Meldewesen und Gemeindegliederdaten: Warum Kirchenmitgliederdaten getrennt von Microsoft 365 bleiben

Es gibt in jeder Kirchengemeinde diese eine Datei. Sie heißt meistens „Gemeinde_aktuell_final_2.xlsx“, sie liegt im OneDrive von jemandem, der seit vier Jahren keinen Dienstauftrag mehr hat, und sie enthält von sämtlichen Gemeindegliedern Name, Anschrift, Geburtsdatum, Familienstand, Taufdatum und in Spalte M eine Bemerkung, die niemand schriftlich wiederholen möchte. Erstellt wurde sie 2019 für einen Serienbrief. Der Serienbrief ist längst verschickt. Die Datei lebt.

Wenn du in einem kirchlichen Träger für IT, Verwaltung oder Datenschutz verantwortlich bist, kennst du diese Datei. Du kennst auch ihre Verwandtschaft: die Geburtstagsliste im Besuchsdienst-Team, den Konfirmandenverteiler im privaten Messenger, die Kommunionkinderliste, die im Sekretariat ausgedruckt an der Pinnwand hängt, weil das Programm im Rechenzentrum „so kompliziert“ ist.

Der Reflex vieler Häuser lautet dann: Wir haben jetzt Microsoft 365, also machen wir das alles dort. Teams für den Besuchsdienst, SharePoint für die Listen, vielleicht eine kleine Power-App für die Erfassung. Und weil der Tenant hübsch aufgeräumt ist, fühlt sich das nach Fortschritt an.

Es ist aber keiner, jedenfalls nicht an dieser Stelle. Das kirchliche Meldewesen gehört nicht nach Microsoft 365. Nicht, weil die Cloud böse wäre – die Diskussion führen wir an anderer Stelle und ehrlicher, als es auf vielen Synodaltagungen geschieht. Sondern weil die Gemeindegliederdaten an einer Rechtskette hängen, die im Melderegister der Kommune beginnt, über das Bundesmeldegesetz in die kirchliche Rechtsordnung führt und dort in Fachverfahren endet, die genau dafür gebaut sind. Microsoft 365 ist in dieser Kette nicht vorgesehen. Es ist das, was danach kommt: der Ort, an dem mit Auszügen gearbeitet wird.

Dieser Beitrag zieht die Linie. Er zeigt, wo die Daten herkommen, welche Auszüge in Microsoft 365 zulässig sind, wie du sie schützt, wie du sie wieder loswirst und was du festlegen musst, bevor die erste ehrenamtliche Person eine Liste bekommt. Für die evangelische und die katholische Seite gleichermaßen, weil beide dasselbe Problem und zwei unterschiedliche Rechtswege dorthin haben.

Er gehört zur Serie Microsoft 365 in Kirche, Diakonie und Caritas, in der wir die Besonderheiten kirchlicher Träger der Reihe nach abarbeiten – und in der du auch die Beiträge findest, die hier nur gestreift werden.

Woher die Daten kommen: eine Rechtskette, die nicht bei dir beginnt

Der erste Fehler in fast jedem Gespräch über Gemeindegliederdaten ist die Annahme, es handele sich um Daten der Gemeinde. Tun sie nicht, jedenfalls nicht ursprünglich. Der weit überwiegende Teil dessen, was im Gemeindegliederverzeichnis oder in der Pfarrkartei steht, ist nicht in der Gemeinde erhoben worden. Er ist geliefert worden.

Der Ursprung liegt im kommunalen Melderegister

Rechtsgrundlage ist § 42 des Bundesmeldegesetzes. Die Meldebehörden übermitteln den öffentlich-rechtlichen Religionsgesellschaften Daten ihrer Mitglieder zur Erfüllung ihrer Aufgaben.

Für die Mitglieder selbst ist der Datenkatalog breit: Familienname, frühere Namen, Vornamen, Geburtsdatum, Staatsangehörigkeit, Familienstand, Anschriften. Für Familienangehörige, die derselben Religionsgesellschaft nicht angehören, ist er deutlich schmaler. Und diese Angehörigen dürfen der Übermittlung ihrer Daten widersprechen; die Meldebehörden müssen bei der Anmeldung und zusätzlich einmal jährlich ortsüblich auf dieses Widerspruchsrecht hinweisen.

Zwei Einschränkungen aus derselben Vorschrift solltest du auswendig können. Erstens: Die Übermittlung erfolgt nicht zu arbeitsrechtlichen Zwecken. Die Meldedaten sind also keine Quelle für die Personalabteilung, auch nicht für die charmante Frage, ob eine Bewerberin eigentlich noch in der Kirche ist. Zweitens: Die Übermittlung ist nur zulässig, wenn sichergestellt ist, dass beim Empfänger ausreichende Maßnahmen zum Datenschutz getroffen sind. Das ist keine Floskel. Das ist der Satz, aus dem die gesamte Diskussion über Exporte, Ablageorte und Ehrenamt folgt.

