Kirchliche Datenschutzaufsicht in der Praxis: Was BfD EKD und Diözesandatenschutzbeauftragte von einem Microsoft-365-Tenant erwarten

Es gibt zwei Arten, wie kirchliche Träger ihrer eigenen Datenschutzaufsicht begegnen. Die erste: Man schreibt der Aufsicht, bevor der Tenant produktiv geht, schildert das Vorhaben, fragt nach Einschätzung, bekommt Rückfragen, arbeitet sie ab. Die zweite: Die Aufsicht schreibt zuerst, weil sich jemand beschwert hat oder weil eine Meldung über eine Datenpanne eingegangen ist. Beide Wege enden bei denselben Unterlagen. Nur ist der Zeitdruck ein sehr unterschiedlicher.

Dieser Artikel beschreibt den ersten Weg und bereitet auf den zweiten vor. Er sagt dir, wer bei dir überhaupt zuständig ist, was die Aufsicht fragen darf, welche sechs Nachweise sie regelmäßig sehen will, wo diese Nachweise in einem Microsoft-365-Tenant entstehen — und wo sie eben nicht entstehen, sondern von Menschen geschrieben werden müssen. Und er sagt ehrlich, wie der Stand der Diskussion ist. Beruhigungspillen gibt es hier keine: Wer behauptet, Microsoft 365 sei im kirchlichen Rechtskreis pauschal geklärt, hat entweder nicht gelesen oder etwas zu verkaufen.

Dieser Beitrag gehört zur Serie Microsoft 365 in Kirche, Diakonie und Caritas. Wenn du die rechtlichen Grundlagen noch nicht sortiert hast, lies zuerst DSG-EKD verständlich: Was das evangelische Datenschutzgesetz für Microsoft 365 konkret bedeutet beziehungsweise KDG verständlich: Microsoft 365 unter dem Kirchlichen Datenschutzgesetz der katholischen Kirche. Hier geht es um das, was danach kommt: das Gespräch mit der Aufsicht.

Wer da eigentlich vor dir sitzt

Bevor du irgendetwas vorbereitest, klär die banalste aller Fragen: Welche Aufsicht ist für deine Einrichtung zuständig? Erstaunlich viele Häuser beantworten diese Frage falsch, weil ihr Systemhaus reflexhaft auf die Landesbeauftragte für den Datenschutz verweist. Die ist zwar fachlich oft hilfreich, aber für eine kirchliche Stelle, auf die kirchliches Datenschutzrecht Anwendung findet, schlicht nicht die entscheidende Instanz.

Evangelisch: der Beauftragte für den Datenschutz der EKD

Auf evangelischer Seite ist in aller Regel der Beauftragte für den Datenschutz der EKD zuständig — für die EKD selbst, für die allermeisten Gliedkirchen und ihre Zusammenschlüsse sowie für die zugeordneten diakonischen Werke und Einrichtungen, unabhängig von deren Rechtsform. Die Dienststelle sitzt in Hannover und arbeitet in vier Datenschutzregionen mit Außenstellen in Hannover, Berlin, Ulm und Dortmund. Dein Ansprechpartner ist damit nicht abstrakt „die EKD“, sondern eine benannte Region.

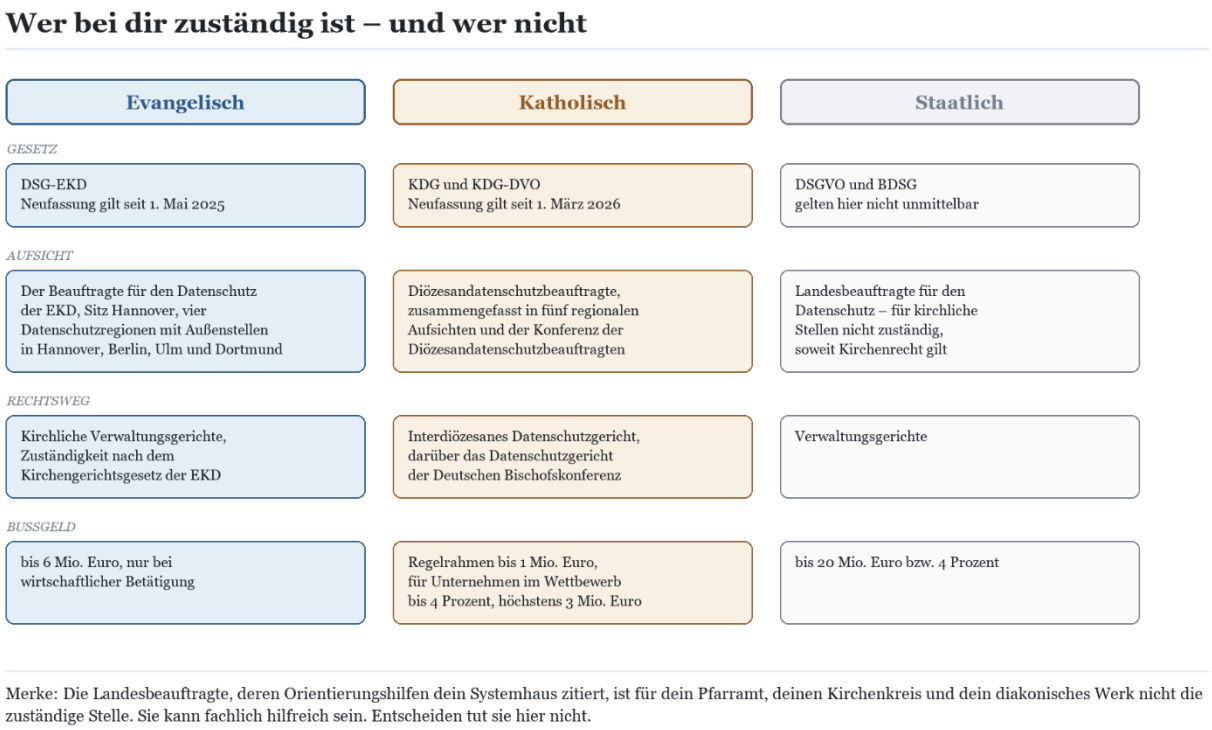
Die Rechtsgrundlage ist das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland. Es wurde am 13. November 2024 von der Synode der EKD novelliert, im Januar 2025 im Amtsblatt veröffentlicht und gilt in der neuen Fassung seit dem 1. Mai 2025. Wenn in deinem Haus noch eine Handreichung von 2019 im Umlauf ist, die Paragrafen zitiert: Vorsicht. Einiges ist verschoben, manches inhaltlich geändert.

Katholisch: Diözesandatenschutzbeauftragte und Datenschutzzentren

Auf katholischer Seite ist die Struktur föderaler und für Außenstehende zunächst unübersichtlich: Jede Diözese hat eine oder einen Diözesandatenschutzbeauftragten. Praktisch sind diese Aufgaben in fünf regionalen Aufsichten gebündelt — für den Norden, den Osten, Nordrhein-Westfalen, die Mitte und Bayern. Fachlich abgestimmt wird in der Konferenz der Diözesandatenschutzbeauftragten der katholischen Kirche Deutschlands, die gemeinsame Beschlüsse fasst und Arbeitshilfen herausgibt.

Maßgeblich ist das Gesetz über den Kirchlichen Datenschutz mit seiner Durchführungsverordnung. Beide wurden am 24. November 2025 von der Vollversammlung des Verbandes der Diözesen Deutschlands neu gefasst, im Dezember 2025 veröffentlicht und gelten seit dem 1. März 2026. Am 27. Februar 2026 hat die Konferenz der Diözesandatenschutzbeauftragten dazu eine Arbeitshilfe veröffentlicht. Wenn du auf katholischer Seite in ein Aufsichtsgespräch gehst und die Novelle noch nicht durchgearbeitet hast, führst du eine Diskussion über ein Gesetz, das es so nicht mehr gibt.

