen betreffen.
- Die Informationstexte für betroffene Personen und das Verfahren, mit dem Auskunftersuchen bearbeitet werden.

Ein Hinweis zur letzten Zeile: Die Reform hat die Betroffenenrechte deutlich näher an das europäische Recht gerückt. Informationen sind jetzt bereits bei der Erhebung zu erteilen und nicht erst auf Verlangen. Wer sein Auskunftsverfahren zuletzt vor 2025 beschrieben hat, sollte es gegenlesen — und dabei gleich prüfen, wie er in einem gewachsenen Microsoft-365-Tenant überhaupt alle Daten zu einer Person findet. Die ehrliche Antwort lautet in vielen Häusern: mit eDiscovery, Geduld und einem gewissen Maß an Glück.

Mitbestimmung: warum Datenschutz allein nicht reicht

Es gibt einen Fehler, der in kirchlichen Microsoft-365-Projekten mit erstaunlicher Regelmäßigkeit gemacht wird, und er ist teuer: Die datenschutzbeauftragte Person hat zugestimmt, also ist alles geklärt. Ist es nicht. Datenschutz und Mitbestimmung sind zwei getrennte Verfahren mit zwei getrennten Gremien und zwei getrennten Rechtsgrundlagen.

In der evangelischen Kirche und ihrer Diakonie gilt das Mitarbeitervertretungsgesetz der EKD, auf katholischer Seite die Mitarbeitervertretungsordnung des jeweiligen Bistums. Beide kennen keinen Betriebsrat und keinen Personalrat, sondern die Mitarbeitervertretung — Ausdruck der Dienstgemeinschaft und des Dritten Weges, auf dem Arbeitsbedingungen in Kirche und Diakonie über die AVR und arbeitsrechtliche Kommissionen geregelt werden statt über Tarifkonflikte.

Für dein Projekt ist die praktische Konsequenz einfach: Sobald ein System geeignet ist, das Verhalten oder die Leistung der Belegschaft zu überwachen, reden wir über Mitbestimmung. Und Microsoft 365 ist dazu geeignet — nicht weil jemand es vorhätte, sondern weil Anwesenheitsanzeigen, Nutzungsberichte, Anmeldeprotokolle und Auswertungen technisch

vorhanden sind. Der übliche und richtige Weg ist eine Dienstvereinbarung, die beschreibt, was ausgewertet wird, was nicht, wer darauf zugreift und was mit den Daten geschieht.

Wichtig: Zwei Verfahren, zwei Unterschriften

Die Zustimmung der örtlich Beauftragten für den Datenschutz ersetzt keine Beteiligung der Mitarbeitervertretung — und umgekehrt genauso wenig. Beide Verfahren laufen parallel und beide können ein Projekt aufhalten.

Die praktische Empfehlung: Nimm die MAV zum selben Zeitpunkt in das Projekt wie die datenschutzbeauftragte Person, also am Anfang. Eine Dienstvereinbarung, die gemeinsam entsteht, braucht Wochen. Eine, die nach dem Pilotbetrieb verhandelt wird, braucht Monate — und beginnt mit einer Vertrauensfrage, die man sich hätte sparen können.

Wie eine Dienstvereinbarung zu Teams, Copilot und Protokollierung aufgebaut wird und welche Punkte MVG-EKD und MAVO dabei jeweils verlangen, behandelt [Mitarbeitervertretung und Microsoft 365: MVG-EKD, MAVO, Dienstvereinbarung und Mitbestimmung bei Teams, Copilot und Protokollierung](#).

Wo die Abgrenzung zur Kommune wirklich besteht

Zum Schluss dieses Abschnitts eine Einordnung, die vor übertriebener Sonderbehandlung schützt. Kirchliche Träger unterscheiden sich von einer Stadtverwaltung an vier Punkten, und an genau diesen vier: Sie haben eine eigene Rechtsordnung, sie haben eine eigene Aufsicht, sie haben eine Mitarbeitervertretung statt eines Personalrats, und sie verarbeiten in großem Umfang Klientendaten mit besonderem Schutzbedarf.