Technisch läuft die Übermittlung über XMeld, das Standardformat des staatlichen Meldewesens. Zusätzlich sieht das Gesetz einen regelmäßigen automatisierten Abgleich zum Zweck der Mitgliederbestandsprüfung vor, mit einem bundeseinheitlichen Stichtag. Für dich heißt das: Der Datenbestand wird laufend von außen aktualisiert. Jeder Export, den du in Microsoft 365 ablegst, ist ab dem Moment seiner Erstellung veraltet. Das ist kein Schönheitsfehler, sondern der Hauptgrund, warum Kopien in Zusammenarbeitsplattformen ein strukturelles Problem sind.

Evangelisch: Gemeindegliederverzeichnis nach dem Kirchenmitgliedschaftsgesetz

Auf evangelischer Seite regelt das Kirchengesetz über die Kirchenmitgliedschaft, das kirchliche Meldewesen und den Schutz der Daten der Kirchenmitglieder den Rahmen. Es bestimmt, dass in den Gliedkirchen für jede Kirchengemeinde ein Verzeichnis der Kirchenmitglieder mit ihren Familienangehörigen geführt wird (§ 14). Welche Daten hineingehören, legt nicht die Gemeinde fest, sondern eine Rechtsverordnung, die der Rat der EKD mit Zustimmung der Kirchenkonferenz erlässt. Das ist bereits die erste Antwort auf die Frage „Können wir uns nicht einfach eine eigene Liste bauen?“ – nein, der Datenkatalog ist gesetzt.

Die Weitergabe innerhalb der Kirche ist zulässig, soweit sie zur Wahrnehmung des Auftrags der Kirche erforderlich ist (§ 15); das Gliedkirchenrecht regelt die Einhaltung der Zweckbestimmung und das Verfahren. Das kirchliche Meldeverfahren selbst steht in § 16: Die Meldepflicht der Kirchenmitglieder gilt als erfüllt, wenn die Anmeldung unter Angabe der Religionszugehörigkeit bei der staatlichen oder kommunalen Meldebehörde erfolgt ist. Und § 17 verpflichtet die Gliedkirchen, den notwendigen Datenaustausch sicherzustellen und dafür einheitliche Datenverarbeitungsprogramme zu entwickeln. Genau das ist die Rechtsgrundlage dafür, dass die Meldewesen-Fachverfahren in den kirchlichen Rechenzentren laufen und nicht in dem, was eine Gemeinde sich selbst zusammenstellt.

Katholisch: Pfarrkartei nach der Kirchenmeldewesenanordnung

Auf katholischer Seite führt der Weg über die Anordnung über das kirchliche Meldewesen, kurz KMAO. Sie wird auf Vorschlag der Deutschen Bischofskonferenz von den Diözesen in Kraft gesetzt, existiert also in diözesanen Fassungen mit gemeinsamem Kern. Die Grundidee ist dieselbe: Weil die Kirche seit Einführung des staatlichen Meldewesens Daten aus den Melderegistern erhält, hat sie kein eigenes Meldewesen im Sinne einer eigenen Erhebung aufgebaut.

Im elektronischen Gemeindemitgliederverzeichnis werden neben den staatlichen Meldedaten die kirchlichen Amtshandlungen geführt – Taufe, Erstkommunion, Firmung, Trauung, Aufnahmen und Wiederaufnahmen –, dazu Kirchenaustritte sowie staatliche und kirchliche Sperren. Verantwortlich für die Erfassung sind die Kirchengemeinden und das jeweilige Ordinariat

beziehungsweise Generalvikariat; die Speicherung erfolgt im kirchlichen Rechenzentrum, und über die lokalen Zugriffsrechte entscheidet der Pfarrer. Diese Zuständigkeitsverteilung ist der Grund, warum ein IT-Dienstleister die Pfarrkartei nicht „mal eben“ nach SharePoint migrieren kann, selbst wenn er technisch dazu in der Lage wäre.

Die Sperren sind der wichtigste Teil – und der am leichtesten verlorene

Beide Systeme kennen Sperrvermerke. Kirchliche Sperren bilden persönliche Wünsche ab: kein Besuchsdienst, kein Gemeindebrief, keine Fundraising-Ansprache. Auf die Widerspruchsmöglichkeiten ist jährlich hinzuweisen. Solange die Daten im Fachverfahren liegen, wirken diese Sperren automatisch – jeder Bericht, jeder Serienbrieflauf, jede Geburtstagsabfrage berücksichtigt sie.

Und jetzt kommt der Satz, um den es in diesem ganzen Beitrag geht: Ein Excel-Export kennt keine Sperren. Er kennt nur die Zeilen, die zum Zeitpunkt des Exports mitgekommen sind. Widerspricht jemand am Tag darauf, steht die Person weiterhin in der Datei, die im Team liegt, im Postfach hängt und in drei OneDrive-Ordnern synchronisiert ist. Die Gemeinde schickt ihr dann trotzdem Post. Nicht aus Bosheit, sondern aus Dateisystem.