Für die Zuständigkeit gilt: Bei über- oder mehrdiözesanen Rechtsträgern richtet sich die Aufsicht nach dem Sitz des Rechtsträgers, nicht nach dem Sitz der einzelnen Einrichtung. Ein Krankenhausverbund mit Standorten in drei Bistümern hat also nicht drei Aufsichten, sondern eine — die des Sitzbistums des Trägers. Das erspart Abstimmungsschleifen und ist ein Argument für saubere Trägerstrukturen, bevor man über Tenants redet.



Skizze 1: Zwei Rechtskreise, zwei Aufsichten, ein Microsoft-365-Tenant. Die staatliche Spalte steht nur zum Vergleich da.

Was die Aufsicht darf — und was du liefern musst

Die Befugnisse der kirchlichen Aufsichten sind denen der staatlichen nachgebildet und reichen deutlich weiter, als viele Leitungen annehmen. Auf katholischer Seite steht ausdrücklich im Gesetz, dass kirchliche Stellen den Anweisungen der Datenschutzaufsicht Folge zu leisten, ihr Auskunft zu

geben, Einsicht in alle Unterlagen und Akten zu gewähren — namentlich in gespeicherte Daten und Datenverarbeitungsprogramme — und während der Dienstzeit Zutritt zu allen Diensträumen zu ermöglichen haben, die der Verarbeitung dienen. Untersuchungen in Form von Datenschutzüberprüfungen sind zuzulassen.

FAKTEN · Die Befugnisse der Aufsicht, kurz sortiert

Untersuchungsbefugnisse: Informationen anfordern, Datenschutzüberprüfungen durchführen, Zugang zu personenbezogenen Daten und zu Räumlichkeiten einschließlich Datenverarbeitungsanlagen erhalten.

Abhilfebefugnisse: warnen, verwarnen, anweisen, Verarbeitungsvorgänge innerhalb einer bestimmten Frist in Einklang mit dem Gesetz bringen lassen, die Verarbeitung vorübergehend oder endgültig beschränken oder verbieten, Löschung anordnen, Datenübermittlungen in Drittländer aussetzen, Geldbußen verhängen.

Eskalation: Werden Maßnahmen nicht in der gesetzten Frist befolgt, verständigt die katholische Datenschutzaufsicht die für die kirchliche Stelle zuständige Aufsicht und fordert eine Stellungnahme an. Auf gut Deutsch: Das Generalvikariat erfährt davon.

Bußgeldrahmen: Auf katholischer Seite wurde die allgemeine Obergrenze mit der Novelle von 500.000 auf eine Million Euro angehoben; für Unternehmen im Wettbewerb gilt ein Rahmen von vier Prozent des Jahreseinkommens, höchstens drei Millionen Euro. Auf evangelischer Seite liegt der Rahmen bei sechs Millionen Euro, beschränkt auf wirtschaftliche Betätigung — die Kirchengemeinde, die Gottesdienste feiert, ist davon nicht erfasst, das Altenheim im Wettbewerb sehr wohl.

Praktisch relevant ist der letzte Punkt seltener, als der Blutdruck vermuten lässt. Die kirchlichen Aufsichten arbeiten überwiegend beratend, und der Regelfall eines Verfahrens endet mit einer Maßnahmenliste und einer Frist, nicht mit einem Bescheid. Die Verhandlungsposition ist trotzdem eine andere, wenn man weiß, dass am Ende der Skala ein Verarbeitungsverbot steht.

Der Stand der Diskussion, ehrlich erzählt

Jetzt der unangenehme Teil. Es gibt keine Freigabe für Microsoft 365 durch eine kirchliche Datenschutzaufsicht. Es gibt kein Papier, das du ausdrucken und in den Ordner heften kannst, auf dem steht: geprüft, konform, viel Erfolg. Wer dir etwas anderes erzählt, verwechselt vermutlich eine Broschüre mit einem Verwaltungsakt.

Was tatsächlich veröffentlicht ist

Der BfD EKD hat sich Ende November 2022 der Feststellung der Datenschutzkonferenz angeschlossen, dass der Einsatz von Microsoft 365 nicht datenschutzkonform möglich sei, solange nicht die notwendige Transparenz über die Verarbeitung personenbezogener Daten zu eigenen Zwecken des Anbieters hergestellt und deren Rechtmäßigkeit belegt sei. Diese Veröffentlichung ist der letzte grundsätzliche Beitrag zum Thema unter dem Schlagwort Microsoft 365 auf der Seite der Dienststelle. Sie ist von 2022 — also aus einer Zeit vor dem Abschluss der EU Data Boundary und vor der Novelle des DSG-EKD. Sie ist damit weder aufgehoben noch fortgeschrieben. Das ist genau der Zustand, in dem du dich bewegst: kein Ja, kein Nein, sondern eine offene Beweislast.

Auf katholischer Seite gibt es Arbeitspapiere einzelner Datenschutzzentren zu datenschutzrechtlichen Aspekten von Microsoft 365, die in dieselbe Richtung argumentieren und

regelmäßig empfehlen, Lösungen unter eigener Hoheit zu prüfen und bei externen Auftragsverarbeitern Anbieter außerhalb des Europäischen Wirtschaftsraums sowie solche unter dem Zugriff des US-amerikanischen CLOUD Act zu meiden. Auch das sind Positionen, keine Verbotsverfügungen — aber es sind die Positionen der Stelle, die dich prüft.

WARNUNG · Die bekannte Orientierungshilfe stammt nicht von einer Aufsicht

In kirchlichen IT-Runden kursiert eine Orientierungshilfe mit dem Titel „Microsoft 365 in Kirche und Wohlfahrt“. Sie ist inhaltlich brauchbar und wird gern als Beleg herumgereicht. Sie stammt aber von einer Datenschutzberatung gemeinsam mit einem kirchennahen IT-Dienstleister, nicht von einer kirchlichen Datenschutzaufsicht. Wenn du sie im Aufsichtsgespräch als Nachweis anführst, wird dir das freundlich, aber deutlich erklärt werden. Nutze sie als Arbeitsmaterial. Zitiere sie nicht als Autorität.

Was sich 2025 und 2026 rechtlich bewegt hat

Zwei Änderungen sind für Microsoft-365-Projekte substanziell, und beide sind gute Nachrichten mit Fußnote.

Erstens, evangelisch: Die frühere Anforderung, Auftragsverarbeiter der kirchlichen Aufsicht zu unterwerfen, ist mit der Novelle entfallen. Das neue DSG-EKD sieht ausdrücklich vor, dass sich die Vertragsinhalte an Artikel 28 DSGVO orientieren dürfen, sofern die kirchlichen Datenschutzbestimmungen auf den Auftragsverarbeiter keine Anwendung finden. Damit ist das jahrelange Ärgernis vom Tisch, einem globalen Anbieter eine Unterwerfungsklausel abringen zu müssen, die er nie unterschreiben würde. Die Fußnote: Der Wegfall der Klausel ersetzt keine Prüfung. Die auftraggebende kirchliche Stelle muss sich weiterhin vor Beginn der Verarbeitung und danach regelmäßig von den technischen und organisatorischen Maßnahmen überzeugen — und das Ergebnis dokumentieren.

Zweitens, katholisch: Das Verarbeitungsverbot außerhalb des Europäischen Wirtschaftsraums, das früher in der Regelung zur Auftragsverarbeitung stand, ist ersatzlos weggefallen. Gleichzeitig regelt die neue Durchführungsverordnung Cloud-Dienste erstmals ausdrücklich, und zwar im Kapitel über besondere Gefahrenlagen. Sie verlangt, vorrangig bereits geprüfte und freigegebene Cloud-Dienste zu nutzen, andere Dienste anhand eines Katalogs von Risikoaspekten zu prüfen und — das ist der Satz, den du dir merken solltest — vor der Nutzung in Abhängigkeit von der Risikoanalyse eine Exit-Strategie zu definieren, etwa Datenlöschung oder Datenübertragung. Die Fußnote hier: Der Katalog der Risikoaspekte liest sich wie eine Beschreibung von Public-Cloud-Kollaboration. Mangelnde Portabilität, Abhängigkeit vom Anbieter mangels Wechselmöglichkeit, herstellerspezifische Datenformate, gemeinsame Nutzung der Infrastruktur durch mehrere Kunden, Unkenntnis über den Speicherort, hohe Mobilität der Informationen, unbefugter Zugriff durch Administrationspersonal des Anbieters. Das ist kein Verbot. Aber es ist eine Prüfliste, die du beantworten musst, und zwar schriftlich.

