

Ehrenamtliche in Microsoft 365: Gastzugang, eigene Konten, geteilte Postfächer oder besser gar nichts?

Es gibt in jedem kirchlichen Tenant eine Zahl, die niemand kennt und die jeder fürchtet: die Zahl der Menschen, die Zugriff haben, aber in keiner Personalliste stehen. Ehrenamtliche. Presbyterinnen und Presbyter, Mitglieder des Kirchenvorstands, Besuchsdienstkreise, Jugendleiter, Organisten, Lektorinnen, Schatzmeister der Fördervereine. Menschen, ohne die in Kirche, Diakonie und Caritas nichts läuft — und die in der Identitätsverwaltung genau deshalb zum Problem werden, weil sie alles sind, nur nicht angestellt.

Das Ehrenamt hat keinen Dienstvertrag nach AVR, keine Eingruppierung, keine Personalakte und keinen letzten Arbeitstag. Es hat eine Wahl, eine Berufung, manchmal nur einen Satz im Presbyteriumsprotokoll — und irgendwann eine Einladung in ein Team, die jemand freundlicherweise verschickt hat, weil die Unterlagen für die nächste Sitzung sonst wieder per Privatmail herumgehen. Diese Einladung ist der Anfang einer Beziehung, die technisch gesehen ewig dauert, wenn niemand sie beendet.

Die gute Nachricht: Microsoft 365 kennt für dieses Problem vier saubere Antworten. Die schlechte: Drei davon werden in der Praxis falsch eingesetzt, und die vierte — gar kein Zugang — gilt als Rückschritt, obwohl sie häufig die richtige ist. Dieser Beitrag geht die vier Modelle durch, einschließlich der unangenehmen Fragen: Wer meldet eigentlich, dass jemand nicht mehr dabei ist? Wie verlangst du Multifaktorauthentifizierung von Menschen, die kein Diensthandy haben und auch keins bekommen? Und was passiert, wenn niemand diese Fragen beantwortet?

Er gehört zur Reihe [Microsoft 365 in Kirche, Diakonie und Caritas](#) und setzt voraus, dass du die Grundlagen — eigene Rechtsordnung, eigene Aufsicht, eigene Mitbestimmung — nicht mehr erklärt bekommen musst. Wenn doch, ist die Einordnung der Reihe der bessere Startpunkt.

Warum das Ehrenamt jede Identitätsverwaltung sprengt

Kein Personalbüro, kein Eintrittsdatum, kein letzter Arbeitstag

Identitätsverwaltung funktioniert, weil sie eine Quelle der Wahrheit hat. Beim Hauptamt ist das die Personalabteilung: Sie weiß, wann jemand anfängt, wann sich die Stelle ändert und wann Schluss ist. Aus diesen drei Ereignissen leiten sich Konto, Rechte und Sperrung ab. Der Prozess ist langweilig, und genau das ist sein Wert.

Beim Ehrenamt gibt es diese eine Stelle nicht. Es gibt sechs davon, und alle sind ehrenamtlich besetzt. Die Wahl ins Presbyterium steht im Protokoll, das die Schriftführerin schreibt. Die Berufung in den Besuchsdienst ist ein Telefonat mit dem Pfarrer. Der Austritt aus dem Kirchenchor passiert dadurch, dass jemand dreimal nicht zur Probe kommt. Keines dieser Ereignisse erreicht jemals eine IT-Abteilung, und ehrlich gesagt: Warum sollte es auch? Der Mensch, der nach zwanzig Jahren Besuchsdienst aufhört, denkt an vieles, aber nicht an sein Gastkonto im Tenant des Kirchenkreises.

Daraus folgt die einzige Regel, die in diesem gesamten Thema wirklich trägt: Wenn niemand zuverlässig das Ende meldet, darf der Zugang nicht unbefristet sein. Alles andere in diesem Beitrag ist Ausgestaltung dieser einen Regel.

Vier Ehrenämter, vier völlig verschiedene Datenlagen

Das Wort Ehrenamt suggeriert eine Gruppe. Technisch sind es mindestens vier, und sie unterscheiden sich nicht in der Motivation, sondern im Schutzbedarf dessen, was sie in die Hand bekommen.

- **Gremien.** Presbyterium, Kirchenvorstand, Pfarrgemeinderat, Kirchenverwaltung, Kreissynodalvorstand, Verwaltungsrat eines diakonischen Trägers. Diese Menschen sehen Bauakten, Haushaltspläne, Kollektenabrechnungen, Vergabeentscheidungen — und in Personalausschusssitzungen auch Bewerbungen, Eingruppierungen und Abmahnungen. Ein Presbyteriumsmitglied hat damit zeitweise Zugriff auf Personaldaten, ohne jemals eine Verschwiegenheitserklärung aus einem Arbeitsvertrag unterschrieben zu haben.
- **Besuchs- und Seelsorgedienste.** Geburtstagslisten aus dem Meldewesen, Adressen von Kranken und Trauernden, Notizen über Gespräche. Hier liegt die Grenze zum Seelsorgegeheimnis, und sie liegt näher, als den Beteiligten bewusst ist.
- **Kinder- und Jugendarbeit.** Teilnehmerlisten von Freizeiten mit Geburtsdaten, Notfallkontakten, Medikamentenplänen, Allergien, Schwimmerlaubnis und gelegentlich dem Hinweis, dass ein Kind nicht mit dem Vater telefonieren darf. Das sind Gesundheitsdaten und Angaben über Minderjährige in einem Dokument, das auf einem privaten Laptop liegt, weil es dort am schnellsten auszudrucken war.
- **Kirchenmusik, Technik, Fördervereine.** Probenpläne, Notenarchive, Chorlisten, Spendenquittungen. Überwiegend harmlos — bis zur Liste mit Bankverbindungen der Mitglieder.

Ehrenamtsfeld	Typische Daten	Schutzbedarf	Sinnvolles Modell
Gremien	Protokolle, Haushalt, Bau, Kollekten, zeitweise Personalsachen	hoch, in Personalsachen sehr hoch	Gastkonto mit Amtszeit-Befristung, Personalsachen in getrenntem Bereich
Besuchsdienst	Adressen, Geburtstage, Gesprächsnotizen nahe am Seelsorgegeheimnis	hoch	Kein Zugang zu Notizen, nur abgestimmte Listen — oder eigenes Konto bei fester Einbindung
Kinder- und Jugendarbeit	Teilnehmerlisten, Notfallkontakte, Gesundheitsangaben Minderjähriger	sehr hoch	Eigenes Konto oder streng befristetes Gastkonto je Freizeit, nie Freigabelink
Kirchenmusik, Technik, Vereine	Probenpläne, Noten, Mitgliederlisten, Bankverbindungen	mittel	Geteiltes Postfach und Freigabelinks reichen meistens
Einmalige Mitwirkung	Programmheft, Plakat, Gemeindebrief, Gemeindefest	niedrig	Freigabelink mit Ablauf oder bewusst gar kein Zugang

Das Ehrenamt ist keine Nutzergruppe, sondern mindestens fünf — mit vier verschiedenen Antworten.