Alles andere ist normales Microsoft 365. Conditional Access funktioniert im Landeskirchenamt genauso wie in der Kreisverwaltung. SharePoint hat dieselben Berechtigungsfallen. Teams-Telefonie klingelt gleich. Wer aus dem kirchlichen Sonderrecht ableitet, dass jede technische Standardlösung neu erfunden werden muss, verbrennt Budget an Stellen, an denen es nichts zu holen gibt — und hat es dann nicht mehr für die vier Punkte, an denen es wirklich darauf ankommt.

Diese Einordnung im Detail — mit dem Vergleich zu Kommune und Mittelstand — findest du in [Microsoft 365 in Kirche, Diakonie und Caritas: Was wirklich anders ist als in Kommune und Mittelstand](#). Eine kompakte Gegenüberstellung beider Datenschutzordnungen aus Verwaltungssicht bietet außerdem [Microsoft 365 für kirchliche Träger: DSGVO-EKD und KDG](#).

Häufige Fragen

Darf ein kirchlicher Träger Microsoft 365 überhaupt einsetzen?

Ja. Es gibt kein Verbot im DSGVO-EKD und keines im KDG. Beide Ordnungen regeln, unter welchen Bedingungen personenbezogene Daten verarbeitet werden dürfen, nicht welcher Hersteller dafür zulässig ist. Der BfD EKD hat bereits 2020 einen Weg beschrieben, wie Microsoft-Cloud-Dienste datenschutzkonform genutzt werden können — damals noch mit einer kirchenrechtlichen Zusatzvereinbarung, die mit der Reform entfallen ist. Was bleibt, ist die Anforderung, den Einsatz zu bewerten, zu dokumentieren und die Schutzmaßnahmen tatsächlich umzusetzen. Wer das tut, hat ein tragfähiges Projekt. Wer darauf hofft, dass niemand fragt, hat ein Risiko mit Ablaufdatum.

Brauchen wir eine Datenschutz-Folgenabschätzung für den ganzen Tenant?

Nein, und das ist eine gute Nachricht. Die Folgenabschätzung bezieht sich auf Verarbeitungen, nicht auf Produkte. Sinnvoll ist eine Betrachtung je Verarbeitungsbereich: Verwaltung und Gremienarbeit, Beratung und Klientenarbeit, Personalwesen, gegebenenfalls Copilot als eigener Fall. Ein einziges Dokument mit dem Titel „DSFA Microsoft 365“ ist meist entweder so allgemein, dass es nichts aussagt, oder so lang, dass es niemand liest. Beides hilft der Aufsicht nicht und dir auch nicht.

Unsere Kirchengemeinde hat sechs Personen im Büro. Gilt das trotzdem alles?

Das Gesetz gilt, ja. Der Aufwand skaliert aber. Die Bestellungspflicht für örtlich Beauftragte greift erst ab zwanzig Personen, die ständig mit automatisierter Verarbeitung betraut sind — mit der wichtigen Ausnahme, dass die Kerntätigkeit nicht in umfangreicher Verarbeitung besonderer Datenkategorien bestehen darf. Auch das Verzeichnis der Verarbeitungstätigkeiten kennt eine Ausnahme für kleine Stellen, allerdings mit Rückausnahmen, die in der Praxis oft greifen. Der übliche und vernünftige Weg: Der Kirchenkreis oder die Landeskirche stellt gemeinsame Beauftragte, gemeinsame Konzepte und gemeinsame Vorlagen. Sechs Personen in einem Pfarramt sollen Gemeindegarbeit machen, nicht Datenschutzrecht.

Was passiert, wenn wir eine Panne nicht melden?