Skizze 2: Die Zeitleiste, die du im Aufsichtsgespräch im Kopf haben solltest. Rechtsgrundlagen und Anbieterentwicklungen laufen nicht synchron.

FAKTEN · Was auf Anbieterseite belegbar passiert ist

Microsoft hat die EU Data Boundary in drei Stufen aufgebaut: Kerndienste ab Januar 2023, pseudonymisierte personenbezogene Daten ab Januar 2024, und mit dem Abschluss im Februar 2025 auch die Daten aus technischem Support — also die vom Kunden übergebenen Protokolle und die von Microsoft erzeugten Fallnotizen — für Kunden in EU und EFTA innerhalb von EU und EFTA.

Prüfberichte nach ISO/IEC 27001, SOC 2 und dem Kriterienkatalog C5 des Bundesamts für Sicherheit in der Informationstechnik stehen Kunden über das Service Trust Portal zum Download bereit. Das ist relevant, weil die katholische Durchführungsverordnung ausdrücklich die Vorlage eines anerkannten Zertifikats, das sich an Veröffentlichungen des BSI orientiert, als Nachweis zulässt und als Alternative ISO/IEC 27001 nennt. Auf evangelischer Seite verweist die IT-Sicherheitsverordnung der EKD für den Sicherheitsstandard ebenfalls auf die Empfehlungen des BSI zur Informationssicherheit und zum IT-Grundschutz.

Achtung bei der Weitergabe: Die aus dem Service Trust Portal geladenen Prüfberichte sind als vertraulich gekennzeichnet und dürfen nicht frei weiterverteilt werden. Für die Vorlage bei der Aufsicht ist das in der Praxis handhabbar, für den Anhang eines öffentlichen Gremienprotokolls nicht.

Was das alles zusammen bedeutet: Die Argumentationslage ist heute deutlich besser als 2022, aber sie ist deine Argumentation, nicht die des Anbieters. Die Aufsicht fragt nicht, was Microsoft veröffentlicht hat. Sie fragt, was du daraus für deine Verarbeitung geschlossen hast und wo das steht. Wer den Unterschied verinnerlicht hat, hat den schwierigsten Teil des Gesprächs hinter sich.

Die Frage, ob ein kirchliches Rechenzentrum die bessere Antwort ist, wird an anderer Stelle ausführlich behandelt: Die Cloud-Frage in der Kirche: Kirchliche Rechenzentren, Microsoft 365 und die Ehrlichkeit über Datenstandorte. Kurzfassung: Die Antwort hängt davon ab, welche Daten du meinst — und für einen erheblichen Teil der kirchlichen Bürowelt lautet sie anders als für die Beratungsakte.

Die sechs Nachweise

Wenn die Aufsicht schreibt, fragt sie nicht nach deinem Tenant. Sie fragt nach Unterlagen. Sechs davon kommen praktisch immer vor. Sie sind unabhängig von der Konfession weitgehend identisch, unterscheiden sich aber in Details, die im Gespräch auffallen.

Skizze 3: Die sechs Nachweise und ihre Herkunft. Drei entstehen am Schreibtisch, drei im Tenant — sofern jemand sie eingeschaltet hat.

Verzeichnis der Verarbeitungstätigkeiten

Beide Gesetze verlangen ein Verzeichnis aller Verarbeitungstätigkeiten mit im Kern denselben Angaben: Verantwortlicher und gegebenenfalls gemeinsam Verantwortliche, Datenschutzbeauftragte, Zwecke, Kategorien betroffener Personen und Daten, gegebenenfalls Profiling, Empfängerkategorien einschließlich Empfängern in Drittländern, Drittlandübermittlungen mit Dokumentation der Garantien, nach Möglichkeit Löschfristen und eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen. Das Verzeichnis ist der Aufsicht auf Anfrage zur Verfügung zu stellen.

Der praktisch wichtigste Unterschied liegt in der Schwelle. Evangelisch gilt die Pflicht nicht für Stellen mit weniger als 250 Beschäftigten; unterhalb dieser Grenze sind Verzeichnisse nur für Verfahren zu führen, die besondere Kategorien personenbezogener Daten einschließen. Katholisch gilt die Pflicht ab 250 Beschäftigten und darüber hinaus für kleinere Einheiten, wenn die Verarbeitung Rechte und Freiheiten gefährdet, nicht nur gelegentlich erfolgt oder besondere Kategorien beziehungsweise Daten über Straftaten umfasst. Das Merkmal „nicht nur gelegentlich“ trifft auf einen produktiven Microsoft-365-Tenant immer zu. Für eine katholische Kirchengemeinde mit acht Beschäftigten heißt das im Ergebnis: Verzeichnis ja.

WICHTIG · Zwei Jahre sind katholisch eine Frist, nicht ein Gefühl

Die katholische Durchführungsverordnung schreibt vor, dass das Verzeichnis bei jeder Veränderung eines Verfahrens zu aktualisieren und im Übrigen in Abständen von höchstens zwei Jahren zu überprüfen ist — und dass Überprüfung wie Aktualisierung zu dokumentieren sind. Dieselbe Zweijahresfrist gilt für die Überprüfung der Wirksamkeit der technischen und organisatorischen

Maßnahmen, ebenfalls mit Dokumentationspflicht.

Wenn deine Aufsicht ein Muster für das Verzeichnis bereitstellt, bildet dieses grundsätzlich den Mindeststandard. Das ist keine Empfehlung, das steht so in der Verordnung. Nimm das Muster deiner Aufsicht, nicht das aus dem Internet.

Datenschutz-Folgenabschätzung

Hier wird es konkret, und hier scheitern die meisten Projekte im Nachhinein. Beide Aufsichten haben 2018 Listen von Verarbeitungsvorgängen veröffentlicht, für die zwingend eine Folgenabschätzung durchzuführen ist. Und beide Listen enthalten eine Position, die auf einen Microsoft-365-Tenant mit sensiblen Daten unmittelbar passt: die Verarbeitung besonderer Kategorien personenbezogener Daten durch Auftragsverarbeiter, denen von einem Gericht oder einer Verwaltungsbehörde eines Drittlands die Pflicht auferlegt werden kann, diese Daten entgegen Artikel 48 DSGVO zu exportieren oder offenzulegen. Als typisches Einsatzfeld nennen beide Listen ausdrücklich Dienstleister mit Sitz außerhalb der EU, als Beispiel die Verarbeitung in einer öffentlichen Cloud.

Übersetzt: Wer Gesundheitsdaten, Sozialdaten, Daten über religiöse Überzeugung, Daten über Straftaten oder vergleichbar geschützte Daten in einem Public-Cloud-Dienst eines Anbieters verarbeitet, der dem Zugriff eines Drittstaats unterliegen kann, steht auf der Muss-Liste. Nicht vielleicht. Auf der Liste.

Weitere Positionen treffen typische Microsoft-365-Vorhaben ebenfalls. Die umfangreiche Verarbeitung von Daten, die dem Sozial-, einem Berufs- oder einem besonderen Amtsgeheimnis unterliegen, mit Krankenhäusern und großen diakonischen Einrichtungen als Einsatzfeld. Die Verarbeitung umfangreicher Angaben über das Verhalten von Beschäftigten, die zur Bewertung ihrer Tätigkeit eingesetzt werden können, mit Data-Loss-Prevention-Systemen, die systematische Profile erzeugen, als ausdrücklich genanntem Einsatzfeld — das ist eine Warnung an jeden, der Purview-DLP oder Insider-Risk-Funktionen scharf schalten will. Die Verarbeitung von Daten der Personenstands- und Melderegister, evangelisch mit dem kirchlichen Meldewesen als Einsatzfeld. Und, für alle, die ein modernes Intranet planen: Der BfD EKD nennt in seiner Liste als Beispiel für die Erstellung umfassender Profile über Interessen, Beziehungsnetze oder Persönlichkeit ausdrücklich den Betrieb eines landeskirchenweiten Intranets.

