

Ein Tenant oder viele? Kirchengemeinde, Kirchenkreis, Landeskirche, Bistum und die Frage der Tenant-Architektur

Die Frage klingt technisch. Sie ist es nicht. Wenn in einem Landeskirchenamt oder einem Generalvikariat die Frage aufkommt, ob man „einen Tenant für alle“ macht oder „jeder seinen eigenen“, dann geht es in Wahrheit um Macht, Geld, Haftung und um die Frage, wer am Ende haftet, wenn eine Beratungsakte im falschen Team landet. Die Technik ist dabei der unkomplizierteste Teil.

Der Grund ist eine Eigenheit, die es außerhalb der Kirche in dieser Schärfe kaum gibt: Eine Landeskirche ist kein Konzern. Ein Bistum ist keine Holding. Die Kirchengemeinde am Stadtrand ist eine eigene Körperschaft des öffentlichen Rechts mit eigenem Leitungsorgan, eigenem Haushalt und eigener datenschutzrechtlicher Verantwortlichkeit. Sie ist keine Filiale. Wenn du in Microsoft 365 alle in einen Tenant steckst, verschmilzt du technisch, was rechtlich getrennt bleibt. Das ist machbar und oft sogar richtig – aber es will aufgeschrieben sein, und zwar bevor der erste Benutzer angelegt wird.

Dieser Beitrag gehört zur Serie [Microsoft 365 in Kirche, Diakonie und Caritas](#). Dort findest du die Übersicht über alle Themen von Datenschutz über Lizenzierung bis Telefonie. Hier geht es um die eine Entscheidung, die man später am teuersten korrigiert: den Zuschnitt der Mandantengrenze.

WICHTIG | Die Reihenfolge entscheidet

Tenant-Architektur ist keine IT-Entscheidung, die man nachträglich der Leitung zur Kenntnis gibt. Sie ist eine Organisationsentscheidung mit IT-Folgen. Wer sie in der IT-Abteilung trifft, bekommt sie in der Synode, im Kirchenvorstand oder im Verwaltungsrat des Trägers wieder auf den Tisch – dann allerdings mit bereits migrierten Postfächern und deutlich schlechteren Karten.

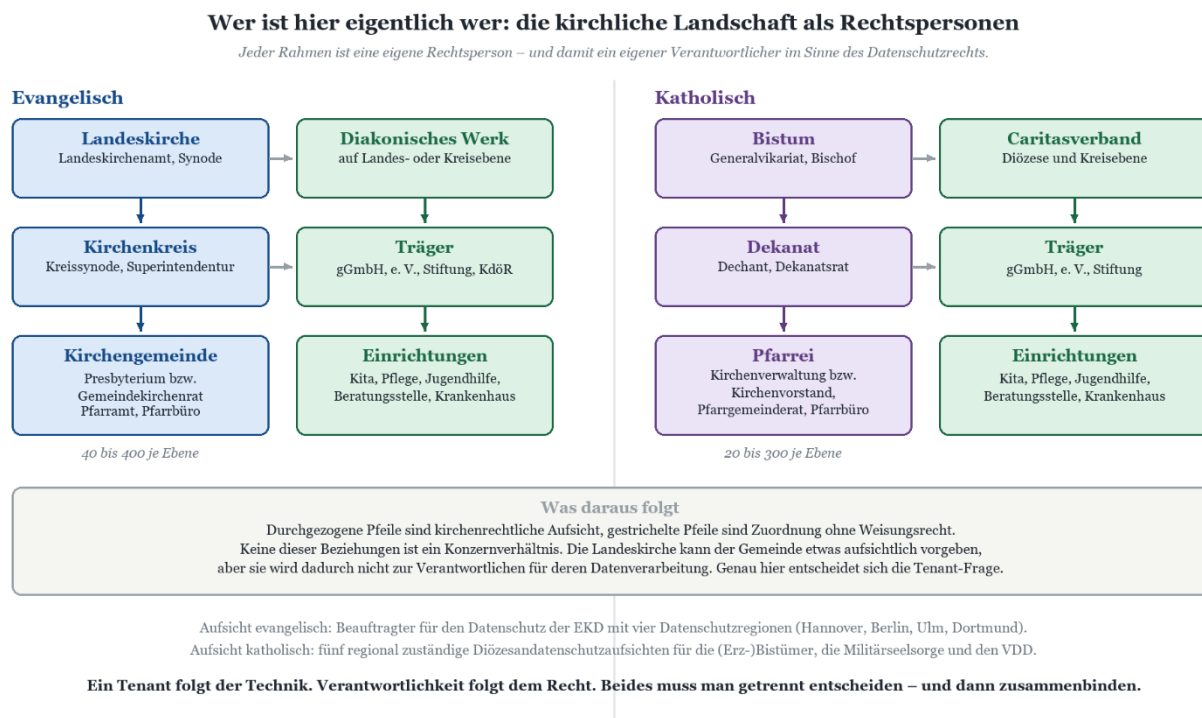
Warum die Frage in der Kirche anders klingt als im Konzern

In einem Unternehmen mit 30 Tochtergesellschaften gibt es eine Muttergesellschaft, die Weisungen erteilen kann. Sie entscheidet, dass alle in einen Tenant gehen, und dann gehen alle in einen Tenant. In der Kirche funktioniert das nicht, weil die Aufsichtsbeziehung nicht dasselbe ist wie ein Weisungsrecht über die Datenverarbeitung – und weil eine Kirchengemeinde in vielen Landeskirchen und Bistümern durchaus das Recht hat, ihre Verwaltung selbst zu organisieren.

Hunderte Körperschaften, keine Konzernmutter

Nimm eine mittlere Landeskirche: ein Landeskirchenamt, zwei Dutzend Kirchenkreise, mehrere hundert Kirchengemeinden, dazu ein diakonisches Werk mit eigenen Trägern, Kindertagesstätten in gemeindlicher und in verbandlicher Trägerschaft, ein paar Stiftungen und ein Krankenhausverbund, der rechtlich längst eine gGmbH ist. Auf katholischer Seite: ein Generalvikariat, Dekanate, Pfarreien mit Kirchenverwaltung oder Kirchenvorstand, ein Diözesan-Caritasverband, Kreis-Caritasverbände, Ordensträger, Bildungswerke. In beiden Fällen redest du über eine dreistellige Zahl eigenständiger Verantwortlicher, die alle E-Mail brauchen, alle mit Word arbeiten und von denen die wenigsten eine eigene IT haben.

Die gesamtkirchlichen Größenordnungen unterstreichen das: Die EKD besteht aus zwanzig Gliedkirchen mit weit über zehntausend Kirchengemeinden, die katholische Kirche in Deutschland aus 27 (Erz-)Bistümern. Keine dieser Ebenen ist rechtlich einfach die Untergliederung der nächsthöheren. Genau deshalb ist der Satz „wir machen einen Tenant für die ganze Landeskirche“ kein Architekturbeschluss, sondern eine Absichtserklärung, der noch dreihundert Beitrittsbeschlüsse folgen müssen.



Skizze 1: Die kirchliche Landschaft als Rechtspersonen – jeder Rahmen ein eigener Verantwortlicher, keine Linie ein Konzernverhältnis.