Was hier wirklich kirchenspezifisch ist — und was nicht

Dass Ehrenamtliche IT-Zugang brauchen, ist keine kirchliche Besonderheit; das kennt jeder Sportverein und jede freiwillige Feuerwehr. Kirchlich sind drei Dinge. Erstens die Menge: In der evangelischen Kirche engagierten sich im Berichtsjahr 2024 rund 886.000 Menschen ehrenamtlich — auf jede hauptamtliche Arbeitskraft der verfassten Kirche kommen damit etwa vier Freiwillige. Zweitens die Rechtslage: Nicht die Datenschutz-Grundverordnung und das Landesdatenschutzgesetz gelten, sondern das [DSG-EKD verständlich: Was das evangelische Datenschutzgesetz für Microsoft 365 konkret bedeutet](#) beziehungsweise das [KDG verständlich: Microsoft 365 unter dem Kirchlichen Datenschutzgesetz der katholischen Kirche](#), mit eigener Aufsicht: dem Beauftragten für den Datenschutz der EKD auf der einen, den regionalen Diözesandatenschutzbeauftragten und dem Katholischen Datenschutzzentrum auf der anderen Seite. Drittens der Schutzbedarf: Kaum ein Verein gibt seinen Ehrenamtlichen Zugriff auf Daten aus Pflege, Beratung, Jugendhilfe oder Seelsorge.

Alles andere ist normales Microsoft 365. Ein Gastkonto verhält sich im Landeskirchenamt genauso wie im Maschinenbau, und die Ablaufsteuerung eines Freigabelinks interessiert sich nicht dafür, ob das Dokument eine Kollektenabrechnung oder eine Lieferantenliste ist. Wer die Unterschiede dort zieht, wo sie wirklich bestehen, spart sich viel Aufwand — nachzulesen in [Microsoft 365 in Kirche, Diakonie und Caritas: Was wirklich anders ist als in Kommune und Mittelstand](#).

Fakten: Größenordnungen

Evangelische Kirche: rund 886.000 ehrenamtlich tätige Menschen im Berichtsjahr 2024, davon gut zwei Drittel Frauen. Auf jede hauptamtliche Arbeitskraft der verfassten Kirche kommen etwa vier Ehrenamtliche.

Caritas: rund 770.000 berufliche Mitarbeiterinnen und Mitarbeiter in etwa 25.000 Einrichtungen und Diensten (Erhebung 2026, Stichtag 31. Dezember 2024) — dazu mehrere hunderttausend Ehrenamtliche. Die lange genannte Zahl von 500.000 war eine Schätzung; eine belastbare Gesamtzahl gibt es bis heute nicht.

Praktische Folge: In einem Kirchenkreis oder einem Caritasverband auf Kreisebene übersteigt die Zahl potenzieller Ehrenamtskonten die Zahl der Beschäftigtenkonten regelmäßig um ein Vielfaches. Wer Ehrenamt pauschal wie Hauptamt behandelt, verdoppelt nicht die Nutzerzahl, sondern verfünffacht sie.

Vier Wege, Ehrenamtliche an kirchliche Daten zu lassen

Dieselbe Person, dieselbe Aufgabe, vier grundverschiedene Spuren im Tenant — und vier Arten, das Aufräumen zu vergessen.

A GASTKONTO (B2B)	B EIGENES KONTO	C POSTFACH UND LINK	D BEWUSST KEIN ZUGANG
- Eigene Identität im Verzeichnis, Anmeldung mit privater Adresse oder mit vorhandenem Arbeitskonto - Bedingter Zugriff, MFA und Protokollierung greifen wie bei eigenen Konten - Kein Postfach, kein OneDrive im Tenant - Abrechnung nach monatlich aktiven Nutzern, keine Microsoft-365-Lizenz nötig - Risiko: Einladungen ohne Ablaufdatum, Wildwuchs durch einladende Teambesitzer	- Kirchliche Identität, kirchliche Adresse, volle Steuerbarkeit - Postfach, Teams, Dateien — je nach Plan auch nur Kalender ohne Postfachrechte - Vertraulichkeitsbezeichnungen und Aufbewahrung greifen vollständig - Kosten je Konto, Verwaltungsaufwand, Kennwortzurücksetzung - Risiko: 300 zusätzliche Konten sind 300 zusätzliche Ziele für Phishing	- Geteiltes Postfach: Funktionsadresse für ein Team, Anmeldung standardmäßig gesperrt - Setzt ein vorhandenes Konto voraus — also kein eigener Zugangsweg - Freigabelink: Datei statt Konto, Ablauf und Leserecht konfigurierbar - Bei Links für jedermann ist nicht nachvollziehbar, wer zugegriffen hat - Risiko: der weitergeleitete Link, der drei Jahre lebt	- Papier, Telefon, Sitzung, Abholung im Pfarramt - Kein Konto, keine Spur, kein Lebenszyklus — nichts zu widerrufen - Richtig überall dort, wo die Daten ohnehin nicht in die Cloud gehören - Nur tragfähig, wenn es einen benannten anderen Weg gibt - Risiko: die private Messenger-Gruppe mit der Teilnehmerliste als Foto

Die Entscheidung fällt nicht zwischen sicher und unsicher, sondern zwischen nachvollziehbar und unauffindbar. A und B hinterlassen eine Identität, die du prüfen und entziehen kannst. C hinterlässt einen Link. D hinterlässt nichts — oder alles, nur woanders.

Ehrenamt in Microsoft 365 — Modellvergleich

Vier Modelle, vier Spuren im Tenant — und vier verschiedene Arten, das Aufräumen zu vergessen.

Die vier Modelle im Klartext

Modell A: Gastkonto über B2B-Zusammenarbeit

Beim Gastkonto lädst du eine externe Adresse in deinen Tenant ein. Es entsteht ein Eintrag im Verzeichnis mit dem Typ Gast; die Person meldet sich weiterhin mit ihrer eigenen Identität an. Wer ein Arbeits- oder Schulkonto bei Microsoft Entra hat, authentifiziert sich direkt beim eigenen Arbeitgeber — praktisch für das Presbyteriumsmitglied, das hauptberuflich in einem Unternehmen arbeitet, das ebenfalls Microsoft 365 nutzt. Alle anderen bekommen eine Einmalkennung per E-Mail. Nach der Aufnahme in ein Team kann es bis zu zwölf Stunden dauern, bis der Zugriff vollständig funktioniert — eine Erfahrung, die zuverlässig am Abend vor der Sitzung gemacht wird.

Der entscheidende Vorteil: Es ist eine echte Identität. Bedingter Zugriff greift, Mehrfaktorauthentifizierung greift, die Anmeldung steht im Protokoll, und der Zugang lässt sich mit einem Klick entziehen. Ein Gastkonto kostet keine Microsoft-365-Lizenz; die Abrechnung für externe Identitäten erfolgt nach monatlich aktiven Nutzern mit einem kostenfreien Kontingent, in dem sich die allermeisten kirchlichen Träger bewegen. Gastkonten sind in Teams sichtbar gekennzeichnet, und der Kanal zeigt an, dass Gäste dabei sind.