WARNUNG · Nicht auf der Liste heißt nicht: keine Folgenabschätzung nötig

Beide Aufsichten schreiben in ihre Listen denselben Hinweis: Steht eine Verarbeitung nicht auf der Liste, folgt daraus nicht, dass keine Folgenabschätzung durchzuführen wäre. Der Verantwortliche muss dann selbst einschätzen, ob voraussichtlich ein hohes Risiko besteht — und diese Einschätzung dokumentieren. Die Nicht-Durchführung braucht also ebenfalls ein Blatt Papier.

Und die Konsequenz steht dort ebenso deutlich: Führt ein Verantwortlicher eine Verarbeitung aus, die im Gesetz oder auf der Liste genannt ist, ohne vorab eine Folgenabschätzung durchgeführt zu haben, kann die Aufsicht von ihren Abhilfebefugnissen einschließlich Geldbußen Gebrauch machen.

Ergibt die Folgenabschätzung, dass trotz aller Maßnahmen ein hohes Risiko bleibt, ist die Aufsicht vor der Verarbeitung zu konsultieren. Beide Rechtskreise kennen diese vorherige Konsultation. Das ist kein Makel, sondern der vorgesehene Weg. Ein Träger, der von sich aus konsultiert, verhandelt

aus einer völlig anderen Position als einer, dem die Konsultation nach einer Beschwerde nahegelegt wird.

Wie eine Folgenabschätzung für Microsoft 365 im kirchlichen Kontext methodisch aufgebaut wird, welche Muster taugen und welche Befunde regelmäßig herauskommen, steht in Datenschutz-Folgenabschätzung für Microsoft 365 nach DSG-EKD und KDG: Vorgehen, Muster und typische Befunde.

Auftragsverarbeitungsverträge — Plural, ausdrücklich

Die häufigste Fehlvorstellung: „Wir haben den Microsoft-Vertrag, also haben wir den Auftragsverarbeitungsvertrag." In einem realistischen kirchlichen Setup gibt es mindestens drei Vertragsbeziehungen, in denen personenbezogene Daten im Auftrag verarbeitet werden: Microsoft als Betreiber der Dienste, das Systemhaus mit administrativem Zugriff auf deinen Tenant, und häufig ein kirchliches Rechenzentrum oder ein Verband, der Teile des Betriebs übernimmt. Dazu kommen Fachverfahren, die per Schnittstelle andocken.

Evangelisch ist der Auftrag in Textform zu erteilen, und das Gesetz zählt zehn Punkte auf, die im Einzelnen festzulegen sind — von Gegenstand und Dauer über die technischen und organisatorischen Maßnahmen und deren Kontrolle, Unterauftragsverhältnisse, Kontrollrechte und Duldungspflichten bis zur Rückgabe von Datenträgern und Löschung nach Auftragsende. Katholisch bedarf der Vertrag der Schriftform, wobei sich die Ersetzung durch elektronische Form oder Textform nach den geltenden staatlichen Regelungen richtet.

WICHTIG · Der Satz, der katholisch oft übersehen wird

Die katholische Durchführungsverordnung sieht vor, dass mit Auftragsverarbeitern, die nicht den Regelungen des KDG unterfallen, grundsätzlich neben der Anwendung der DSGVO die Anwendung des KDG zu vereinbaren ist. Das ist in Verhandlungen mit einem globalen Anbieter kein Selbstläufer und in Verhandlungen mit dem regionalen Systemhaus sehr wohl durchsetzbar. Wer die Klausel im Systemhausvertrag nicht hat, sollte eine Begründung parat haben, warum nicht.

Ebenfalls dort: Fernwartung darf nur erfolgen, wenn der Beginn aktiv vom Auftraggeber eingeleitet wurde, über sichere Verbindungen läuft und systemseitig protokolliert wird. Übertragen auf delegierte Administrationsrechte eines Partners heißt das: zeitlich begrenzt, vom Kunden ausgelöst, nachvollziehbar protokolliert. Ein dauerhaft aktiver Partnerzugang mit Vollrechten hält dieser Regelung nicht stand.

Die vertragliche Kette im Detail — Microsoft, Systemhaus, Rechenzentrum, Unterauftragnehmer — behandelt Auftragsverarbeitung nach DSG-EKD und KDG: Microsoft, Systemhaus und Rechenzentrum vertraglich richtig einbinden.

Berechtigungskonzept

Ein Berechtigungskonzept ist kein Screenshot der Gruppenliste. Es ist die schriftliche Antwort auf die Frage, wer aus welchem Grund auf welche Daten zugreifen darf und wie das überprüft wird. Die katholische Durchführungsverordnung wird hier ungewöhnlich konkret: Berechtigte dürfen ausschließlich auf die ihrer Zuständigkeit unterliegenden Daten zugreifen; im Netzwerk- und Einzelplatzbetrieb ist eine abgestufte Rechteverwaltung erforderlich; Anwender- und

Administrationsrechte sind zu trennen. Der letzte Halbsatz ist die kirchenrechtliche Fassung dessen, was in Entra ID separate Administratorkonten und Privileged Identity Management heißt.

Hinzu kommt die Einordnung in Datenschutzklassen, die es auf katholischer Seite gibt und auf evangelischer nicht. Daten, deren missbräuchliche Verarbeitung die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse erheblich beeinträchtigen kann, fallen in die höchste Klasse — dazu gehören ausdrücklich auch Daten über arbeitsrechtliche Rechtsverhältnisse und Disziplinarentscheidungen sowie Namens- und Adressangaben mit Sperrvermerken. Und: Erfolgt keine Einordnung, gilt automatisch die höchste Klasse. Wer die Einordnung schuldig bleibt, hat sich damit selbst das strengste Schutzniveau auferlegt.

Wie ein Regelwerk aus Rollen, Gruppen, bedingtem Zugriff und Mehrfaktor-Authentifizierung für Pfarrbüro, Pflegedienst, Verwaltung und Ehrenamt aussieht, steht in Conditional Access und MFA in Kirche und Diakonie: Ein Regelwerk für Pfarrbüro, Pflegedienst, Verwaltung und Ehrenamt. Die Identitätsseite dazu behandelt Entra ID für kirchliche Träger: Identitäten zwischen Landeskirche, Verband, Träger und Einrichtung.

Löschkonzept

Beide Verzeichnispflichten verlangen, nach Möglichkeit die vorgesehenen Löschfristen der verschiedenen Datenkategorien anzugeben. Genau daran scheitert die Vorlage regelmäßig: Das Verzeichnis ist gepflegt, die Spalte „Löschfrist“ steht auf „wird noch geklärt“. Damit hast du der Aufsicht schriftlich mitgeteilt, dass du kein Löschkonzept hast.

Die Fristen selbst kommen nicht aus Microsoft 365, sondern aus kirchlichem Recht, aus Kassationsordnungen, aus Archivgesetzen der Landeskirchen und Bistümer, aus dem Sozial- und Steuerrecht. Microsoft 365 ist das Werkzeug, das sie durchsetzt — über Aufbewahrungsrichtlinien, Aufbewahrungsbezeichnungen und Datensatzverwaltung in Purview. Die Aufsicht interessiert sich für beides: Wo steht die Frist, und wodurch wird sie technisch wirksam?

Zur Abbildung kirchlicher Aufbewahrungsfristen und Kassationsordnungen in Purview: Kirchliche Aufbewahrungsfristen, Kassationsordnungen und Archivgesetze in Microsoft Purview abbilden. Zur Klassifizierung, die dem Löschkonzept vorausgeht: Sensitivity Labels für kirchliche Träger: Ein Label-Konzept vom Gemeindebrief bis zur Beratungsakte.