Die Aufsicht ist ebenfalls föderal

Der zweite Unterschied zur Kommune: Die Datenschutzaufsicht ist nicht die Landesbehörde, und sie ist auch nicht eine einzige Stelle. Auf evangelischer Seite ist der Beauftragte für den Datenschutz der EKD zuständig, und zwar für die EKD selbst, für die allermeisten Gliedkirchen und deren Zusammenschlüsse sowie für die zugeordneten diakonischen Werke und Einrichtungen, unabhängig von deren Rechtsform. Diese Behörde gliedert sich in vier Datenschutzregionen mit Außenstellen in Hannover, Berlin, Ulm und Dortmund. Auf katholischer Seite gibt es fünf regional zuständige Diözesandatschutzaufsichten, darunter das Katholische Datenschutzzentrum in Dortmund für den Westen und das Katholische Datenschutzzentrum in Frankfurt für Mitte und Südwest.

Das hat eine handfeste Konsequenz für die Tenant-Frage: Wenn ein diakonischer Träger und eine Landeskirche in einen Tenant gehen, bleiben beide gegenüber derselben Aufsicht erklärungs-pflichtig – das ist einfach. Wenn aber ein evangelisches und ein katholisches Haus im selben Tenant zusammenarbeiten, etwa in einem ökumenischen Träger oder einer gemeinsamen Beratungsstelle, dann schauen zwei verschiedene Aufsichten auf dieselbe Konfiguration, jede nach ihrem eigenen Recht. Wer das plant, sollte es vorher mit beiden besprechen und nicht hinterher erklären.

Was die Aufsichten im Detail sehen wollen – Verzeichnis der Verarbeitungstätigkeiten, Protokollierung, Nachweis über die Auftragsverarbeitung –, steht in [Kirchliche](#)

Datenschutzaufsicht in der Praxis: Was BfD EKD und Diözesandatenschutzbeauftragte von einem Microsoft-365-Tenant erwarten. Die Rechtsgrundlagen selbst sind in DSG-EKD verständlich: Was das evangelische Datenschutzgesetz für Microsoft 365 konkret bedeutet und KDG verständlich: Microsoft 365 unter dem Kirchlichen Datenschutzgesetz der katholischen Kirche ausführlich behandelt.

Was Microsoft von alldem weiß: nichts

Ein Microsoft-365-Tenant kennt keine Körperschaften. Er kennt ein Verzeichnis, Domänen, Benutzer, Gruppen, Lizenzen und Richtlinien. Die Mandantengrenze ist die härteste Grenze, die das System hat: Innerhalb eines Tenants ist ein globaler Administrator faktisch überall zuständig, zwischen zwei Tenants muss man jede Zusammenarbeit einzeln erlauben. Alles, was wir im Folgenden „Delegation“ nennen, ist eine Schicht Verwaltung oberhalb dieser harten Grenze – nützlich, belastbar, aber eben keine zweite Mandantengrenze.

FAKTEN | Die harten technischen Randbedingungen

Eine Domäne gehört immer nur genau einem Tenant. Solange die Gemeinde ihre Domäne in ihrem eigenen Tenant hat, kann niemand sonst sie verwenden – ein Wechsel bedeutet, die Domäne im Quell-Tenant zu lösen, was bei vielen abhängigen Objekten mehrere Stunden dauern kann.

Microsoft 365 Business-Pläne sind auf 300 Plätze je Tenant begrenzt. Wer über 300 Arbeitsplätze hinauswächst, braucht Enterprise-Pläne – was den „einen Tenant für alle“ schlagartig teurer macht, wenn man nicht sauber mit Frontline- und Enterprise-Plänen mischt.

Das Microsoft-Nonprofit-Angebot umfasst bis zu 300 gespendete Lizenzen Microsoft 365 Business Basic sowie Rabatte auf weitere Pläne. Die früheren kostenlosen Zuwendungen für Office 365 E1 und Microsoft 365 Business Premium sind zum 1. Juli 2025 ausgelaufen; Business Premium gibt es seitdem nur noch vergünstigt.

Zwei Tenants lassen sich nicht zusammenführen. Es gibt keinen Knopf „Tenants verschmelzen“ – eine Konsolidierung ist immer eine Migration mit Werkzeug, Zeitplan und Nacharbeit.

Die vier Modelle und was sie wirklich kosten

In der Praxis landet man immer bei einem von vier Mustern – oder bei einer Mischung, was der Normalfall ist. Wichtig ist, dass du die Mischung bewusst wählst und nicht als Ergebnis von zehn Jahren Einzelentscheidungen vorfindest.

Modell	Governance	Datenschutz-Verantwortlichkeit	Aufwand	Passt für
Zentraler Tenant mit Verwaltungseinheiten	Eine Stelle betreibt, örtliche Administratoren verwalten ihren Ausschnitt; Richtlinien gelten für alle	Jede Körperschaft bleibt eigener Verantwortlicher; Vereinbarung über gemeinsame Verantwortlichkeit und Auftragsverarbeitung nötig	Hoch beim Aufbau, niedrig im Betrieb	Landeskirche oder Bistum mit Kirchenkreisen, Dekanaten und Gemeinden; Verbände mit vielen kleinen Einrichtungen
Tenant je Träger oder Verband	Jeder Träger entscheidet und betreibt selbst; Abstimmung nur freiwillig	Sauber getrennt, jeder für sich; kein Abstimmungsbedarf, aber auch keine gemeinsame Linie	Niedrig beim Aufbau, hoch und dauerhaft im Betrieb	Große Träger mit eigener IT: Krankenhausverbund, großes diakonisches Werk, Caritasverband mit eigener Abteilung
Multi-Tenant-Organisation	Mehrere Tenants bleiben eigenständig,	Getrennt, aber Benutzerdaten fließen zwischen den Tenants –	Mittel beim Aufbau, mittel im Betrieb, Lizenzvoraussetzung	Landeskirche und großer Träger, die eng zusammenarbeiten, aber

	werden aber als eine Organisation verbunden	das ist selbst eine Verarbeitung und braucht eine Grundlage	beachten	getrennt bleiben müssen oder wollen
B2B-Föderation und geteilte Kanäle	Keine gemeinsame Organisation, nur punktuelle Brücken zwischen Tenants	Vollständig getrennt; jede Freigabe ist ein eigener Vorgang	Niedrig, dafür mühsam in der Pflege	Projektbezogene Zusammenarbeit, ökumenische Vorhaben, Gremien mit Externen, Ehrenamt

Modell 1: Ein Tenant, viele Verwaltungseinheiten

Das ist das Modell, das in den letzten Jahren in den meisten Landeskirchen und Bistümern gewonnen hat – aus einem sehr praktischen Grund: Es ist der einzige Weg, auf dem eine Kirchengemeinde mit einer halben Verwaltungsstelle jemals einen ordentlichen bedingten Zugriff, Mehrfaktor-Anmeldung, Aufbewahrungsrichtlinien und ein getestetes Notfallkonzept bekommt. Alles andere wäre die Erwartung, dass ein Pfarrbüro nebenbei Sicherheitsarchitektur betreibt. Das wird nicht passieren, und es ist auch nicht fair, es zu erwarten.