Die Nachteile sind ebenso klar. Ein Gast hat kein Postfach und kein OneDrive in deinem Tenant — er arbeitet an deinen Dateien, aber seine Arbeitsablage bleibt seine. Die Einladung geht an eine private Adresse, was zwangsläufig bedeutet, dass Betreffzeilen und Benachrichtigungen bei einem Anbieter landen, mit dem du keinen Vertrag hast. Und das größte Problem ist organisatorisch: Wenn jeder Teambesitzer einladen darf, wächst die Gastliste schneller als jede Übersicht. Die Berechtigung zum Einladen ist eine eigene Rolle im Verzeichnis — nutze sie, statt das Einladen allen zu erlauben oder allen zu verbieten.

Modell B: Eigenes Mitgliedskonto mit Frontline-Lizenz

Das andere Extrem: Die ehrenamtlich tätige Person bekommt eine kirchliche Identität mit kirchlicher Adresse. Damit greift alles, was du sonst auch einsetzt —

Vertraulichkeitsbezeichnungen, Aufbewahrungsrichtlinien, Gerätebedingungen, Protokollierung. Für Menschen, die regelmäßig mit Klientenbezug arbeiten, ist das der einzige Weg, der sauber trägt; siehe [Klientendaten in Diakonie und Caritas: Sozialdaten, Schweigepflicht und Schutz mit Microsoft Purview](#).

Der Kostenhebel heißt Frontline. Die F-Pläne sind deutlich günstiger als die E-Pläne, unterscheiden sich aber erheblich: Der kleinste Plan enthält keine Postfachrechte — ein Postfach wird technisch bereitgestellt, damit der Teams-Kalender funktioniert, genutzt werden darf es nicht. Erst der nächstgrößere Plan bringt ein Postfach mit zwei Gigabyte, erreichbar über Outlook im Browser, ohne Archivpostfach. Für eine Jugendleiterin, die einen Dienstplan und eine Teilnehmerliste braucht, reicht das. Für den Schatzmeister, der drei Jahre Korrespondenz aufbewahren will, nicht. Welche Pläne kirchliche Träger überhaupt beziehen dürfen und wo die Nonprofit-Angebote greifen, steht in [Microsoft-365-Lizenzierung für kirchliche Träger: Nonprofit-Angebote, Frontline-Pläne und die Frage der Berechtigung](#).

Was in Kalkulationen gern vergessen wird: Die Lizenz ist der kleinere Teil der Kosten. Der größere sind Kennwortzurücksetzungen, Anrufe im Pfarrbüro, Einweisung und das Aufräumen. Und sicherheitstechnisch gilt: Dreihundert zusätzliche Konten sind dreihundert zusätzliche Angriffsflächen, von denen viele auf privaten Geräten ohne Verwaltung genutzt werden. Ein eigenes Konto ist nicht per se sicherer als ein Gastkonto — es ist nur besser steuerbar, wenn du die Steuerung auch einrichtest.

Modell C: Geteilte Postfächer und Freigabelinks

Hier lohnt sich eine Klarstellung, die in Konzepten erstaunlich oft fehlt: Ein geteiltes Postfach ist kein Zugangsweg. Es ist ein Postfach ohne eigene Anmeldung — neu angelegte geteilte Postfächer haben die Anmeldung standardmäßig gesperrt —, auf das Personen mit einem bestehenden Konto zugreifen. Wer kein Konto hat, kommt auch nicht an das geteilte Postfach. Es löst also die Frage nach der Funktionsadresse, nicht die Frage nach dem Zugang.

Trotzdem ist es ein gutes Werkzeug: Die Adresse des Besuchsdienstes, des Kirchenchors oder der Freizeitanmeldung gehört dem Träger und nicht der Person, die sie gerade betreut. Wechselt die Zuständigkeit, wechselt die Berechtigung, und der Verlauf bleibt, wo er hingehört. Geteilte Postfächer benötigen in der Regel keine eigene Lizenz; eine wird erst fällig, wenn das Postfach mehr als 50 Gigabyte belegt, ein Archivpostfach nutzt oder unter Beweissicherung gestellt wird.

Wirklich eigenständig ist dagegen der Freigabelink. Er ersetzt das Konto durch ein Dokument. Auf Organisationsebene stehen vier Stufen zur Wahl: Freigabe für jedermann ohne Anmeldung, für neue und vorhandene Gäste, nur für vorhandene Gäste oder ausschließlich intern. Einzelne Websites dürfen strenger eingestellt sein als die Organisation, nie lockerer. Links für jedermann lassen sich auf Leserecht beschränken und mit einem Ablauf in Tagen versehen — was du unbedingt tun solltest, denn bei diesen Links lässt sich nicht nachvollziehen, wer Zugriff hat und wer zugegriffen hat. Ein Link ohne Ablauf ist ein Gastkonto ohne Gesicht.

Für Gemeindebriefentwürfe, Plakate und Programmhefte ist das völlig in Ordnung. Für eine Teilnehmerliste ist es das nicht. Wie sich diese Stufen in eine belastbare Websitestruktur einfügen, beschreibt [SharePoint-Informationsarchitektur für Kirchengemeinde und Kirchenkreis](#).

Modell D: Bewusst kein Zugang

Das unterschätzte Modell. Kein Konto, kein Link, keine Einladung — stattdessen die ausgedruckte Tagesordnung, der Anruf aus dem Pfarramt, die Mappe, die im Gemeindebüro abgeholt wird. Das klingt nach 1995 und ist in vielen Fällen die beste Entscheidung: Es gibt nichts zu widerrufen, nichts zu überprüfen, nichts zu vergessen. Wer zweimal im Jahr eine Sitzungsvorlage liest, braucht kein Konto in einem Tenant.

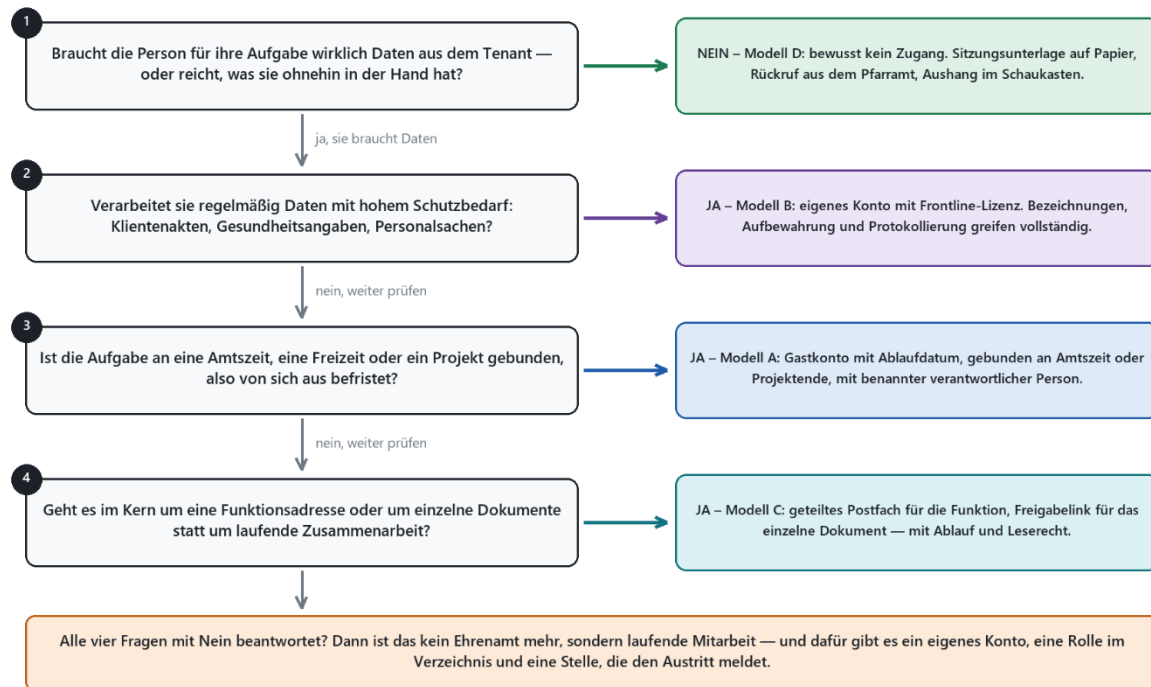
Aber — und das ist der Haken — kein Zugang ist nur dann eine Entscheidung, wenn es einen benannten anderen Weg gibt. Fehlt der, entsteht der Weg von selbst, und er heißt dann privater Messenger, privates Postfach oder das Foto der Teilnehmerliste auf dem Handy des Jugendleiters. Die Verweigerung von Zugang ohne Alternative ist keine Datensparsamkeit, sondern eine Verlagerung des Risikos an einen Ort, an dem du es weder sehen noch beenden kannst.