Protokollierung

Hier gibt es eine Zahl, die du kennen solltest, weil sie kirchenrechtlich verbindlich ist und sich direkt mit einer Produkteinstellung vergleichen lässt. Die katholische Durchführungsverordnung verlangt im Rahmen der Eingabekontrolle, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in IT-Systemen verarbeitet worden sind — und dass die Eingabekontrolle unbeschadet gesetzlicher Aufbewahrungsfristen mindestens einen Zeitraum von sechs Monaten umfasst.

Sechs Monate sind 180 Tage. Genau so lange bewahrt Microsoft Purview Audit in der Standardvariante Datensätze auf, die seit Oktober 2023 erzeugt wurden — vorher waren es 90 Tage. Mit Audit Premium liegt die Aufbewahrung für Exchange Online, SharePoint, OneDrive und Entra ID bei einem Jahr, für die übrigen Aktivitäten weiterhin bei 180 Tagen; über eigene Aufbewahrungsrichtlinien und eine Zusatzlizenz sind bis zu zehn Jahre möglich. Das heißt: Der Standard erfüllt die Sechsmonatsanforderung ziemlich exakt und ohne Puffer. Wer eine gesetzliche

Aufbewahrungsfrist hat, die länger läuft, braucht eine bewusste Entscheidung — und die gehört ins Konzept, nicht in eine Fußnote.

TIPP · Protokolle sind nicht rückwirkend beschaffbar

Der ärgerlichste Satz in einem Aufsichtsverfahren nach einer Datenpanne lautet: „Der Zeitraum liegt außerhalb unserer Aufbewahrung." Prüfe vor dem Rollout, welche Aktivitäten überhaupt protokolliert werden, wie lange sie liegen und wer im Ernstfall suchen darf. Und prüfe, ob die Berechtigung, im Überwachungsprotokoll zu suchen, ihrerseits sauber eingeschränkt und dokumentiert ist — sonst hast du ein zweites Problem geschaffen, während du das erste lösen wolltest.

Bei Copilot gilt eine Besonderheit: Das Überwachungsprotokoll hält fest, dass eine Interaktion stattgefunden hat, nicht den Wortlaut. Eingaben und Antworten liegen im Postfach der Nutzenden und sind über eDiscovery zu finden. Wer im Konzept schreibt, Copilot-Nutzung sei „vollständig protokolliert", sollte wissen, was er damit meint.

Zur Mitbestimmung bei Protokollierung, Auswertungen und Copilot: Mitarbeitervertretung und Microsoft 365: MVG-EKD, MAVO, Dienstvereinbarung und Mitbestimmung bei Teams, Copilot und Protokollierung. Zur Copilot-Einführung selbst: Copilot in Kirche und Diakonie: Nutzen, Grenzen, Oversharing und die Copilot-Überprüfung vor dem Rollout.

Die Übersicht: Nachweis, Herkunft, Zuständigkeit

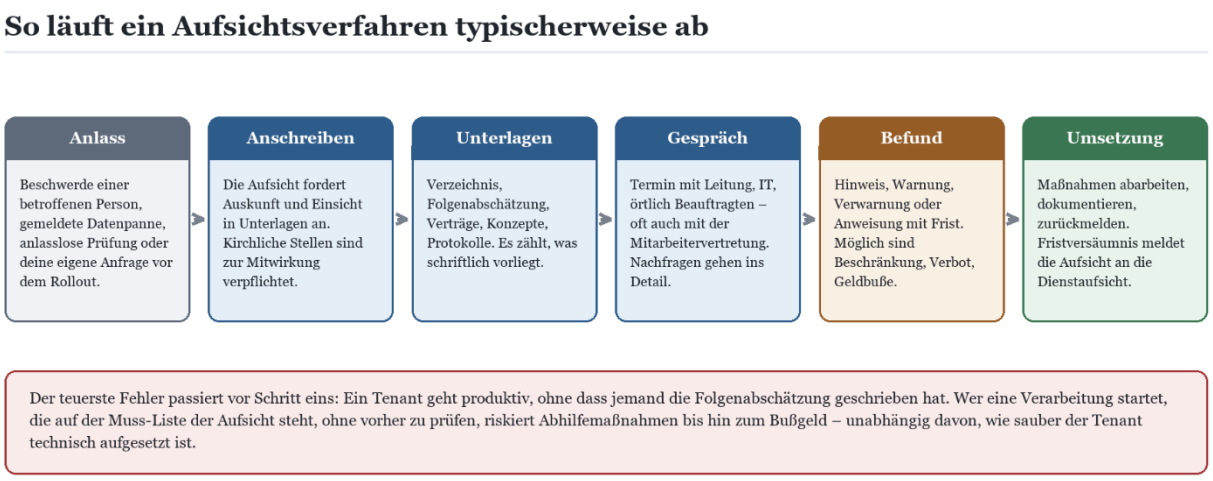
Nachweis	Wo in Microsoft 365 erzeugt	Wer liefert
Verzeichnis der Verarbeitungs-tätigkeiten	Nicht im Tenant. Zuarbeit: Liste der aktiven Dienste, Speicherorte, Datenklassifizierung aus Purview, Berichte zur Gastnutzung aus Entra ID.	Fachbereiche und Verwaltungsleitung schreiben; örtlich Beauftragte prüfen; IT liefert die technischen Angaben zu.
Datenschutz-Folgenabschätzung	Nicht im Tenant. Belege stammen aus Tenant-Konfiguration, aus dem Service Trust Portal und aus dem Vertragswerk.	Verantwortliche Stelle, also die Leitung. Örtlich Beauftragte werden angehört, entscheiden aber nicht.
Auftragsverarbeitungs-verträge	Nicht im Tenant. Die Liste der Unterauftragsverarbeiter und die Datenschutz-bestimmungen veröffentlicht der Anbieter.	Verwaltungsleitung und Justiziariat mit Microsoft, Systemhaus, Rechenzentrum und jedem Fachverfahren.
Berechtigungskonzept	Entra ID: Rollenzuweisungen, Gruppen, Zugriffsüberprüfungen, Privileged Identity Management, Conditional Access. Dazu SharePoint- und Teams-Berechtigungen, Freigabeeinstellungen, Gastrichtlinien.	IT-Leitung schreibt und pflegt; Fachbereiche liefern die Zuständigkeiten; Leitung genehmigt.
Löschkonzept	Purview Data Lifecycle Management: Aufbewahrungsrichtlinien und -bezeichnungen, Datensatzverwaltung, Löschung von Postfächern und Websites.	Registratur, Archiv und Fachbereiche liefern die Fristen aus Kirchenrecht und Kassationsordnung; IT setzt um.
Protokollierung	Purview Audit: einheitliches Überwachungsprotokoll. Standard 180 Tage, Premium ein Jahr für die großen Dienste, bis zu zehn Jahre mit Zusatzlizenz. Anmeldeprotokolle in Entra	IT-Leitung konfiguriert und dokumentiert; die Mitarbeitervertretung ist bei Auswertungsmöglichkeiten zu beteiligen.

	ID.	
Technische und organisatorische Maßnahmen, Überprüfung	Prüfberichte nach ISO/IEC 27001, SOC 2 und C5 über das Service Trust Portal; Tenant-seitige Konfigurationsnachweise; Compliance Manager als Arbeitsmittel.	IT-Leitung und Informationssicherheitsbeauftragte. Katholisch ist die Wirksamkeitsprüfung mindestens alle zwei Jahre zu dokumentieren.
Exit-Strategie	Nicht im Tenant, aber technisch zu unterlegen: Exportwege, Datenformate, Aufwandsschätzung für Rückführung oder Löschung.	IT-Leitung und Verwaltungsleitung. Katholisch seit der Novelle ausdrücklich vor Nutzung des Cloud-Dienstes zu definieren.

Tabelle 1: Die Nachweise, ihre Herkunft und die verantwortlichen Rollen. Auffällig ist die Verteilung: Die IT liefert Bausteine, die Verantwortung liegt bei der Leitung.