Technisch trägt dieses Modell auf Verwaltungseinheiten in Microsoft Entra ID. Eine Verwaltungseinheit ist ein Behälter für Benutzer, Gruppen und Geräte, der den Wirkungskreis einer Administratorrolle auf genau diesen Ausschnitt begrenzt. Der ehrenamtliche IT-Verantwortliche eines Kirchenkreises kann Kennwörter für seine vierzig Pfarrbüros zurücksetzen, aber nicht für das Landeskirchenamt. Das ist genau die Delegation, die man braucht.

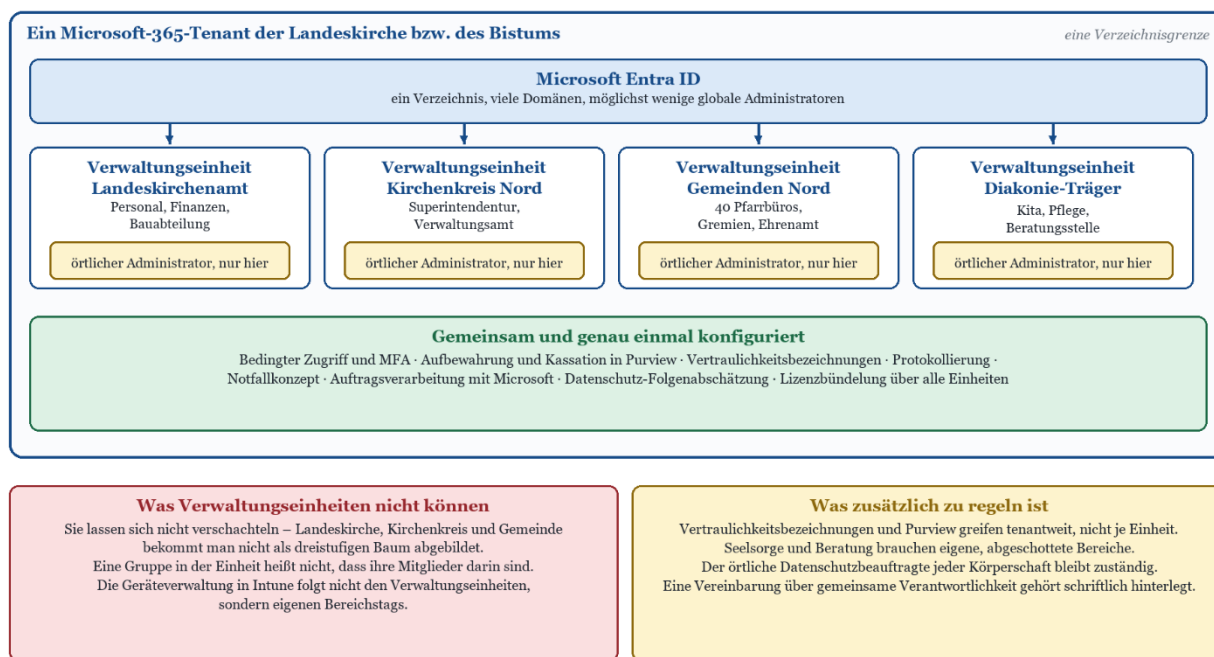
Es gibt allerdings Grenzen, und man sollte sie kennen, bevor man die Struktur zeichnet. Verwaltungseinheiten lassen sich nicht verschachteln – die dreistufige Hierarchie aus Landeskirche, Kirchenkreis und Gemeinde bildest du also nicht als Baum ab, sondern als flache Liste mit sprechenden Namen und gegebenenfalls Mehrfachmitgliedschaft. Wer eine Gruppe in eine Verwaltungseinheit aufnimmt, hat damit die Gruppe im Wirkungskreis, nicht aber deren Mitglieder: Der Kirchenkreis-Administrator könnte also die Mitgliedschaft der Gruppe ändern, aber nicht die Kennwörter der darin enthaltenen Personen zurücksetzen, solange diese nicht selbst Mitglied der Verwaltungseinheit sind. Und die Geräteverwaltung in Intune folgt nicht den Verwaltungseinheiten, sondern eigenen Bereichstags – wer Delegation plant, muss beide Mechanismen zusammen denken.

TIPP | Eingeschränkt verwaltete Verwaltungseinheiten für Seelsorge und Beratung

Microsoft Entra ID kennt Verwaltungseinheiten mit eingeschränkter Verwaltung. Objekte darin sind gegen Zugriffe auch durch tenantweite Administratoren geschützt, solange diese nicht ausdrücklich für die Einheit berechtigt sind. Für Konten in der Seelsorge, in der Schwangerschafts- oder Schuldnerberatung und für Personalverwaltung ist das das stärkste Instrument, das ein zentraler Tenant zu bieten hat. Es ersetzt keine Trennung der Inhalte, aber es nimmt dem Argument „der zentrale Administrator kann eh alles“ die Spitze.

Zielbild A: ein Tenant, viele Verwaltungseinheiten

Eine Mandantengrenze, delegierte Administration je Körperschaft, gemeinsame Sicherheits- und Aufbewahrungspolitik.



Skizze 2: Zielbild A – ein Tenant, delegierte Administration je Körperschaft, gemeinsame Sicherheits- und Aufbewahrungspolitik.

Modell 2: Tenant je Träger oder Verband

Die ehrliche Variante für alle, die tatsächlich eigene IT haben. Ein katholischer Krankenhausverbund mit mehreren Standorten hat eine IT-Abteilung mit zwei Dutzend Leuten, ein Rechenzentrum, ein Krankenhausinformationssystem, Schichtbetrieb rund um die Uhr und Anforderungen, die mit denen eines Pfarrbüros exakt nichts zu tun haben. Diesen Verbund in den Tenant des Bistums zu zwingen, erzeugt keinen Nutzen, sondern zwei unzufriedene Parteien und eine Governance, die niemandem passt.

Der Preis ist die Vervielfachung aller Regelwerke. Jede Richtlinie für bedingten Zugriff, jedes Aufbewahrungskonzept, jede Vertraulichkeitsbezeichnung, jeder Notfallplan, jede Schulungsreihe und jeder Auftragsvertragsvertrag existiert n-mal. Das ist bei drei großen Trägern vertretbar und bei dreißig kleinen Gemeinden absurd. Die Faustregel, die sich in der Praxis bewährt hat: Ein eigener Tenant lohnt sich ab der Größenordnung, in der eine Vollzeitstelle allein für den Betrieb der Zusammenarbeitsplattform da ist. Darunter wird es Schatten-IT.

Modell 3: Die Multi-Tenant-Organisation

Seit Microsoft die Multi-Tenant-Organisation eingeführt hat, gibt es eine Zwischenstufe, die vorher fehlte. Mehrere Tenants bleiben rechtlich und administrativ getrennt, werden aber als eine Organisation verbunden: Benutzer werden per tenantübergreifender Synchronisierung in die anderen Tenants übertragen, und zwar nicht als Gäste, sondern als B2B-Benutzer vom Typ Mitglied. Das Ergebnis ist eine gemeinsame Personensuche, Teams-Chat und Besprechungen über die Tenantgrenzen hinweg, ohne dass jemand das Konto wechseln muss.