Modell	Kontrolle	Aufwand	Datenschutz	Passt für
A — Gastkonto (B2B)	Hoch: bedingter Zugriff, MFA, Protokoll, Entzug in Sekunden, Zugriffsüberprüfungen möglich	Mittel: Einladung, Genehmigung, Befristung, Überprüfung	Gut steuerbar; Schwachpunkt sind Benachrichtigungen an private Adressen und Wildwuchs bei freiem Einladungsrecht	Gremien mit Amtszeit, Projektmitarbeit, Bauausschuss, Fach- und Arbeitskreise
B — Eigenes Konto mit Frontline-Lizenz	Sehr hoch: volle Steuerung wie beim Hauptamt, Bezeichnungen und Aufbewahrung greifen	Hoch: Lizenzkosten, Betreuung, Kennwortzurücksetzung, Einweisung	Stärkster Schutz, solange der Austritt zuverlässig gemeldet wird — sonst das gefährlichste Modell	Dauerhaft eingebundene Ehrenamtliche mit Klienten-, Gesundheits- oder Personalbezug
C — Geteiltes Postfach und Freigabelink	Postfach hoch, Link niedrig: bei Links für jedermann ist der Zugriff nicht nachvollziehbar	Niedrig: schnell eingerichtet, schnell vergessen	Tragfähig für Funktionsadressen; bei Links nur mit Ablauf und Leserecht vertretbar	Funktionsadressen, Gemeindebrief, Plakate, Probenpläne, einzelne Dokumente
D — Bewusst kein Zugang	Vollständig, solange es einen benannten anderen Weg gibt	Niedrig in der IT, höher im Pfarramt — jemand muss drucken, kuvertieren, anrufen	Beste Variante für alles, was ohnehin nicht in die Cloud gehört; ohne Alternative entsteht Schatten-IT	Seltene Mitwirkung, Seelsorgenahes, alles mit sehr kleinem Umfang

Die Wahl fällt nicht einmal für den ganzen Träger, sondern je Aufgabe — und sie darf sich ändern, wenn sich die Aufgabe ändert.

Welches Modell passt? Vier Fragen vor dem ersten Konto

Der Weg ganz nach unten ist der teure. Wer früh abbiegt, spart sich den halben Lebenszyklus.



Ehrenamt in Microsoft 365 — Modellauswahl

Vier Fragen vor dem ersten Konto. Wer früh abbiegt, spart sich den halben Lebenszyklus.

Fakten: Technische Eckwerte, die Diskussionen abkürzen

Gastkonten benötigen keine Microsoft-365-Lizenz. Externe Identitäten werden nach monatlich aktiven Nutzern abgerechnet, mit kostenfreiem Kontingent.

Nach dem Hinzufügen eines Gastes zu einem Team kann es bis zu zwölf Stunden dauern, bis alle Funktionen bereitstehen.

Wer kein Arbeits- oder Microsoft-Konto hat, bestätigt die Einladung über eine Einmalkennung per E-Mail.

Geteilte Postfächer haben die Anmeldung standardmäßig gesperrt und brauchen erst ab 50 Gigabyte Belegung, bei Nutzung eines Archivpostfachs oder bei Beweissicherung eine eigene Lizenz.

Der kleinste Frontline-Plan enthält keine Postfachrechte; der nächstgrößere bringt zwei Gigabyte Postfach ohne Archiv.

Der Gastzugang in Teams ist eine organisationsweite Einstellung. Pro Team steuerst du ihn über Vertraulichkeitsbezeichnungen.

Diese letzte Zeile ist wichtiger, als sie aussieht: Sie ist der Unterschied zwischen „Gäste erlaubt“ und „Gäste erlaubt, aber nicht im Team des Personalausschusses“. Wie ein Bezeichnungskonzept vom Gemeindebrief bis zur Beratungsakte aussieht, steht in [Sensitivity Labels für kirchliche Träger: Ein Label-Konzept vom Gemeindebrief bis zur Beratungsakte](#).

Wichtig: Wo das Modell egal ist, weil die Daten gar nicht in Frage kommen

Seelsorge- und Beichtgeheimnis kennen keine Abstufung nach Kontotyp. Gesprächsnotizen aus der Seelsorge gehören weder in ein Team mit Gästen noch in ein Team ohne Gäste, weder in OneNote noch in ein geteiltes Postfach — und schon gar nicht in einen Index, den ein Assistenzsystem durchsuchen

kann.

Beim Besuchsdienst verläuft die Grenze mitten durch die Aufgabe: Die Liste, wer wann Geburtstag hat, ist Organisation. Was im Gespräch gesagt wurde, ist es nicht.

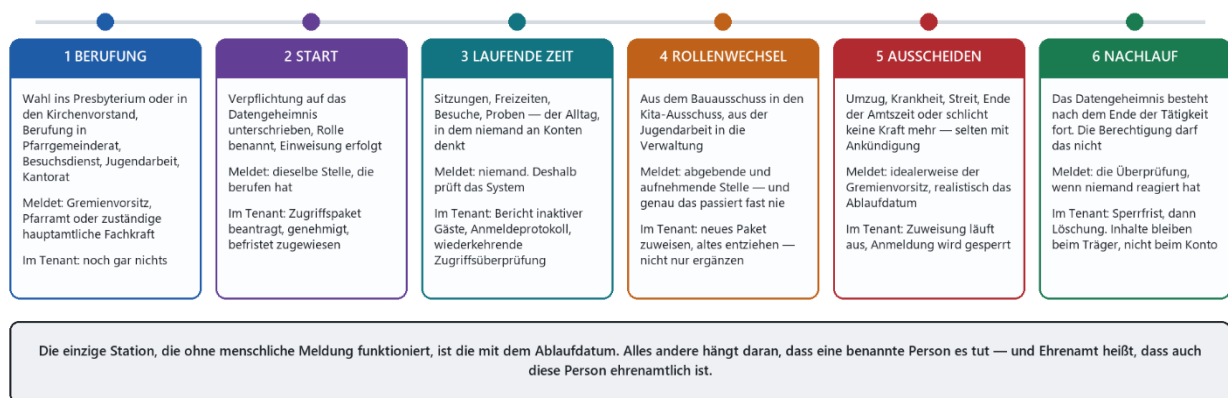
Ausführlich dazu: [Seelsorgegeheimnis und Beichtgeheimnis in Microsoft 365: Was nie in Teams, OneNote oder Copilot landen darf.](#)

Der Lebenszyklus: Eintritt, Rollenwechsel, Austritt — und wer das meldet

Die Modellwahl ist die einfache Hälfte. Die schwierige ist der Betrieb über Jahre, und der scheitert fast immer an derselben Stelle: Niemand fühlt sich zuständig für das Ende.