Das Gespräch selbst

Ein Aufsichtsgespräch ist kein Verhör und keine Prüfung im Schulsinn. Es ist ein Fachgespräch zwischen Menschen, die dasselbe Recht anwenden, aber unterschiedliche Rollen haben. Die Aufsicht will verstehen, ob deine Verarbeitung beherrscht ist. Du willst zeigen, dass sie es ist. Wenn beide Seiten das ernst nehmen, ist der Termin produktiv. Wenn eine Seite improvisiert, wird er lang.



Skizze 4: Der typische Verfahrensablauf. Der Anlass entscheidet über den Ton, nicht über die Anforderungen.

Vor dem Termin

Die Unterlagen sind wichtiger als die Präsentation. Stelle einen vollständigen Satz zusammen und schicke ihn vorab, wenn die Aufsicht darum bittet — das verkürzt den Termin erheblich, weil die Rückfragen dann konkret sind statt explorativ. Und kläre intern die Rollenverteilung: Wer antwortet auf Rechtsfragen, wer auf technische Fragen, wer auf Fragen zur Organisation? Nichts wirkt unvorbereiteter als drei Personen, die einander im Kreis ansehen.

- Verzeichnis der Verarbeitungstätigkeiten, aktuell und mit Datum der letzten Überprüfung.
- Datenschutz-Folgenabschätzung mit dokumentierter Anhörung der örtlich Beauftragten beziehungsweise der betrieblichen Datenschutzbeauftragten.
- Vertragsmappe: Microsoft, Systemhaus, Rechenzentrum, Fachverfahren, jeweils mit Unterauftragsverarbeitern.

- Berechtigungskonzept einschließlich der Regelung für administrative Konten und für den Zugriff des Dienstleisters.
- Löschkonzept mit Herleitung der Fristen und Nachweis der technischen Umsetzung.
- Protokollierungskonzept: was protokolliert wird, wie lange, wer auswerten darf, unter welchen Voraussetzungen.
- IT-Sicherheitskonzept. Evangelisch ist es nach der IT-Sicherheitsverordnung der EKD verpflichtend zu erstellen und fortzuschreiben; der Sicherheitsstandard orientiert sich an den Empfehlungen des BSI.
- Dienstvereinbarung mit der Mitarbeitervertretung, soweit vorhanden — und wenn nicht vorhanden, eine Erklärung dazu.
- Nachweise über Verpflichtung auf das Datengeheimnis und über Schulungen, einschließlich der ehrenamtlich Tätigen.

AUS DER PRAXIS · Vorbereitung eines Aufsichtsgesprächs bei einem diakonischen Werk

Ein diakonisches Werk in einer Großstadt — Beratungsstellen, ambulante Pflege, mehrere Kitas, rund 600 Beschäftigte — bekam nach einer Beschwerde aus dem Beratungsbereich Post von der Aufsicht. Anlass war ein Verdacht auf zu weite Zugriffsrechte auf einer SharePoint-Website. Angefordert wurden Verzeichnis, Folgenabschätzung, Auftragsverarbeitungsverträge und Berechtigungskonzept, mit Frist von vier Wochen.

Der Befund der internen Sichtung war typisch. Das Verzeichnis existierte, war aber zwei Jahre alt und kannte weder Teams noch OneDrive. Eine Folgenabschätzung lag für das Klientenverwaltungssystem vor, nicht für Microsoft 365. Der Microsoft-Vertrag war vorhanden, der Vertrag mit dem Systemhaus regelte Datenschutz in einem Satz. Ein Berechtigungskonzept gab es als Entwurf von der Einführung, ohne Beschluss, ohne Datum. Die Protokollierung lief in der Standardkonfiguration, was in diesem Fall ein Glücksfall war: Der fragliche Zeitraum lag noch innerhalb der Aufbewahrung.

Was in vier Wochen tatsächlich zu schaffen war: Das Verzeichnis wurde für die Microsoft-365-Dienste vollständig neu geschrieben, gegliedert nach Arbeitsbereichen statt nach Technik. Die Folgenabschätzung wurde begonnen, nicht abgeschlossen — dafür aber mit belastbarem Projektplan, benannten Beteiligten und Terminen. Der Systemhausvertrag wurde um eine ordentliche Auftragsverarbeitungsvereinbarung ergänzt, samt Regelung zu befristeten administrativen Zugängen. Das Berechtigungskonzept wurde in der Geschäftsführung beschlossen und datiert, mit dem ehrlichen Vermerk, dass die Bereinigung der Altbestände sechs Monate dauern wird.

Im Termin selbst war genau dieser letzte Punkt der wichtigste. Die Aufsicht bemängelte die Lücken — und akzeptierte den Plan, weil er datiert, verantwortet und realistisch war. Das Verfahren endete mit einer Maßnahmenliste und einer Frist von sechs Monaten. Der entscheidende Satz der Geschäftsführung im Termin lautete sinngemäß: Wir sind nicht fertig, wir wissen aber genau, was fehlt, und hier steht, wann es da ist. Das ist keine Verhandlungstaktik. Das ist die einzige Position, die trägt.

Im Termin

Die Fragen sind vorhersehbar. Sie zielen fast nie auf Produktdetails und fast immer auf Verantwortung, Nachvollziehbarkeit und Grenzen.

Typische Frage der Aufsicht	Was eine tragfähige Antwort enthält

Wer ist bei Ihnen verantwortliche Stelle für den Tenant?	Eine Rechtsperson, nicht eine Abteilung. Bei geteilten Tenants zwischen Landeskirche oder Bistum und Trägern: die Vereinbarung über die Verteilung der Aufgaben. Evangelisch kennt das Gesetz dafür ausdrücklich zentrale Verfahren, für die die Verteilung der Aufgaben, Befugnisse und Verantwortlichkeiten geregelt werden kann.
Welche Daten liegen in diesem Tenant, und welche ausdrücklich nicht?	Eine Positiv- und eine Negativliste. Insbesondere die Aussage, wie Seelsorgeunterlagen, Beratungsakten und Gemeindegliederdaten behandelt werden — und wodurch die Abgrenzung technisch wirksam wird, nicht nur organisatorisch gewollt ist.
Wo werden die Daten gespeichert und verarbeitet?	Die Regionsangabe des Tenants, die Aussage zur EU Data Boundary einschließlich der Supportdaten, und die ehrliche Benennung der Dienste, die davon abweichen. Wer „alles in Deutschland“ sagt, ohne es prüfen zu können, verliert an dieser Stelle die Glaubwürdigkeit für den Rest des Termins.
Wer kann als Administrator auf Inhalte zugreifen?	Anzahl und Namen der privilegierten Konten, Trennung von Anwender- und Administrationsrechten, zeitlich begrenzte Rechteaktivierung, Protokollierung administrativer Zugriffe — und dieselbe Auskunft für den Dienstleister.
Wie lange bewahren Sie Protokolle auf, und wer darf sie auswerten?	Die konkrete Aufbewahrungsdauer, die Rechtsgrundlage für die Auswertung, das Verfahren bei Verdachtsfällen und die Beteiligung der Mitarbeitervertretung.
Welche Löschfristen gelten, und wie werden sie durchgesetzt?	Fristen mit Herkunft aus Kirchenrecht, Kassationsordnung oder staatlichem Recht, und die konkrete technische Umsetzung. „Manuell durch die Sachbearbeitung“ ist eine zulässige Antwort, wenn sie dokumentiert und geprüft wird.
Was passiert, wenn Sie den Dienst verlassen wollen oder müssen?	Die Exit-Strategie. Katholisch ist sie seit der Novelle vor der Nutzung zu definieren; evangelisch folgt sie aus der Pflicht, Rückgabe und Löschung nach Auftragsende zu regeln. Konkret: Exportformate, Aufwand, Zuständigkeit, geprüft oder nur geplant.
Wie melden Sie eine Datenpanne, und haben Sie das geübt?	Der Meldeweg mit Namen und Erreichbarkeit, die interne Eskalation aus Kita, Pflegedienst oder Pfarramt heraus, und ehrlicherweise: ob es je einen Probelauf gab.