Das klingt nach der eierlegenden Wollmilchsaue und ist es nicht ganz. Die Voraussetzungen sind konkret: Entra ID P1 oder höher in allen beteiligten Tenants, ein Maximum von 100 Tenants in der Organisation, bis zu 100.000 synchronisierte Benutzer je Synchronisierungsauftrag. Der neue Teams-Desktopclient ist für die gute Erfahrung erforderlich; Microsoft Teams Rooms werden nicht

unterstützt. Und der Hinweis, der in Projekten am häufigsten für Irritation sorgt: Nach der Synchronisierung kann es bis zu sieben Tage dauern, bis eine Person in der Suche auftaucht. Wer am Montag synchronisiert und am Dienstag die Abnahme ansetzt, hat ein Gespräch vor sich.

WARNUNG | Tenantübergreifende Synchronisierung ist selbst eine Verarbeitung

Wenn Beschäftigtendaten aus dem Tenant eines diakonischen Trägers in den Tenant der Landeskirche synchronisiert werden, ist das eine Übermittlung personenbezogener Daten zwischen zwei Verantwortlichen. Sie braucht eine Rechtsgrundlage, gehört ins Verzeichnis der Verarbeitungstätigkeiten, und die Mitarbeitervertretung wird fragen, welche Attribute genau übertragen werden. Die Antwort „alle, das ist der Standard“ ist keine gute Antwort. Schränke die Attributzuordnung ein und dokumentiere sie.

Modell 4: B2B-Föderation, geteilte Kanäle, Gastzugang

Die schlanke Variante für alles, was Zusammenarbeit ist, aber keine gemeinsame Organisation. Geteilte Kanäle in Teams arbeiten über B2B Direct Connect: Ein Kanal im Tenant des Kirchenkreises kann Personen aus dem Tenant des diakonischen Trägers aufnehmen, die Inhalte bleiben aber im Heimat-Tenant des Kanals. Für eine ökumenische Arbeitsgruppe, einen gemeinsamen Bauausschuss oder ein befristetes Projekt ist das genau richtig. Für die dauerhafte Zusammenarbeit von zweihundert Personen ist es Nervenkrieg.

Für Ehrenamtliche gilt Ähnliches, nur mit mehr Fallstricken. Die Frage, ob das Presbyteriumsmitglied ein eigenes Konto, einen Gastzugang oder schlicht eine PDF-Datei per E-Mail bekommt, ist ausführlich behandelt und verdient eine eigene Entscheidung je Personengruppe.

Mechanismus	Was er leistet	Wo er aufhört	Voraussetzung
Verwaltungseinheiten	Delegierte Verwaltung von Benutzern, Gruppen und Geräten je Körperschaft	Keine Verschachtelung; Intune folgt eigenen Bereichstags; keine Trennung der Inhalte	Entra ID P1 für jeden delegierten Administrator
Eingeschränkt verwaltete Einheiten	Schutz sensibler Konten auch vor tenantweiten Administratoren	Schützt Konten, nicht Postfachinhalte oder Dateien	Entra ID P1, sorgfältige Rollenplanung
Intune-Bereichstags	Delegierte Geräte- und Richtlinienverwaltung je Region oder Träger	Vergeben keine Rechte, sie begrenzen nur die Sicht	Intune-Plan, eigene Rollenzuweisungen
Multi-Tenant-Organisation	Gemeinsame Personensuche, Chat und Besprechungen über Tenantgrenzen	Keine gemeinsamen Richtlinien, keine gemeinsame Aufbewahrung	Entra ID P1 in allen Tenants, max. 100 Tenants
Geteilte Kanäle	Gemeinsame Kanäle ohne Kontowechsel, Daten bleiben im Heimat-Tenant	Nur Kanäle, kein vollständiger Team-Zugriff	B2B Direct Connect je Tenant konfigurieren
Gastzugang	Punktueller Zugriff für Externe und Ehrenamt	Pflegeaufwand, Ablaufsteuerung, Übersichtsverlust bei hohen Zahlen	Zugriffsüberprüfungen, sonst wächst es zu

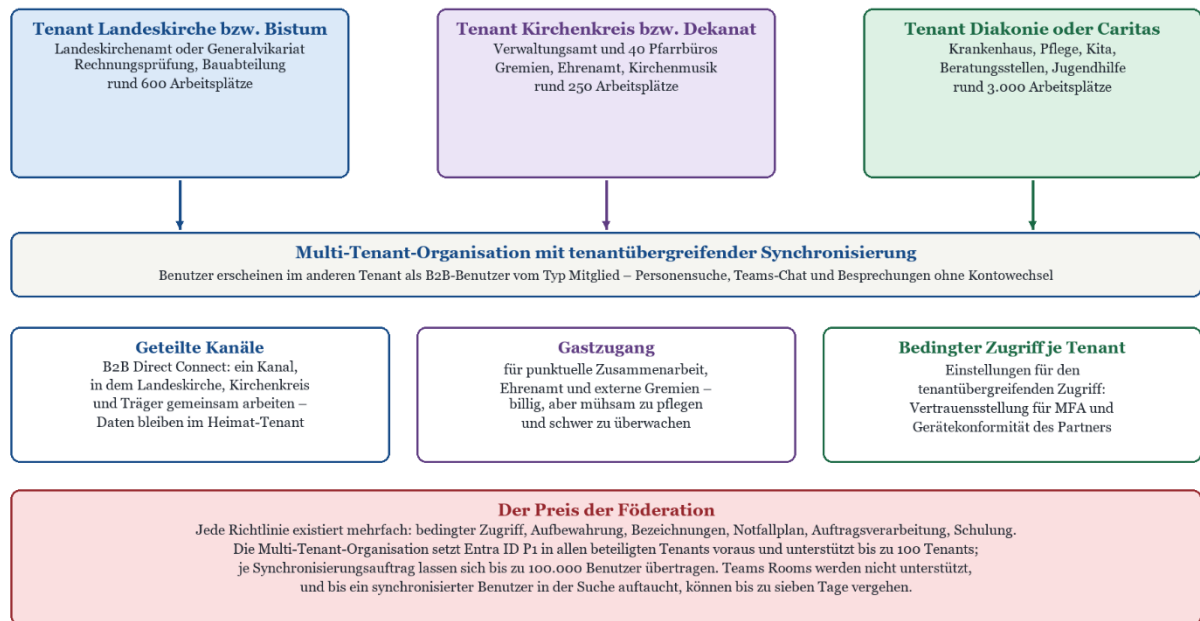
Zwei Zielbilder und die sechs Fragen, die dazwischen entscheiden

Die beiden Endpunkte des Spektrums lassen sich gut zeichnen. Alles, was in echten Projekten gebaut wird, liegt dazwischen: ein zentraler Tenant für Landeskirche, Kirchenkreise und

Gemeinden, daneben zwei oder drei große Träger mit eigenem Tenant, verbunden über eine Multi-Tenant-Organisation. Das ist nicht Unentschlossenheit, das ist der Normalfall.

Zielbild B: mehrere Tenants, verbunden statt verschmolzen

Jede Körperschaft behält ihre Mandantengrenze; die Zusammenarbeit läuft über definierte Brücken.