Der Ehrenamts-Lebenszyklus — und die Frage, wer meldet

Beim Hauptamt erledigt das die Personalabteilung. Beim Ehrenamt gibt es keine Personalabteilung, also braucht jede Station einen Namen.



Ehrenamt in Microsoft 365 — Lebenszyklus

Sechs Stationen — und für jede die Frage, wer sie meldet. Nur eine funktioniert ohne Menschen.

Eintritt: ohne benannte verantwortliche Person kein Zugang

Die wirksamste Maßnahme im gesamten Thema kostet keine Lizenz: Für jede ehrenamtliche Rolle wird eine hauptamtliche oder zumindest namentlich benannte Stelle festgelegt, die Zugänge beantragt, genehmigt und bestätigt. Für Gremien ist das der Vorsitz oder das Pfarramt, für die Jugendarbeit die hauptamtliche Fachkraft, für die Kirchenmusik das Kantorat, für einen diakonischen Träger die Einrichtungsleitung. Kein Zugang ohne Namen — und zwar ohne Ausnahme, auch nicht kurz vor der Sitzung.

Diese Person bestätigt zugleich, dass die Verpflichtung auf das Datengeheimnis vorliegt. Damit koppelst du die rechtliche Voraussetzung an den technischen Vorgang, statt beides getrennt zu führen und am Ende weder das eine noch das andere nachweisen zu können.

Rollenwechsel: der Rechte-Rucksack

Ehrenamtliche wechseln häufiger die Rolle als die Organisation. Aus dem Bauausschuss geht es in den Kita-Ausschuss, aus der Jugendarbeit in den Kreissynodalvorstand, aus dem Förderverein in den Verwaltungsrat. Jeder dieser Wechsel fügt Rechte hinzu. Fast keiner nimmt welche weg. Nach

acht Jahren Engagement hat eine einzelne Person Zugriff auf fünf Teams, von denen sie zwei nutzt und drei vergessen hat — und in einem davon liegen Protokolle des Personalausschusses.

Technisch löst du das über rollenbezogene Zugriffspakete statt über Einzeleinladungen: Das Paket „Kirchenvorstand St. Beispiel“ enthält die Mitgliedschaften, die zu dieser Rolle gehören. Endet die Rolle, endet das Paket, und mit ihm die Mitgliedschaften. Wer in ein anderes Gremium wechselt, beantragt ein neues Paket — und verliert das alte automatisch. Organisatorisch löst du es dadurch, dass die abgebende Stelle den Wechsel meldet und nicht nur die aufnehmende.

Austritt: das Ablaufdatum ist die einzige Meldung, die immer kommt

Gremien haben etwas, das die meisten Ehrenämter nicht haben: eine Amtszeit. Presbyterium, Kirchenvorstand und Pfarrgemeinderat werden für feste Perioden gewählt, Ausschüsse werden für die Dauer der Amtsperiode besetzt. Das ist das beste Ablaufdatum, das du bekommen kannst, und es steht in der Kirchenordnung, nicht in deiner Konfiguration. Setze die Gültigkeit der Zuweisung auf das Ende der Amtsperiode — nicht auf unbefristet, nicht auf „bis auf Weiteres“. Wer wiedergewählt wird, verlängert; wer nicht, verschwindet von selbst. Wie sich Gremienarbeit sauber in Teams abbilden lässt, steht in [Gremienarbeit in Microsoft Teams: Presbyterium, Kirchenvorstand, Pfarrgemeinderat und Synode digital](#).

Für alles ohne natürliche Frist gilt eine Ersatzregel: Eine Freizeit endet mit der Rückkehr, ein Projekt mit dem Abschlussbericht, ein Arbeitskreis mit dem Jahresende. Und wo auch das nicht passt, setzt du schlicht zwölf Monate an. Eine jährliche Bestätigung durch die verantwortliche Person ist zumutbar; ein Zugang, der fünf Jahre läuft, ohne dass jemand hinsieht, ist es nicht.

Zugriffsüberprüfungen — mit und ohne Governance-Lizenz

Microsoft Entra bietet dafür fertige Werkzeuge. Der Bericht über inaktive Gäste zeigt, wer sich seit einem einstellbaren Schwellenwert — voreingestellt sind 90 Tage — nicht mehr angemeldet hat; bei Konten, die sich nie angemeldet haben, zählt das Erstellungsdatum. Zugriffsüberprüfungen lassen sich wiederkehrend einrichten, wahlweise mit Selbstauskunft der Betroffenen in einer ersten Stufe und einer Entscheidung der verantwortlichen Person in einer zweiten. Entscheidend sind zwei Einstellungen: Reagiert niemand, wird der Zugriff entzogen — nicht verlängert. Und abgelehnte Gastkonten werden für 30 Tage gesperrt und anschließend aus dem Verzeichnis entfernt; wiederherstellbar bleiben sie danach noch einmal 30 Tage, dann braucht es eine neue Einladung.

Ehrlichkeit an dieser Stelle: Zugriffsüberprüfungen und die Berechtigungsverwaltung mit Zugriffspaketen setzen Lizenzen für Microsoft Entra ID Governance beziehungsweise die Entra Suite voraus. Die hat nicht jede Kirchengemeinde, und für einen Träger mit überwiegend Frontline-Arbeitsplätzen ist das eine echte Investitionsentscheidung. Ohne diese Lizenzen bleibt der Weg über Bordmittel: eine regelmäßig erzeugte Liste aller Gastkonten mit einladender Person und letzter Anmeldung, halbjährlich an die Verantwortlichen, Rückmeldefrist vier Wochen, keine Antwort bedeutet Sperrung. Das funktioniert — solange es jemand tut.

Vom Antrag bis zur Löschung: Zugang mit Verfallsdatum

Oben die Kette mit Governance-Werkzeugen, unten dieselbe Kette mit Tabelle und Disziplin. Beide funktionieren — eine davon auch im Advent.



Mit Berechtigungsverwaltung und Zugriffsüberprüfungen läuft diese Kette automatisch, einschließlich der Regel, dass ein nicht bestätigter Zugang erst gesperrt und dann gelöscht wird. Das setzt Governance-Lizenzen voraus.

Ohne diese Lizenzen: eine Liste aller Gastkonten mit einladender Person und letzter Anmeldung, halbjährlich an die Gremienvorsitze, Rückmeldefrist vier Wochen, keine Antwort bedeutet Sperrung.