Tabelle 2: Die Fragen, die in Aufsichtsgesprächen regelmäßig fallen — und woran eine belastbare Antwort erkennbar ist.

WARNUNG · „Der Systemhaus-Partner hat gesagt, das ist alles konform“

Dieser Satz ist im Aufsichtsgespräch wertlos, und zwar aus einem strukturellen Grund: Der Auftragsverarbeiter ist nicht der Verantwortliche. Die Verantwortung für die Einhaltung der kirchlichen Datenschutzbestimmungen liegt bei der auftraggebenden kirchlichen Stelle — das steht in beiden Gesetzen, und daran ändert kein Beratungsprotokoll etwas.

Hinzu kommt die Prüfpflicht. Evangelisch muss sich die auftraggebende Stelle vor Beginn der Datenverarbeitung und danach regelmäßig von den beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugen und das Ergebnis dokumentieren. Katholisch muss sich der Verantwortliche bei Auftragsverarbeitung in geeigneter Weise, insbesondere durch persönliche Überprüfung oder Vorlage von Nachweisen, vom Bestehen des erforderlichen Schutzniveaus überzeugen. Beides sind Handlungen, die du vorweisen musst — nicht Zusicherungen, die du entgegennimmst.

Praktisch heißt das: Eine E-Mail des Partners mit dem Inhalt „ist DSGVO-konform“ ist kein Nachweis. Ein Prüfbericht nach C5 oder ISO/IEC 27001, ein dokumentierter Konfigurationsstand,

ein Protokoll einer Überprüfung mit Datum und Ergebnis — das sind Nachweise. Und noch ein Detail, das im Termin regelmäßig unangenehm wird: Ein Auftragsverarbeiter, der unter Verstoß gegen das Gesetz Zwecke und Mittel der Verarbeitung selbst bestimmt, gilt katholisch in Bezug auf diese Verarbeitung als Verantwortlicher. Wer seinem Systemhaus die Tenant-Konfiguration ohne Weisung und ohne Dokumentation überlässt, verschiebt damit möglicherweise Verantwortlichkeiten, die niemand verschieben wollte.

Nach dem Termin

Rechne mit einem Protokoll und einer Maßnahmenliste mit Fristen. Beides gehört unverzüglich in ein Gremium — Presbyterium, Kirchenvorstand, Kirchenverwaltung, Verbandsausschuss oder Aufsichtsrat, je nach Struktur. Nicht wegen der Formalität, sondern weil Maßnahmen mit Fristen Geld und Personal brauchen und beides an dieser Stelle beschlossen wird.

Und melde zurück. Die häufigste vermeidbare Eskalation entsteht nicht durch schlechte Umsetzung, sondern durch Schweigen. Wer eine Frist nicht halten kann, sollte das vor Ablauf der Frist mit Begründung und neuem Termin mitteilen. Die Alternative ist, dass die Aufsicht die vorgesetzte kirchliche Stelle einschaltet — und dann sitzt beim nächsten Termin jemand aus dem Landeskirchenamt oder dem Generalvikariat mit am Tisch, der bis dahin von nichts wusste.

Wo Kirche wirklich anders ist — und wo nicht

Ein großer Teil eines Microsoft-365-Projekts bei einem kirchlichen Träger ist völlig normales Microsoft 365. Die Identitätsverwaltung ist dieselbe, die Migration ist dieselbe, der bedingte Zugriff ist derselbe, die Schulungsfragen sind dieselben. Es hilft niemandem, künstliche Sonderwege zu bauen, wo keine nötig sind. Es gibt aber vier Bereiche, in denen die Unterschiede echt und nicht verhandelbar sind.

Bereich	Kommune oder Unternehmen	Kirchlicher Träger
Rechtsordnung	DSGVO und Bundes- oder Landesdatenschutzgesetz.	DSG-EKD beziehungsweise KDG mit Durchführungsverordnung. Eigene Begriffe, eigene Fristen, eigene Schwellenwerte.
Aufsicht und Rechtsweg	Landesbeauftragte für den Datenschutz, Rechtsweg zu den Verwaltungsgerichten.	BfD EKD beziehungsweise Diözesandatenschutzbeauftragte. Evangelisch führt der Rechtsweg zu den kirchlichen Verwaltungsgerichten, katholisch über das Interdiözesane Datenschutzgericht zum Datenschutzgericht der Deutschen Bischofskonferenz.
Beteiligung der Beschäftigten	Personalrat oder Betriebsrat, Betriebs- oder Dienstvereinbarung.	Mitarbeitervertretung nach MVG-EKD oder MAVO, Dienstvereinbarung im Rahmen des Dritten Weges und der Dienstgemeinschaft. Andere Gremien, andere Verfahren, vergleichbare Wirkung.
Besonders geschützte Inhalte	Sozialdaten, Berufsgeheimnisse, Personalakten.	Zusätzlich Seelsorge- und Beichtgeheimnis. Evangelisch dürfen Aufzeichnungen aus der Wahrnehmung eines Seelsorgeauftrags Dritten nicht zugänglich sein. Katholisch dürfen Daten, die dem Beichtgeheimnis unterliegen, überhaupt nicht

		verarbeitet werden; Daten unter dem Seelsorgegeheimnis nur mit Maßnahmen, die erforderlichenfalls über das höchste Schutzniveau hinausgehen.
Ehrenamt	Spielt in der IT selten eine Rolle.	Ehrenamtlich Tätige sind katholisch ausdrücklich in die Verpflichtung auf das Datengeheimnis und in die Schulungspflicht einbezogen. Presbyterium, Kirchenvorstand und Pfarrgemeinderat arbeiten mit personenbezogenen Daten.

Tabelle 3: Die Unterschiede, die wirklich bestehen. Alles andere ist normales Microsoft 365 und sollte auch so behandelt werden.

WICHTIG · Der Satz zum Beichtgeheimnis ist wörtlich zu nehmen

Die katholische Durchführungsverordnung formuliert unmissverständlich: Personenbezogene Daten, die dem Beichtgeheimnis unterliegen, dürfen nicht verarbeitet werden. Nicht „nur verschlüsselt“, nicht „nur mit besonderen Maßnahmen“ — nicht.

Für Daten unter dem Seelsorgegeheimnis nennt dieselbe Verordnung als mögliche Maßnahme ausdrücklich einen eigenen Server oder eine eigene Datenablage in einem Netzwerk ohne externe Datenverbindung. Wer also in einer Konzeption schreibt, seelsorgliche Gesprächsnotizen lägen „geschützt in einem eigenen Teams-Kanal“, sollte sich auf eine sehr direkte Rückfrage einstellen.

Der Umgang mit Seelsorgeunterlagen in Teams, OneNote und Copilot ist eigens behandelt in Seelsorgegeheimnis und Beichtgeheimnis in Microsoft 365: Was nie in Teams, OneNote oder Copilot landen darf. Für Klientendaten in Diakonie und Caritas: Klientendaten in Diakonie und Caritas: Sozialdaten, Schweigepflicht und Schutz mit Microsoft Purview. Zur Trennung von Meldewesen und Gemeindegliederdaten: Meldewesen und Gemeindegliederdaten: Warum Kirchenmitgliederdaten getrennt von Microsoft 365 bleiben.

Häufige Fragen

Muss ich die Aufsicht vor der Einführung von Microsoft 365 fragen?

Fragen musst du nicht. Konsultieren musst du dann, wenn deine Datenschutz-Folgenabschätzung ergibt, dass die Verarbeitung trotz der geplanten Maßnahmen ein hohes Risiko zur Folge hat. Beide Rechtskreise kennen diese vorherige Konsultation. Unabhängig davon ist die freiwillige frühe Ansprache in der Praxis fast immer die günstigere Variante: Sie kostet ein paar Wochen und erspart im Zweifel eine Maßnahmenliste mit Frist.