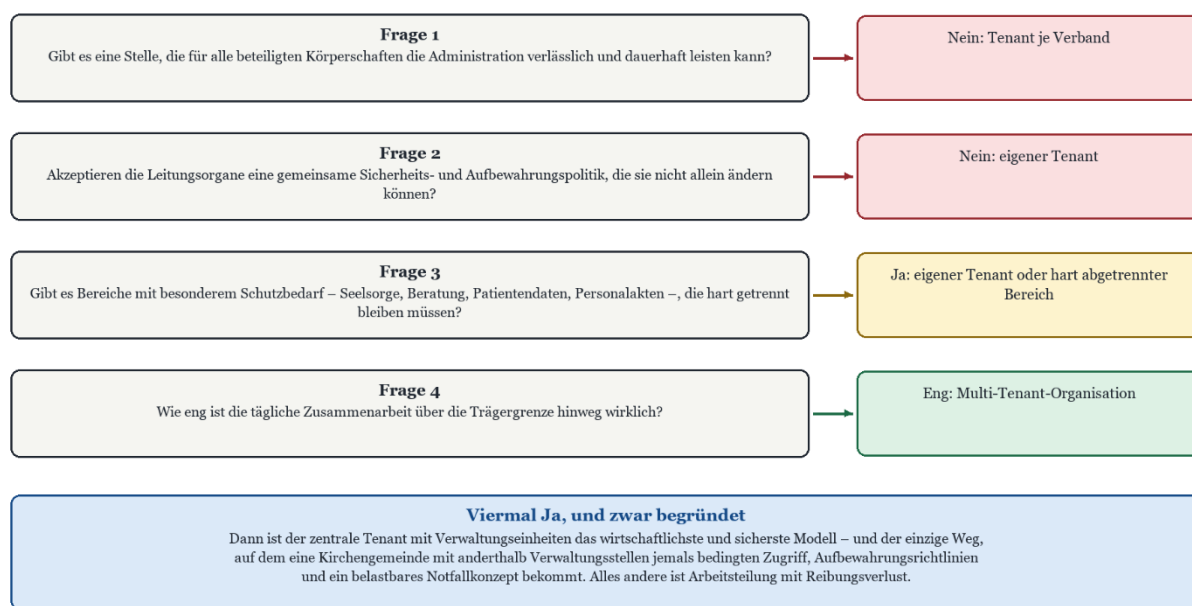
Skizze 3: Zielbild B – mehrere Tenants, verbunden über Multi-Tenant-Organisation, geteilte Kanäle und Gastzugang.

Die Kriterien, die wirklich tragen

Kriterium	Die Leitfrage	Spricht für zentralen Tenant	Spricht für eigenen Tenant
Rechtsträgerschaft	Wie viele eigenständige Körperschaften und Gesellschaften sind beteiligt?	Viele kleine Träger mit gleichartigen Aufgaben	Wenige große Träger mit völlig unterschiedlichem Betrieb
Verantwortlichkeit	Lässt sich die gemeinsame Verantwortlichkeit sauber vereinbaren und leben?	Ja, es gibt eine Stelle, die Vereinbarungen führt und pflegt	Nein, oder besondere Kategorien machen Trennung zwingend
Administrationskapazität	Wer betreibt das morgens um sieben, wenn die Anmeldung klemmt?	Zentrale IT oder gemeinsames Rechenzentrum vorhanden	Eigene IT-Abteilung mit Bereitschaft und Verantwortung
Lizenzbündelung	Wo entsteht der bessere Preis und die bessere Ausstattung?	Bündelung über alle Einheiten, einheitliche Schutzstufe	Eigener Vertrag, eigene Bedarfe, eigener Beschaffungsweg
Zusammenarbeit	Wie viel Alltag läuft über die Trägergrenze hinweg?	Täglich: gemeinsame Projekte, Gremien, Verwaltung	Selten und projektbezogen
Schutzbedarf	Gibt es Daten, die technisch hart getrennt bleiben müssen?	Schutzbedarf ist mit Bereichen und Bezeichnungen abbildbar	Seelsorge, Beratung, Patientendaten in großem Umfang

Der Entscheidungsweg: vier Fragen, vier Modelle

In dieser Reihenfolge gestellt – nicht in der Reihenfolge, in der sie im Gremium hochkommen.



Skizze 4: Der Entscheidungsweg – vier Fragen in der Reihenfolge, in der sie beantwortet werden müssen.

Der Fehler, den fast alle machen

Der häufigste Fehler ist nicht die falsche Modellwahl. Es ist die Entscheidung nach der Lautstärke. In jeder Beratung gibt es die eine Einrichtung, die sehr energisch erklärt, warum sie unbedingt einen eigenen Tenant braucht – und bei der sich nach zwei Fragen herausstellt, dass es um eine einzige Fachanwendung geht oder um die Sorge, dass jemand aus der Zentrale in die Postfächer schaut. Beides sind legitime Anliegen. Für beides ist ein eigener Tenant die teuerste denkbare Lösung.

Die Gegenprobe ist genauso häufig: Eine zentrale IT möchte alle in einen Tenant holen, weil es einfacher ist, und unterschätzt dabei, dass sie damit auch den Anruf aus jedem einzelnen Pfarrbüro bekommt, wenn der Drucker nicht will. Ein zentraler Tenant ohne aufgebaute Serviceorganisation ist kein Sparmodell, sondern eine Überlastungszusage mit Zeitverzögerung.

AUS DER PRAXIS | Ein Kirchenkreis mit 40 Gemeinden

Ausgangslage: 40 Kirchengemeinden, jede mit eigenem Pfarrbüro, jede eine eigene Körperschaft. Vorgefunden wurden sieben eigene Microsoft-365-Tenants, drei davon von einem Ehrenamtlichen eingerichtet und seit Jahren ohne Mehrfaktor-Anmeldung, elf Gemeinden mit reinen Freemail-Adressen im Gemeindebrief und ein Verwaltungsamt mit einem gewachsenen Exchange-Server im Keller.

Entscheidung: ein Tenant auf Ebene des Kirchenkreises, eine Verwaltungseinheit je Gemeinde, zusätzlich eine Verwaltungseinheit für das Verwaltungsamt und eine eingeschränkt verwaltete Einheit für Personal und Seelsorge. Je Gemeinde wurde eine Person benannt, die Kennwörter zurücksetzen und Gruppen pflegen darf – und ansonsten nichts. Die Kirchenmusik, die Kindertagesstätten in gemeindlicher Trägerschaft und der Friedhofsverband kamen in eigene Verwaltungseinheiten.

Was wirklich Arbeit gemacht hat: nicht die Technik. Sondern 40 Beschlüsse der Presbyterien über den Beitritt, eine Vereinbarung über gemeinsame Verantwortlichkeit, die Klärung, wer örtlicher Datenschutzbeauftragter bleibt, und die Frage, was mit den Mailadressen passiert, die seit 2009 auf dem Gemeindebrief stehen. Kalkulierte Projektdauer: acht Monate. Tatsächliche Dauer: vierzehn –

weil zwei Presbyterien erst nach der Sommerpause tagten.