Der Unterschied liegt nicht im Ergebnis, sondern in der Wahrscheinlichkeit: Die automatische Kette läuft auch im Advent. Die manuelle Liste wandert im Advent nach unten.

Ehrenamt in Microsoft 365 — Zugriffsüberprüfung

Dieselbe Kette, zwei Umsetzungen: automatisiert oder diszipliniert. Der Unterschied zeigt sich im Advent.

Tipp: Drei Stellschrauben, die sofort wirken

Einladungsrecht einschränken: Nur eine benannte Rolle darf Gäste einladen, nicht jeder Teambesitzer. Das kostet nichts und halbiert die Gastliste innerhalb eines Jahres.

Gastablauf je Website aktivieren: Der Zugriff von Gästen auf eine SharePoint-Website oder ein OneDrive kann nach einer festgelegten Zahl von Tagen automatisch enden.

Ablauf für Links für jedermann erzwingen und diese Links auf Leserecht beschränken. Standard-Linktyp im ganzen Tenant auf „bestimmte Personen“ setzen — der Klick, der am meisten Oversharing verhindert.

Warnung: Aus der Praxis: zwei Jahre zu lange im Team

Ein Kirchenkreis in einer Großstadt betreibt die Jugendarbeit seiner Gemeinden über ein gemeinsames Team. Darin liegen die Anmeldungen der Sommerfreizeiten: Geburtsdaten, Notfallkontakte, Medikamentenpläne, Allergien, Angaben zu Therapien. Ein ehrenamtlicher Jugendleiter war als Gast eingeladen worden — ordentlich, mit Verpflichtung auf das Datengeheimnis, mit Einweisung, alles richtig gemacht.

Zwei Jahre nach seinem Wegzug in eine andere Stadt und dem Ende seiner Mitarbeit hatte er das Team noch immer in seiner Teams-App, auf dem privaten Telefon, einschließlich aller Listen der beiden Folgejahre. Aufgefallen ist es, weil er sich meldete: Er wollte wissen, ob das so richtig sei. Die ehrlichste Antwort auf diese Frage ist die unangenehmste — er war der Einzige, dem es aufgefallen ist.

Was gefehlt hat, war keine Technik, sondern drei Kleinigkeiten: ein Ablaufdatum an der Einladung, ein benannter Verantwortlicher für das Team und eine jährliche Überprüfung der Gastliste. Was zusätzlich gefehlt hat: die Trennung zwischen dem Dauerteam der Jugendarbeit und dem Team je Freizeit, das nach der Abrechnung archiviert wird.

Rechtlich war es eine Verarbeitung ohne Rechtsgrundlage — die Berechtigung bestand fort, der Zweck nicht. Ob daraus eine meldepflichtige Panne wird, entscheidet der Einzelfall; die Bewertung gehört in die Hände der örtlich Beauftragten und im Zweifel der Aufsicht.

Wie die Aufsichten auf solche Sachverhalte blicken und was sie typischerweise als Erstes sehen wollen, steht in [Kirchliche Datenschutzaufsicht in der Praxis: Was BfD EKD und](#)

[Diözesandatenschutzbeauftragte erwarten](#). Und was nach dem Ende eines Engagements mit den Inhalten passiert — nicht mit dem Konto, sondern mit den Dokumenten —, gehört in das Aufbewahrungskonzept: [Kirchliche Aufbewahrungsfristen, Kassationsordnungen und Archivgesetze in Microsoft Purview abbilden](#).

MFA auf Privatgeräten, Datengeheimnis und die Grenzen der Zumutbarkeit

Zwei Faktoren ohne Diensthandy

Der häufigste Einwand aus der Gemeinde lautet: „Das können wir den Ehrenamtlichen nicht zumuten.“ Der häufigste Einwand aus dem Presbyterium lautet: „Ich installiere dafür nichts auf meinem privaten Telefon.“ Beide Einwände sind ernst zu nehmen, und beide führen nicht zu dem Schluss, dass Ehrenamt ohne zweiten Faktor auskommt. Ein Zugang ohne zweiten Faktor ist heute ein Zugang mit Ansage.

Der Ausweg besteht aus mehreren Wegen statt einem. Die Authentifizierungs-App auf dem privaten Telefon ist der bequemste, und das wichtigste Argument dafür ist ein Missverständnis, das du ausräumen musst: Eine App für die Anmeldebestätigung verwaltet das Gerät nicht. Sie sieht keine Fotos, liest keine Nachrichten und erlaubt niemandem, das Telefon zu löschen. Wer es trotzdem nicht will, bekommt einen Sicherheitsschlüssel zum Anstecken — ein Gegenstand, kein Eingriff, und gleichzeitig die stabilste Variante für Menschen ohne Smartphone. Zehn dieser Schlüssel im Schreibtisch des Pfarramts lösen mehr Diskussionen als drei Informationsabende.

Tipp: Faustregel für die Diskussion im Gremium

Wer digitalen Zugang zu Daten anderer Menschen bekommt, übernimmt Verantwortung für diese Daten. Der zweite Faktor ist der Preis dafür, und er ist niedriger als der Schlüssel zum Gemeindehaus, den dieselbe Person selbstverständlich unterschreibt und zurückgibt.

Wer weder App noch Schlüssel will, bekommt keinen Zugang — und für diesen Fall gibt es Modell D. Das ist keine Strafe, sondern eine Wahl.

Das Privatgerät bleibt privat

Ehrenamtliche arbeiten auf ihren eigenen Geräten. Der Versuch, diese Geräte in die Geräteverwaltung aufzunehmen, ist in den meisten Fällen unverhältnismäßig und politisch chancenlos — mit gutem Grund: Ein Träger, der das Telefon einer ehrenamtlich tätigen Person verwaltet, greift auf eine Weise ein, die zu einem unentgeltlichen Engagement nicht passt.

Der bessere Weg führt über die Anwendung statt über das Gerät: Zugriff nur über den Browser ohne die Möglichkeit, Dateien herunterzuladen; Synchronisierung auf nicht verwaltete Geräte unterbinden; Anwendungsschutzrichtlinien für die mobilen Apps, die Kopieren in private Apps verhindern und einen eigenen PIN-Schutz für den dienstlichen Bereich verlangen; kürzere Sitzungsdauern für Gäste als für Beschäftigte. Damit bleibt das Gerät privat und die Daten bleiben es nicht.

Zwei Ausschlüsse gehören in jede Regelung: keine Weitergabe von Dateien aus kirchlichen Bereichen in private Ablagen, und kein Zugriff auf Assistenz- oder KI-Funktionen für Gastkonten

— nicht, weil die Technik schlecht wäre, sondern weil das, was ein Assistenzsystem zusammenstellt, immer nur so gut abgegrenzt ist wie die Berechtigungen darunter. Bei einem über Jahre gewachsenen Rechte-Rucksack ist das kein beruhigender Gedanke.

Die Verpflichtung auf das Datengeheimnis

Beide kirchlichen Datenschutzgesetze verlangen, dass Personen, die personenbezogene Daten verarbeiten, bei Aufnahme ihrer Tätigkeit schriftlich auf das Datengeheimnis verpflichtet werden. Evangelisch steht das im DSG-EKD unter der Überschrift Datengeheimnis in Paragraph 26, katholisch im KDG in Paragraph 5 — dort ausdrücklich mit dem Zusatz, dass dies auch für ehrenamtlich tätige Personen gilt, soweit sie personenbezogene Daten verarbeiten. In beiden Rechtskreisen gilt: Das Datengeheimnis besteht nach dem Ende der Tätigkeit fort. Die Landeskirchenämter, Generalvikariate und Datenschutzzentren veröffentlichen dafür Musterformulare einschließlich Merkblättern; du musst nichts erfinden.