Brauchen wir überhaupt einen Datenschutzbeauftragten?

Die Schwelle liegt in beiden Rechtskreisen inzwischen bei zwanzig Personen, die sich in der Regel ständig mit der Verarbeitung personenbezogener Daten beschäftigen — früher waren es zehn. Unabhängig von der Zahl greift die Pflicht, wenn die Kerntätigkeit in umfangreicher Verarbeitung besonderer Kategorien personenbezogener Daten oder in umfangreicher regelmäßiger und systematischer Überwachung besteht. Für ein Krankenhaus, einen Pflegedienst oder eine Beratungsstelle ist die Zahl also gar nicht die entscheidende Größe. Neu ist katholisch, dass auch eine juristische Person benannt werden kann; die Benennung ist der Aufsicht anzuzeigen und die Kontaktdaten sind zu veröffentlichen.

Wie schnell muss eine Datenpanne gemeldet werden?

Hier unterscheiden sich die Rechtskreise im Wortlaut, und das ist einer der wenigen Punkte, an denen die Unterscheidung praktisch zählt. Katholisch ist unverzüglich zu melden; erfolgt die Meldung nicht binnen 72 Stunden nach Bekanntwerden, ist ihr eine Begründung für die Verzögerung beizufügen. Evangelisch ist ebenfalls unverzüglich zu melden, wenn die Verletzung voraussichtlich zu einem nicht unerheblichen Risiko für die Rechte natürlicher Personen führt — eine feste Stundenzahl nennt das Gesetz an dieser Stelle nicht. Verlass dich trotzdem nicht auf die Auslegung von „unverzüglich“: Beide Aufsichten erwarten Tempo, und beide verlangen eine Dokumentation aller Verletzungen, auch der nicht gemeldeten.

Ablauf, Meldeformulare und ein Vorschlag für eine Übung stehen in Datenpannen bei kirchlichen Trägern: Meldung an BfD EKD oder Diözesandatenschutzbeauftragten, Fristen, Ablauf und Übung.

Reicht der Microsoft-Vertrag als Auftragsverarbeitungsvertrag?

Für die Beziehung zu Microsoft ist das Vertragswerk des Anbieters der übliche und in der Regel akzeptierte Weg — evangelisch ausdrücklich gestützt darauf, dass sich die Vertragsinhalte an Artikel 28 DSGVO orientieren dürfen, wenn kirchliches Datenschutzrecht auf den Auftragsverarbeiter keine Anwendung findet. Für alle anderen Beteiligten reicht er nicht: Das Systemhaus mit administrativem Zugriff, das Rechenzentrum und jedes Fachverfahren brauchen eigene Vereinbarungen. Und in keinem Fall ersetzt der Vertrag die eigene Prüfung der technischen und organisatorischen Maßnahmen.

Können wir einen gemeinsamen Tenant für Landeskirche und Kirchenkreise nutzen?

Technisch ja, rechtlich mit Aufwand. Entscheidend ist die saubere Zuordnung der Verantwortlichkeit: Wer ist verantwortliche Stelle für welche Verarbeitung, wer erteilt Weisungen, wer beantwortet Auskunftsersuchen? Das evangelische Gesetz kennt dafür ausdrücklich zentrale Verfahren, für die kirchliches Recht die Verteilung der datenschutzrechtlichen Aufgaben, Befugnisse und Verantwortlichkeiten zwischen den beteiligten Stellen abweichend regeln kann. Katholisch verständigen sich bei gemeinsamer Verantwortlichkeit die betroffenen Datenschutzaufsichten miteinander.

Die Architekturfrage im Detail: Ein Tenant oder viele? Kirchengemeinde, Kirchenkreis, Landeskirche, Bistum und die Frage der Tenant-Architektur.

Ist Copilot im kirchlichen Umfeld überhaupt zulässig?

Es gibt keine pauschale Antwort und erst recht keine Freigabe. Was sich belastbar sagen lässt: Copilot arbeitet auf den Berechtigungen, die im Tenant bereits vergeben sind. Ein unsauberes Berechtigungskonzept wird durch Copilot nicht schlimmer, aber schlagartig sichtbar — mit dem Unterschied, dass es vorher niemand gemerkt hat. Für die Aufsicht ist deshalb die Reihenfolge entscheidend: erst Berechtigungen bereinigen und klassifizieren, dann Folgenabschätzung, dann Mitbestimmung, dann Rollout. Wer die Reihenfolge umdreht, hat die Diskussion verloren, bevor sie beginnt.

Was ist mit Ehrenamtlichen und Gastzugängen?

Ehrenamtlich Tätige sind kirchenrechtlich keine Randgruppe. Katholisch zählen sie ausdrücklich zu den Personen, die auf das Datengeheimnis zu verpflichten und mit den Datenschutzvorschriften vertraut zu machen sind. Das gilt für das Presbyteriumsmitglied mit Zugriff auf Protokolle ebenso wie für die Person, die den Gemeindebrief-Verteiler pflegt. Im Aufsichtsgespräch wird nach den Verpflichtungserklärungen gefragt — und die Antwort „ehrenamtlich, deshalb formlos“ ist keine.

Wie bereite ich mich vor, wenn die Frist knapp ist?

Priorisiere nach Nachweisbarkeit, nicht nach Vollständigkeit. Ein aktuelles, ehrliches Verzeichnis, ein datierter Beschluss zum Berechtigungskonzept und ein realistischer Plan für die Folgenabschätzung wirken deutlich besser als vier halbfertige Dokumente ohne Datum. Und schreibe auf, was fehlt. Eine dokumentierte Lücke mit Termin ist ein Zeichen von Steuerung. Eine unerwähnte Lücke, die im Termin auffliegt, ist ein Zeichen von etwas anderem.

Fazit

Die kirchliche Datenschutzaufsicht erwartet von einem Microsoft-365-Tenant nichts Exotisches. Sie erwartet dieselben sechs Nachweise, die jede ordentliche Verwaltung ohnehin führen sollte — nur nach kirchlichem Recht, gegenüber einer eigenen Stelle und mit ein paar Besonderheiten, die man kennen muss: die Zweijahresrhythmen und Datenschutzklassen auf katholischer Seite, die Exit-Strategie für Cloud-Dienste seit der Novelle, die Sechsmonatsanforderung an die Eingabekontrolle, die Sonderstellung von Seelsorge- und Beichtgeheimnis, die Rolle der Mitarbeitervertretung.

Was sie nicht erwartet, ist Perfektion. Die Aufsichten wissen sehr genau, in welchem Personal- und Finanzrahmen kirchliche Träger arbeiten. Was sie erwartet, ist Steuerung: dass jemand namentlich verantwortlich ist, dass Entscheidungen datiert und begründet vorliegen, dass Lücken bekannt sind und einen Termin haben. Ein Träger, der seine Schwachstellen selbst benennt, wird anders behandelt als einer, dem sie nachgewiesen werden müssen.

Und der wichtigste Satz zum Schluss, weil er im Alltag am häufigsten verletzt wird: Die Verantwortung ist nicht delegierbar. Nicht an Microsoft, nicht an das Systemhaus, nicht an das Rechenzentrum, nicht an die örtlich Beauftragten. Sie liegt bei der Leitung der kirchlichen Stelle — bei der Geschäftsführung des diakonischen Werks, beim Vorstand des Caritasverbandes, beim Presbyterium, beim Kirchenvorstand. Wer das akzeptiert hat, führt ein produktives Gespräch. Wer es nicht akzeptiert hat, führt ein langes.

Wenn du für die Vorbereitung eines Aufsichtsgesprächs oder für die Aufarbeitung der Nachweise Unterstützung suchst: Microsoft 365 Beratung für kirchliche Träger. Für die Einordnung der Rechtslage insgesamt lohnt der Blick auf Microsoft 365 für Kirche, Diakonie und Caritas – DSG-EKD und KDG sowie auf Microsoft 365 in Kirche, Diakonie und Caritas: Was wirklich anders ist als in Kommune und Mittelstand.