Ergebnis nach zwei Jahren: eine einzige Richtlinie für bedingten Zugriff statt sieben ungeschützter Tenants, Mehrfaktor-Anmeldung flächendeckend, ein gemeinsames Aufbewahrungskonzept – und eine Stelle, die im Notfall tatsächlich handlungsfähig ist. Der Kirchenkreis zahlt heute mehr für Lizenzen als vorher und deutlich weniger für Zwischenfälle.

Verantwortlichkeit: Wer haftet, wenn alle im selben Tenant sind

Hier liegt der eigentliche Kern der Frage, und hier wird in Projekten am meisten durcheinandergebracht. Der zentrale Tenant macht die Landeskirche oder das Bistum nicht automatisch zur verantwortlichen Stelle für alles, was darin passiert. Und er entlastet die Kirchengemeinde nicht von ihrer eigenen Verantwortlichkeit.

Gemeinsame Verantwortlichkeit oder Auftragsverarbeitung

Beide kirchlichen Datenschutzgesetze kennen die beiden Konstruktionen, und beide meinen damit dasselbe wie das staatliche Recht. Im evangelischen Recht regelt § 29 DSG-EKD die gemeinsam verantwortlichen Stellen: Wenn zwei oder mehr Verantwortliche gemeinsam über Zwecke und Mittel der Verarbeitung entscheiden, müssen sie in einer transparenten Vereinbarung festlegen, wer welche Pflicht erfüllt; wesentliche Inhalte sind den Betroffenen zugänglich zu machen, und Betroffene können ihre Rechte gegenüber jedem einzelnen Verantwortlichen geltend machen. § 30 DSG-EKD behandelt die Verarbeitung im Auftrag. Im katholischen Recht steht die gemeinsame Verantwortlichkeit in § 28 KDG, die Verarbeitung im Auftrag in § 29 KDG, und die Datenschutz-Folgenabschätzung in § 35 KDG.

Für die Tenant-Architektur heißt das übersetzt: Wenn das Landeskirchenamt den Tenant betreibt und die Gemeinde ihn nutzt, ist das in aller Regel eine Auftragsverarbeitung – die Gemeinde bestimmt, was mit ihren Daten geschieht, das Landeskirchenamt stellt den Betrieb. Sobald aber gemeinsame Zwecke hinzukommen, etwa ein landeskirchenweites Dokumentenmanagement mit gemeinsamem Meldewesen-Bezug oder eine zentrale Auswertung, kippt es in Richtung gemeinsamer Verantwortlichkeit. Beides ist zulässig. Beides muss schriftlich sein. Nichts davon regelt sich durch die Tatsache, dass man denselben Tenant benutzt.

WARNUNG | Der Satz, der ein Projekt kostet

„Die Gemeinden sind ja bei uns mit drin, dann brauchen wir dafür keinen eigenen Vertrag.“ – Doch. Der Betrieb eines Tenants für eine andere Körperschaft ist eine Verarbeitung personenbezogener Daten für einen anderen Verantwortlichen. Ohne Vereinbarung fehlt genau das Dokument, nach dem die Aufsicht als Erstes fragt. Und der Vertrag mit Microsoft ersetzt ihn nicht: Der regelt das Verhältnis zum Anbieter, nicht das Verhältnis der kirchlichen Körperschaften untereinander.

Wie diese Kette aus Microsoft, Systemhaus, kirchlichem Rechenzentrum und eigener Verwaltung vertraglich sauber gebaut wird, ist eigenes Thema. Die Grundlagen dazu und zur Abgrenzung gegenüber Kommune und Mittelstand stehen in [Microsoft 365 in Kirche, Diakonie und Caritas: Was wirklich anders ist als in Kommune und Mittelstand](#).

Seelsorge, Beratung und Personalakte als harte Grenze

Es gibt Daten, bei denen die Tenant-Frage gar nicht mehr die entscheidende ist, weil sie unabhängig vom Modell eine eigene Abschottung brauchen. Das Seelsorgegeheimnis und das

Beichtgeheimnis sind kein Datenschutzthema mit erhöhtem Schutzbedarf, sondern eine Grenze eigener Art: Was darunter fällt, gehört schlicht nicht in ein Werkzeug, in dem ein Administrator Wiederherstellungen durchführt, eine Aufbewahrungsrichtlinie greift oder ein Assistenzsystem den Inhalt zusammenfasst. Für Klientendaten in der Beratung, in der Jugendhilfe und in der Pflege gilt ein abgestuftes, aber ähnlich striktes Regime.

In der Architekturentscheidung schlägt das in beide Richtungen aus. Ein großer Beratungsträger kann daraus ein starkes Argument für einen eigenen Tenant bauen. Genauso gut kann man im zentralen Tenant mit eingeschränkt verwalteten Einheiten, streng abgetrennten Bereichen, Vertraulichkeitsbezeichnungen und ausgeschlossenen Aufbewahrungsbereichen arbeiten. Was nicht geht: die Frage offenlassen und hoffen, dass die Beratungsstelle schon selbst weiß, was sie nicht in Teams schreiben darf.

Die Mitarbeitervertretung entscheidet mit

Ein Punkt, der in Tenant-Projekten regelmäßig zu spät kommt: Die Zusammenführung mehrerer Dienststellen in einen gemeinsamen Tenant verändert die technischen Möglichkeiten der Leistungs- und Verhaltenskontrolle – und damit ist die Mitbestimmung berührt, im evangelischen Bereich nach dem MVG-EKD, im katholischen nach der MAVO. Die Besonderheit ist hier hübsch föderal: Wenn zehn Dienststellen in einen Tenant gehen, hat man es potenziell mit zehn Mitarbeitervertretungen zu tun, die jeweils für ihre Dienststelle zuständig sind. Wer nur mit der MAV der größten Einrichtung spricht, hat neun Gespräche vor sich, die er noch nicht kennt.

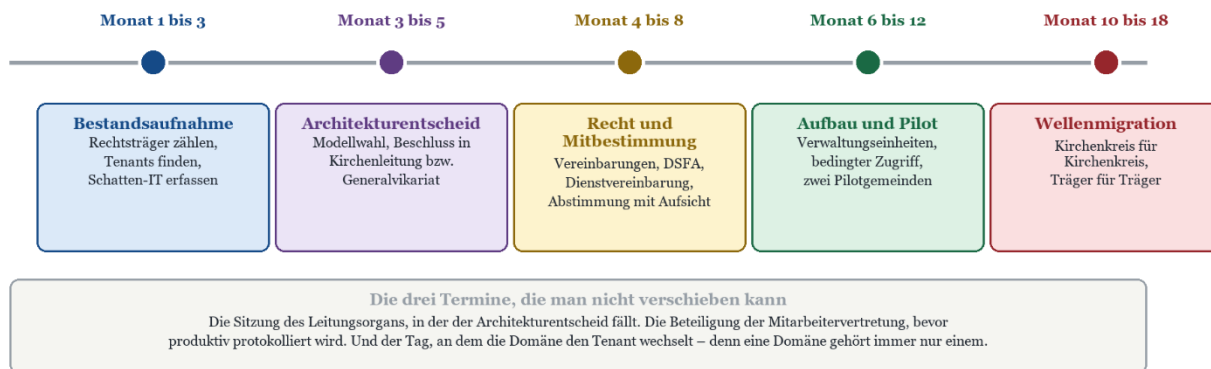
Der praktikable Weg ist eine Rahmen-Dienstvereinbarung auf der Ebene, auf der der Tenant betrieben wird, plus örtliche Ergänzungen. Was hineingehört – Protokollierung, Auswertungsverbot, Umgang mit Berichtsfunktionen, Regeln für Assistenzsysteme –, ist in [Mitarbeitervertretung und Microsoft 365: MVG-EKD, MAVO, Dienstvereinbarung und Mitbestimmung bei Teams, Copilot und Protokollierung](#) ausführlich beschrieben. Der wichtigste Rat daraus gilt auch hier: Beteilige die MAV, wenn die Architektur noch eine Skizze ist. Danach ist es keine Beteiligung mehr, sondern eine Mitteilung.