Zunächst: oft nichts. Danach: unter Umständen sehr viel. Die unterlassene Meldung ist ein eigenständiger Verstoß, und sie wiegt in der Bewertung durch die Aufsicht regelmäßig schwerer als der Vorfall selbst — weil sie Vorsätzlichkeit nahelegt, wo sonst nur Pech war. Dazu kommt: Betroffene Personen können sich direkt bei der Aufsicht beschweren, und in der Diakonie mit ihren Klientenkontakten passiert genau das. Die Bußgeldobergrenze liegt seit der Reform bei sechs Millionen Euro, wobei Bußgelder nur für wirtschaftliche Tätigkeiten in Betracht kommen. Der größere Schaden ist ohnehin meist ein anderer: Vertrauen, das eine Beratungsstelle braucht, um überhaupt zu funktionieren.

Reicht die Zustimmung der datenschutzbeauftragten Person für den Rollout?

Nein. Datenschutz und Mitbestimmung sind getrennt. Ohne Beteiligung der Mitarbeitervertretung nach MVG-EKD beziehungsweise MAVO fehlt dir die zweite Hälfte der Grundlage — und zwar bei allem, was Verhalten oder Leistung auswertbar macht. Das betrifft in Microsoft 365 mehr Funktionen, als man beim ersten Hinsehen vermutet.

Wo genau liegen unsere Daten?

Für Kunden mit Anmeldeort in der EU oder EFTA gilt die europäische Datengrenze von Microsoft, deren Umsetzung im Februar 2025 für abgeschlossen erklärt wurde: Kundendaten, pseudonymisierte personenbezogene Daten und die Daten aus professionellen Dienstleistungen werden in der EU beziehungsweise EFTA gespeichert und verarbeitet. Wer eine vertragliche Zusage für die Speicherung ruhender Daten in einer bestimmten Länderregion braucht, kann Advanced Data Residency als kostenpflichtige Erweiterung hinzubuchen. Wichtig für Gremienvorlagen: Das ist eine differenzierte Antwort, keine Ja-Nein-Antwort. Wer im

Presbyterium behauptet, alles liege garantiert in Deutschland, wird beim nächsten Nachfragen unangenehm genau werden müssen.

Müssen die Gemeindegliederdaten aus dem Meldewesen in den Tenant?

Nein, und in aller Regel sollen sie das auch nicht. Das kirchliche Meldewesen läuft über eigene Verfahren mit eigenen Rechtsgrundlagen und eigenen Zugriffsregeln. Der Reflex, „damit alles an einem Ort ist“ eine Kopie in SharePoint zu legen, erzeugt genau die Schattenbestände, die später niemand mehr pflegt und die bei einer Prüfung als Erstes auffallen. Ausführlicher steht das in dem Beitrag zum Meldewesen weiter unten im Weiter-Kasten.

Was ist mit ehrenamtlich Tätigen?

Sie sind der Punkt, an dem kirchliche Tenants sich von jedem Unternehmens-Tenant unterscheiden — nicht rechtlich, sondern zahlenmäßig. Eine Kirchengemeinde hat oft mehr ehrenamtlich Tätige als Angestellte, und viele davon sollen an Gremienunterlagen mitarbeiten. Datenschutzrechtlich brauchen sie dieselbe Verpflichtung auf das Datengeheimnis wie Angestellte und dieselbe Einweisung. Technisch reicht die Bandbreite vom Gastzugang über eigene Konten bis zur bewussten Entscheidung, bestimmte Inhalte gar nicht digital zugänglich zu machen. Es gibt keine allgemeingültig richtige Antwort — aber eine falsche: das persönliche Privatpostfach eines Presbyteriumsmitglieds als De-facto-Gremienablage.

Gilt für uns das DSG-EKD oder das KDG, wenn wir ökumenisch kooperieren?

Beides — jeweils für die eigene Seite. Eine gemeinsame Beratungsstelle in Trägerschaft eines diakonischen Werks und eines Caritasverbandes hat zwei Verantwortliche unter zwei Rechtsordnungen mit zwei Aufsichten. Das ist handhabbar, verlangt aber eine klare Zuordnung: Wer ist für welche Daten verantwortlich, wo liegen sie, wer meldet bei einer Panne an wen. Diese Klärung gehört vor die Tenant-Entscheidung. Danach ist sie deutlich teurer.