Praktisch scheitert es nicht am Formular, sondern an der Ablage. Drei Regeln helfen: Die Verpflichtung wird vor der Kontoerstellung unterschrieben, nicht danach. Sie wird dort abgelegt, wo sie zwei Jahre später noch gefunden wird — beim Träger, nicht im Ordner der Person, die damals das Gremium geleitet hat. Und sie wird bei einem Rollenwechsel in einen Bereich mit höherem Schutzbedarf wiederholt, verbunden mit einer kurzen Einweisung. Schweigepflichten aus dem Sozialbereich und Führungszeugnisse aus der Prävention sind davon getrennt zu behandeln: andere Rechtsgrundlage, anderer Zweck, andere Aufbewahrung.

Wichtig: Verpflichtung ist kein Ersatz für Berechtigung

Eine unterschriebene Verpflichtung auf das Datengeheimnis erlaubt nicht die Verarbeitung — sie verpflichtet nur zur Verschwiegenheit. Die Rechtsgrundlage für den Zugriff ergibt sich aus der Aufgabe, und die Reichweite des Zugriffs aus dem, was diese Aufgabe erfordert.

Im Klartext: Das Presbyteriumsmitglied darf die Bauakte sehen, weil es über den Bau entscheidet. Es darf die Personalakte nicht sehen, nur weil es unterschrieben hat, nichts weiterzuerzählen.

Deshalb ist die Trennung der Bereiche wichtiger als jede Erklärung: getrennte Teams für Personal- und Bauausschuss, getrennte Websites, getrennte Zugriffspakete.

Was die Mitarbeitervertretung damit zu tun hat

Ehrenamtliche sind keine Mitarbeiterinnen und Mitarbeiter im Sinne des MVG-EKD oder der MAVO; sie wählen keine MAV und werden von ihr nicht vertreten. Trotzdem gehört das Thema auf den Tisch der Mitarbeitervertretung, und zwar aus einem schlichten Grund: Ehrenamtliche arbeiten in denselben Teams, Kanälen und Postfächern wie die Beschäftigten. Jede Protokollierung, jede Auswertung, jede Anwesenheitsanzeige, die auf Ehrenamtliche zielt, erfasst zwangsläufig auch Hauptamtliche — und genau dort liegt die Mitbestimmung bei der Einführung und Anwendung technischer Einrichtungen, die zur Überwachung von Verhalten oder Leistung geeignet sind: evangelisch in Paragraph 40 MVG-EKD, katholisch in Paragraph 36 Absatz 1 Nummer 9 MAVO.

Praktisch heißt das: Die Dienstvereinbarung zu Microsoft 365 sollte den Umgang mit Ehrenamtskonten ausdrücklich mitregeln — welche Protokolle entstehen, wer sie auswerten darf, wie mit dem Anwesenheitsstatus umgegangen wird und was bei Zugriffsüberprüfungen an wen berichtet wird. Wer das vorher klärt, erspart sich die Diskussion an der Stelle, an der sie am

teuersten ist: mitten im Rollout. Die Verhandlungslinien im Detail stehen in [Mitarbeitervertretung und Microsoft 365: MVG-EKD, MAVO, Dienstvereinbarung und Mitbestimmung](#).

Ein Umsetzungsplan, der im Gemeindealltag überlebt

Der Reiz dieses Themas liegt darin, dass die ersten Schritte kaum etwas kosten und sofort wirken. Die Reihenfolge ist wichtiger als die Vollständigkeit: Zuerst wissen, was da ist. Dann verhindern, dass es weiter wächst. Erst dann aufräumen.

Schritt	Was dabei herauskommt	Wer macht es
1. Bestandsaufnahme	Liste aller Gastkonten mit einladender Person, Einladedatum und letzter Anmeldung; dazu alle Teams ohne aktiven Besitzer und alle Websites mit Links für jedermann	IT-Leitung oder Dienstleister, eine Woche
2. Zuflusssperre	Einladungsrecht auf eine benannte Rolle begrenzt, Standard-Linktyp auf „bestimmte Personen“, Ablauf für Links für jedermann erzwungen	IT-Leitung, ein Nachmittag
3. Verantwortliche benennen	Je Ehrenamtsfeld eine Stelle, die beantragt, genehmigt und bestätigt — schriftlich festgehalten, nicht mündlich vereinbart	Verwaltungsleitung mit Pfarramt, Dekanat oder Einrichtungsleitung
4. Modell je Feld festlegen	Entscheidung nach den vier Fragen, dokumentiert — einschließlich der Felder, die bewusst keinen Zugang bekommen	IT-Leitung, Datenschutzbeauftragte, Fachbereiche
5. Befristung einbauen	Zuweisungen an Amtszeit, Freizeit oder Projekt gekoppelt; wo nichts passt, zwölf Monate	IT-Leitung, gemeinsam mit den Verantwortlichen
6. Überprüfung terminieren	Wiederkehrende Zugriffsüberprüfung oder ein fester Termin im Jahreslauf mit Rückmeldefrist und klarer Folge bei Schweigen	IT-Leitung; Ergebnis an die örtlich Beauftragten
7. Verpflichtung und Einweisung	Unterschiedene Verpflichtung vor Kontoerstellung, kurze Einweisung, Nachweis beim Träger abgelegt	Verantwortliche Stelle je Feld

Sieben Schritte, von denen die ersten beiden zusammen weniger als zwei Tage kosten — und den größten Teil des Risikos abräumen.

Zwei Punkte, an denen Träger regelmäßig stolpern: Erstens die Tenant-Frage. Wenn Kirchenkreis, Gemeinden und ein diakonischer Träger in getrennten Tenants arbeiten, wird aus jedem gemeinsamen Gremium ein Fall für Gastkonten — und aus jeder Ehrenamtsrolle ein Konto in mehreren Tenants. Das ist kein Gegenargument gegen getrennte Tenants, aber ein Kostenfaktor, den man vorher kennen sollte; die Abwägung steht in [Ein Tenant oder viele? Kirchengemeinde, Kirchenkreis, Landeskirche, Bistum und die Frage der Tenant-Architektur](#). Zweitens die Einweisung: Der teuerste Fehler in diesem Thema ist nicht ein falsch gesetztes Recht, sondern eine Person, die nicht weiß, was sie tut. Kurze, konkrete Einweisung für Ehrenamtliche schlägt jede Richtlinie — Formate dafür gibt es unter [Microsoft-365-Schulung für kirchliche Träger](#).

Häufige Fragen

Dürfen Ehrenamtliche überhaupt Zugriff auf kirchliche Daten bekommen?