Vom Beschluss in den Betrieb

Angenommen, die Entscheidung ist gefallen. Dann beginnt der Teil, für den in Projektplänen typischerweise ein Drittel der nötigen Zeit steht.

Ein realistischer Fahrplan von der Entscheidung zum Betrieb

Zwölf bis achtzehn Monate – wer schneller plant, plant an der Synode vorbei.



Skizze 5: Ein realistischer Fahrplan – zwölf bis achtzehn Monate von der Bestandsaufnahme bis zur letzten Migrationswelle.

Zuerst zählen, dann planen

Die Bestandsaufnahme ist unbeliebt und unverzichtbar. Wie viele Rechtsträger gibt es wirklich – nicht laut Organigramm, sondern laut Registern und Satzungen? Wie viele Microsoft-365-Tenants existieren bereits? Die Antwort lautet fast immer „mehr als gedacht“, weil irgendwer irgendwann für die Jugendarbeit etwas eingerichtet hat und weil jede kostenlose Testversion einen Tenant erzeugt. Dazu: Welche Domänen liegen wo, welche Mailadressen stehen im Gemeindebrief, welche Fachanwendungen hängen an welcher Anmeldung, und wer hat heute faktisch administrative Rechte?

Ein Nebenbefund, der in praktisch jedem Projekt auftaucht: Es gibt bereits einen Tenant, den niemand kennt, weil Microsoft ihn bei der Registrierung einer Domäne durch einen Beschäftigten automatisch angelegt hat. Solange dieser Tenant die Domäne beansprucht, kann der neue ihn nicht verwenden. Das ist lösbar, kostet aber Zeit – und Zeit ist in einem Migrationsfenster die knappste Ressource.

Namensraum und Domänen

Die Frage, ob die Gemeinde weiterhin unter ihrer eigenen Domäne erreichbar ist, wenn sie im Tenant des Kirchenkreises sitzt, hat eine beruhigende Antwort: Ja. Ein Tenant kann viele Domänen führen, und Postfächer können unterschiedliche Hauptadressen haben. Die Identität nach außen bleibt also erhalten, auch wenn die Verwaltung zusammenläuft. Was nicht geht, ist dieselbe Domäne in zwei Tenants. Für Migrationsphasen heißt das: entweder Umstellung an einem Stichtag oder Betrieb über Zwischenadressen mit Weiterleitung, was man niemandem länger als ein paar Wochen zumuten sollte.

TIPP | Namenskonventionen vor dem ersten Objekt festlegen

Lege fest, wie Verwaltungseinheiten, Gruppen, Teams und SharePoint-Bereiche heißen, bevor das erste Objekt entsteht. Ein Präfix je Körperschaft – Kürzel für Kirchenkreis oder Träger, dann Aufgabe – wirkt kleinlich und rettet dir später die Zugriffsüberprüfung, die Aufbewahrungszuordnung und jede Auswertung. Nachträgliches Umbenennen von tausend Objekten ist möglich, aber es ist genau die Art Arbeit, für die im Haushalt kein Titel vorgesehen ist.

Migration heißt Wellen, nicht Stichtag

Vierzig Gemeinden migriert man nicht an einem Wochenende. Man migriert sie in Wellen von drei bis fünf, beginnend mit zwei Pilotgemeinden, die freiwillig dabei sind und ein wenig Leidensfähigkeit mitbringen. Jede Welle folgt demselben Muster: Vorbereitung der Konten, Übernahme der Postfächer und Dateien, Umstellung der Domäne oder Adressen, Schulung, dann zwei Wochen erhöhte Betreuung. Wer das gut macht, braucht für den Rest keine Überzeugungsarbeit mehr – die Gemeinden, die noch warten, fragen von selbst nach einem früheren Termin.

Und noch ein Punkt zur Lizenzbündelung, weil er in Gremien immer kommt: Der zentrale Tenant erlaubt eine gemeinsame Beschaffung und damit oft bessere Konditionen und eine einheitliche Schutzstufe. Er zwingt aber auch dazu, die Zuordnung sauber zu halten – wer welche Lizenz trägt, muss der Kostenstelle folgen, sonst bekommst du eine Umlage, die keiner nachvollziehen kann. Verwaltungseinheiten helfen dabei, weil die Lizenzverwaltung auf ihren Wirkungskreis begrenzt werden kann.

Welche Lizenzen für welche Gruppe überhaupt in Frage kommen und wer nach den Nonprofit-Bedingungen berechtigt ist, klärt [Microsoft-365-Lizenzierung für kirchliche Träger: Nonprofit-Angebote, Frontline-Pläne und die Frage, wer überhaupt berechtigt ist](#). Und wenn die Diskussion an der Stelle landet, ob es statt Microsoft 365 nicht das kirchliche Rechenzentrum tut, lohnt der nüchterne Blick in [Die Cloud-Frage in der Kirche: Kirchliche Rechenzentren, Microsoft 365 und die Ehrlichkeit über Datenstandorte](#).

Häufige Fragen

Können wir später noch vom föderierten Modell in einen zentralen Tenant wechseln?

Ja, aber es ist eine Migration, keine Umkonfiguration. Zwei Tenants lassen sich nicht zusammenführen; Postfächer, Dateien, Teams, Geräte und Identitäten werden mit Werkzeugen übertragen, Domänen müssen im Quell-Tenant gelöst werden, bevor sie im Ziel verwendet werden können. Rechne mit einem Projekt, nicht mit einem Wochenende. Der umgekehrte Weg – aus einem zentralen Tenant einzelne Träger herauslösen – ist genauso aufwendig. Deshalb lohnt sich die Sorgfalt am Anfang so sehr.

Verliert unsere Gemeinde ihre Selbstständigkeit, wenn sie in den Tenant des Kirchenkreises geht?

Rechtlich nicht. Die Gemeinde bleibt eigene Körperschaft, bleibt eigene verantwortliche Stelle, behält ihr Leitungsorgan und in der Regel auch ihre Domäne und ihre Mailadressen. Was sie abgibt, ist der technische Betrieb und ein Stück Gestaltungsfreiheit bei Sicherheitsrichtlinien – sie kann dann nicht mehr allein entscheiden, ob Mehrfaktor-Anmeldung Pflicht ist. Das ist genau der Punkt, den der Beitrittsbeschluss des Presbyteriums oder der Kirchenverwaltung ausdrücklich benennen sollte.