Fazit

Das DSG-EKD ist kein Hindernis für Microsoft 365. Es ist eine eigenständige Rechtsordnung mit eigener Aufsicht, eigenem Rechtsweg und einem Anwendungsbereich, der von der Landeskirche bis zur Kita reicht. Inhaltlich verlangt es das, was gutes IT-Management ohnehin verlangt: zu wissen, welche Daten wo liegen, warum sie dort liegen, wer darauf zugreift und wann sie verschwinden.

Die Reform, die seit dem 1. Mai 2025 gilt, hat das Ganze eher einfacher gemacht als schwerer: näher am europäischen Recht, ohne die Sonderklausel zur Unterwerfung von Auftragsverarbeitern, mit einer höheren Schwelle für die Bestellung örtlich Beauftragter. Was härter geworden ist, sind die Konsequenzen: eine Bußgeldobergrenze von sechs Millionen Euro und Betroffenenrechte, die man nicht mehr durch Fristverlängerung entschärft.

Wer jetzt anfängt, fängt an der richtigen Stelle an: bei einer ehrlichen Bestandsaufnahme des vorhandenen Tenants, bei einem Verzeichnis, das den Namen verdient, und bei einem Gespräch mit der datenschutzbeauftragten Person und der Mitarbeitervertretung, das nicht mit einer Unterschriftenbitte beginnt. Alles andere — Labels, Aufbewahrung, Conditional Access, Copilot-Vorbereitung — baut darauf auf und wird deutlich billiger, wenn das Fundament stimmt.

Und wenn beim nächsten Mal jemand in der Runde sagt, das gehe wegen des DSG-EKD alles nicht, kannst du sinngemäß antworten: Doch, das geht. Es geht nur nicht ohne Hausaufgaben. Das ist eine deutlich bessere Nachricht, als sie im ersten Moment klingt.

Weiterlesen

- › [Microsoft 365 in Kirche, Diakonie und Caritas](#) — die Übersicht der gesamten Serie
- › [KDG verständlich: Microsoft 365 unter dem Kirchlichen Datenschutzgesetz der katholischen Kirche](#) — dieselbe Frage von der katholischen Seite
- › [Kirchliche Datenschutzaufsicht in der Praxis: Was BfD EKD und Diözesandatenschutzbeauftragte von einem Microsoft-365-Tenant erwarten](#) — was bei einer Prüfung tatsächlich passiert
- › [Auftragsverarbeitung nach DSG-EKD und KDG: Microsoft, Systemhaus und Rechenzentrum vertraglich richtig einbinden](#) — die Vertragskette im Detail
- › [Datenschutz-Folgenabschätzung für Microsoft 365 nach DSG-EKD und KDG: Vorgehen, Muster und typische Befunde](#) — Methodik und Vorlagen
- › [Datenpannen bei kirchlichen Trägern: Meldung an BfD EKD oder Diözesandatenschutzbeauftragten, Fristen, Ablauf und Übung](#) — der Ernstfall, geübt
- › [Mitarbeitervertretung und Microsoft 365: MVG-EKD, MAVO, Dienstvereinbarung und Mitbestimmung bei Teams, Copilot und Protokollierung](#) — die zweite Hälfte der Grundlage
- › [Meldewesen und Gemeindegliederdaten: Warum Kirchenmitgliederdaten getrennt von Microsoft 365 bleiben](#) — die Grenze zum Fachverfahren
- › [Sensitivity Labels für kirchliche Träger: Ein Label-Konzept vom Gemeindebrief bis zur Beratungsakte](#) — Schutzstufen, die im Alltag funktionieren
- › [Kirchliche Aufbewahrungsfristen, Kassationsordnungen und Archivgesetze in Microsoft Purview abbilden](#) — Speicherbegrenzung in der Praxis

Wenn du das Ganze nicht allein sortieren willst: Wir begleiten kirchliche und diakonische Träger von der Bestandsaufnahme bis zum prüfungsfesten Tenant — Details unter [Microsoft 365 Beratung für kirchliche Träger](#). Wer zuerst die eigene Mannschaft sprachfähig machen will, findet passende Formate unter [Microsoft 365 Schulung für kirchliche Träger](#).