Ja. Weder DSGVO-EKD noch KDG verbieten das; sie verlangen eine Rechtsgrundlage für die Verarbeitung, eine Begrenzung auf das Erforderliche und die Verpflichtung auf das

Datengeheimnis. Das Ehrenamt ist Teil der Aufgabenerfüllung des Trägers, und wer eine Aufgabe hat, darf die dafür nötigen Daten verarbeiten. Die interessante Frage ist nie, ob überhaupt, sondern wie viel und wie lange.

Reicht eine Einwilligung, oder braucht es die Verpflichtung auf das Datengeheimnis?

Das sind zwei verschiedene Dinge, die oft verwechselt werden. Die Einwilligung betrifft die Daten der ehrenamtlich tätigen Person selbst, etwa die Veröffentlichung ihres Namens im Gemeindebrief. Die Verpflichtung auf das Datengeheimnis betrifft die Daten anderer Menschen, mit denen sie umgeht. Du brauchst die Verpflichtung; ob du zusätzlich eine Einwilligung brauchst, hängt davon ab, was du mit den Daten dieser Person vorhast.

Ist ein Gastkonto mit privater E-Mail-Adresse datenschutzrechtlich vertretbar?

In aller Regel ja — mit zwei Einschränkungen. Erstens landen Benachrichtigungen und Betreffzeilen beim Anbieter dieser Adresse; deshalb gehören sprechende Betreffzeilen mit Klientenbezug nicht in automatische Benachrichtigungen. Zweitens ist die private Adresse kein Ort für Inhalte: Der Gast arbeitet in deinem Tenant, er bekommt dort nichts hingeschickt. Wo regelmäßig sensibler Inhalt verarbeitet wird, ist das eigene Konto der sauberere Weg.

Müssen wir wirklich Multifaktorauthentifizierung verlangen, obwohl niemand ein Diensthandy hat?

Ja — aber du musst nicht auf einer einzigen Methode bestehen. App auf dem privaten Telefon, Sicherheitsschlüssel zum Anstecken oder, in der Reihenfolge der Widerstandsfähigkeit ganz hinten, ein Code per SMS. Wichtig ist die Botschaft, dass eine Authentifizierungs-App das private Gerät nicht verwaltet. Die meisten Bedenken sind Missverständnisse, keine Grundsätze.

Können wir Ehrenamtliche einfach in das bestehende Team des Pfarramts aufnehmen?

Besser nicht. Im Team des Pfarramts liegen Meldedaten, Seelsorgliches, Personalangelegenheiten und Vertrauliches aus dem Alltag. Ein Gast sieht den Inhalt der Kanäle, zu denen er gehört — und die Dateien liegen auf einer gemeinsamen Website. Richtig ist ein eigenes Team je Gremium oder je Aufgabe, mit eigener Website und eigener Vertraulichkeitsbezeichnung. Das ist etwas mehr Arbeit beim Anlegen und deutlich weniger Arbeit beim Erklären.

Was passiert mit den Daten, wenn jemand ausscheidet?

Inhalte gehören dem Träger, nicht dem Konto. Protokolle, Anmeldungen und Abrechnungen bleiben in den Teams und auf den Websites des Trägers und unterliegen dessen Aufbewahrungsregeln — das Ausscheiden einer Person ändert daran nichts. Entzogen wird die Berechtigung, gelöscht wird das Konto. Bei eigenen Konten kommt der Umgang mit dem persönlichen Postfach und OneDrive hinzu: vorher festlegen, wer Inhalte sichtet, was übernommen wird und wann der Rest gelöscht wird.

Brauchen wir für Zugriffsüberprüfungen zwingend Zusatzlizenzen?

Für die automatisierten Verfahren — Zugriffspakete, wiederkehrende Überprüfungen, automatisches Sperren und Löschen — ja, dafür sind Governance-Lizenzen nötig. Für das Ergebnis nein: Eine halbjährliche Liste, eine Rückmeldefrist und die Regel, dass Schweigen zur Sperrung führt, erreichen dasselbe. Die Lizenz kauft dir nicht die Ordnung, sondern die Wahrscheinlichkeit, dass sie auch in einem vollen Dezember eingehalten wird.

Was machen wir mit den Messenger-Gruppen in der Jugendarbeit?

Anerkennen, dass sie existieren, und ihnen die Daten wegnehmen, nicht die Funktion. Absprachen über Uhrzeiten und Treffpunkte in einer privaten Gruppe sind ein überschaubares Problem. Teilnehmerlisten, Fotos von Anmeldebogen und Gesundheitsangaben sind es nicht. Die Regel lautet deshalb nicht „kein Messenger“ — die hält niemand ein —, sondern: keine personenbezogenen Unterlagen außerhalb der kirchlichen Umgebung. Dazu gehört, dass die kirchliche Umgebung auf dem Telefon genauso schnell erreichbar ist wie die private Gruppe.

Fazit

Die Frage aus der Überschrift hat keine einzelne Antwort, und das ist die eigentliche Erkenntnis. Gastkonten sind richtig für Gremien mit Amtszeit und projektbezogene Mitarbeit. Eigene Konten mit Frontline-Lizenz sind richtig, wo dauerhaft mit Klienten-, Gesundheits- oder Personalbezug gearbeitet wird. Geteilte Postfächer sind richtig für Funktionsadressen und Freigabelinks für einzelne Dokumente, sofern sie ablaufen. Und gar kein Zugang ist richtig, wo die Aufgabe ihn nicht braucht — vorausgesetzt, es gibt einen benannten anderen Weg.

Was in allen vier Fällen gleich bleibt: Der Zugang braucht eine verantwortliche Person, ein Ablaufdatum und einen Termin, an dem jemand hinsieht. Der Rest ist Konfiguration. Kirchliche Träger haben für das Ablaufdatum sogar einen Vorteil, den andere nicht haben: Amtszeiten, Wahlperioden und Freizeiten sind von sich aus befristet. Wer die Berechtigung an diese natürlichen Fristen koppelt, hat den Lebenszyklus gelöst, ohne einen einzigen Prozess zu erfinden.

Und wenn du am Ende nur eine Maßnahme umsetzen kannst, dann diese: Zieh die Liste aller Gastkonten deines Tenants mit Einladedatum und letzter Anmeldung. Die Zahl der Zeilen älter als zwei Jahre beantwortet die Frage, wie dringend der Rest ist. Erfahrungsgemäß ist diese Zahl unangenehm — und genau deshalb ist sie ein guter Anfang.

Weiter im Thema: Weiter im Thema

Verwandte Beiträge aus der Reihe:

- › [Gremienarbeit in Microsoft Teams: Presbyterium, Kirchenvorstand, Pfarrgemeinderat und Synode digital](#)
- › [Microsoft-365-Lizenzierung für kirchliche Träger: Nonprofit-Angebote, Frontline-Pläne und die Frage der Berechtigung](#)
- › [Klientendaten in Diakonie und Caritas: Sozialdaten, Schweigepflicht und Schutz mit Microsoft Purview](#)
- › [Sensitivity Labels für kirchliche Träger: Ein Label-Konzept vom Gemeindebrief bis zur Beratungsakte](#)
- › [Mitarbeitervertretung und Microsoft 365: MVG-EKD, MAVO, Dienstvereinbarung und](#)

Mitbestimmung

- › Microsoft 365 in Kirche, Diakonie und Caritas
- › Unterstützung bei Konzept und Umsetzung: Microsoft-365-Beratung für kirchliche Träger