Kann der zentrale Administrator dann in unsere Postfächer schauen?

Technisch kann ein globaler Administrator sich Zugriff verschaffen – das gilt in jedem Tenant, auch im eigenen. Die Antwort ist deshalb nicht technisch, sondern organisatorisch: möglichst wenige globale Administratoren, Rollen nur zeitlich begrenzt und mit Begründung, lückenlose Protokollierung privilegierter Zugriffe, eingeschränkt verwaltete Verwaltungseinheiten für sensible Konten und eine Dienstvereinbarung, die den Zugriff auf Beschäftigtenpostfächer an ein Verfahren bindet. Wer das umsetzt, hat mehr Schutz als in einem eigenen Tenant, der von einem Ehrenamtlichen mit Dauerkennwort betreut wird.

Wie viele Verwaltungseinheiten sind sinnvoll?

So viele wie es delegierte Zuständigkeiten gibt – und keine einzige mehr. In der Praxis ist eine Einheit je Körperschaft mit eigener Verwaltung ein guter Schnitt, ergänzt um Einheiten für Funktionsbereiche mit besonderem Schutzbedarf. Weil Verwaltungseinheiten sich nicht verschachteln lassen, brauchst du eine flache, sprechende Namensstruktur. Microsoft empfiehlt ausdrücklich, den Zuschnitt anfangs zu erproben, unnötige Einheiten danach wieder abzuräumen und erst dann zu stabilisieren.

Unser Krankenhaus will auf keinen Fall in den Bistums-Tenant. Ist das Sturheit?

Meistens nicht. Ein Krankenhaus hat Schichtbetrieb, ein Krankenhausinformationssystem, eigene Meldewege, andere Verfügbarkeitsanforderungen und in der Regel eine eigene IT-Abteilung mit Rufbereitschaft. Das sind sachliche Gründe. Die Multi-Tenant-Organisation ist für genau diese Konstellation gebaut: getrennte Tenants, gemeinsame Personensuche, Chat und Besprechungen ohne Kontowechsel. Wichtig bleibt, dass die Büro-IT und das Fachsystem sauber getrennt betrachtet werden – das KIS bleibt das KIS.

Was ist mit Ehrenamtlichen im Presbyterium oder Pfarrgemeinderat?

Das ist eine eigene Entscheidung je Personengruppe und sollte nicht als Nebeneffekt der Tenant-Architektur fallen. Grob: Wer regelmäßig mit personenbezogenen Daten arbeitet, braucht ein eigenes Konto mit Mehrfaktor-Anmeldung – Gastzugänge sind dafür auf Dauer unpraktisch. Wer nur Sitzungsunterlagen liest, ist mit einem geteilten Kanal oder einer kontrollierten Freigabe besser bedient. In jedem Fall gehören Zugriffsüberprüfungen dazu, sonst hast du nach drei Wahlperioden mehr inaktive Gastkonten als Gemeindeglieder im Gottesdienst.

Braucht jede beteiligte Körperschaft einen eigenen örtlich Beauftragten für den Datenschutz?

Die Benennungspflicht richtet sich nach dem jeweiligen kirchlichen Datenschutzgesetz und nach der Art der Verarbeitung, nicht nach der Tenant-Architektur. Ein gemeinsamer Tenant ändert daran nichts: Die Verantwortlichkeit bleibt bei der einzelnen Körperschaft, und damit bleibt auch die Frage der Benennung bei ihr. Üblich und sinnvoll ist, dass sich mehrere kleine Körperschaften einen Beauftragten teilen – das ist etwas anderes, als keinen zu haben.

Wir haben schon fünf Tenants gewachsen. Wo fangen wir an?

Mit einer Bestandsaufnahme, die ehrlich ist, und mit einer Risikobewertung: Welcher dieser Tenants ist heute ungeschützt? Meist gibt es ein oder zwei, in denen weder Mehrfaktor-Anmeldung noch Protokollierung noch ein Notfallkontakt existiert. Diese sichert man zuerst, unabhängig von der Zielarchitektur. Danach entscheidest du das Zielbild und konsolidierst in Wellen. Wer zuerst das Zielbild diskutiert und dabei die ungeschützten Tenants sechs Monate weiterlaufen lässt, hat die Reihenfolge falsch herum.

Fazit

Die Tenant-Frage ist eine Organisationsfrage im Kostüm einer IT-Frage. Wer sie technisch beantwortet, bekommt eine technisch saubere Lösung, die im Gremium scheitert. Wer sie politisch beantwortet, bekommt einen Kompromiss, den niemand betreiben kann. Die brauchbare Antwort entsteht, wenn beides zusammenkommt: Rechtsträgerschaft und Verantwortlichkeit klären, ehrlich prüfen, wer Administration wirklich leisten kann, den Schutzbedarf von Seelsorge und Beratung ernst nehmen – und dann das Modell wählen, das zu den Antworten passt.

Für die große Mehrheit der kirchlichen Landschaft läuft das auf ein gemischtes Bild hinaus: ein zentraler Tenant für Landeskirche oder Bistum, Kirchenkreise oder Dekanate und Gemeinden, mit Verwaltungseinheiten als Delegationsschicht und eingeschränkt verwalteten Einheiten für die sensiblen Bereiche – daneben eigene Tenants für die wenigen großen Träger mit eigener IT, verbunden über eine Multi-Tenant-Organisation und geteilte Kanäle. Das ist kein eleganter Entwurf. Es ist der Entwurf, der zu einer Kirche passt, die seit Jahrhunderten föderal organisiert ist und es auch bleiben wird.

Und der beste Zeitpunkt, diese Entscheidung zu treffen, ist der, an dem noch wenig migriert ist. Der zweitbeste ist heute. Der schlechteste ist der Tag, an dem die dreizehnte Gemeinde auf eigene Faust einen Tenant anlegt, weil das Warten auf ein Konzept länger gedauert hat als eine Kreditkartenzahlung.

WEITER IM THEMA

- › [Microsoft 365 in Kirche, Diakonie und Caritas](#)
- › [Microsoft 365 in Kirche, Diakonie und Caritas: Was wirklich anders ist als in Kommune und Mittelstand](#)
- › [Kirchliche Datenschutzaufsicht in der Praxis: Was BfD EKD und Diözesandatenschutzbeauftragte von einem Microsoft-365-Tenant erwarten](#)
- › [Mitarbeitervertretung und Microsoft 365: MVG-EKD, MAVO, Dienstvereinbarung und Mitbestimmung bei Teams, Copilot und Protokollierung](#)
- › [Microsoft 365 Einführungskonzept für kirchliche Träger: Die Kirchenedition zum Festpreis](#)
- › [Kirche, Diakonie, Caritas – DSG-EKD, KDG, MAV](#)

Wenn du diese Entscheidung nicht allein treffen willst: Die Modellwahl, die Delegationsstruktur und die Vereinbarungen dahinter sind Gegenstand der [Microsoft-365-Beratung für kirchliche Träger](#). Für die Menschen, die anschließend damit arbeiten, gibt es [Microsoft-365-Schulungen für kirchliche Träger](#).