Fakten: Was in der Rechtskette feststeht

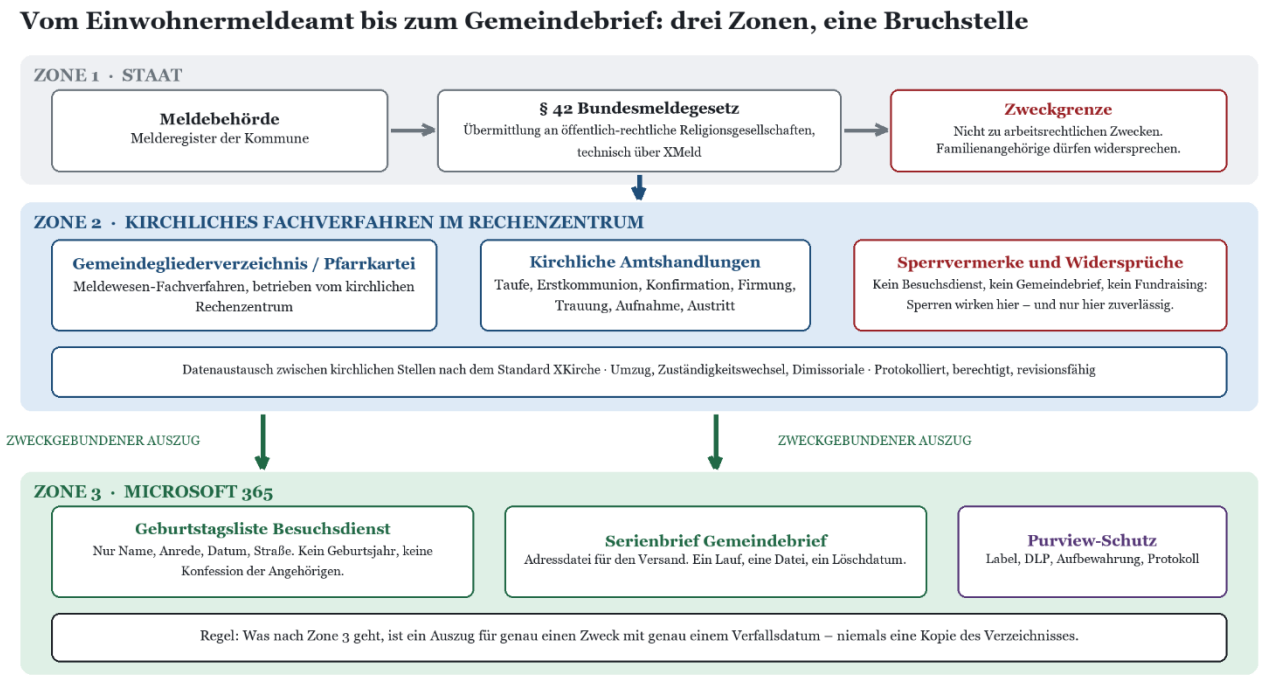
Die Meldebehörden übermitteln nach § 42 Bundesmeldegesetz Daten an öffentlich-rechtliche Religionsgesellschaften zur Aufgabenerfüllung, ausdrücklich nicht zu arbeitsrechtlichen Zwecken, und nur, wenn beim Empfänger ausreichende Datenschutzmaßnahmen getroffen sind.

Nicht der Religionsgesellschaft angehörende Familienangehörige können der Übermittlung widersprechen; darauf ist bei der Anmeldung und einmal jährlich ortsüblich hinzuweisen.

Evangelisch: Das Kirchenmitgliedschaftsgesetz der EKD regelt das Gemeindegliederverzeichnis (§ 14), die Weitergabe an kirchliche Stellen zur Wahrnehmung des kirchlichen Auftrags (§ 15), das kirchliche Meldeverfahren (§ 16) und die einheitlichen Datenverarbeitungsprogramme (§ 17).

Katholisch: Die Kirchenmeldewesenanordnung wird auf Vorschlag der Deutschen Bischofskonferenz diözesan in Kraft gesetzt und regelt das elektronische Gemeindemitgliederverzeichnis einschließlich der kirchlichen Amtshandlungen und der Sperren.

Der Datenaustausch zwischen kirchlichen Stellen läuft über den gemeinsam von evangelischer und katholischer Seite entwickelten XÖV-Standard XKirche; zwischen allen deutschen (Erz-)Diözesen erfolgt er seit 2018 elektronisch.



Skizze 1: Der Datenfluss vom kommunalen Melderegister bis zum Gemeindebrief. Zone 3 bekommt Auszüge, niemals den Bestand.

Was daran wirklich anders ist als in der Kommune

Ein Teil der Abgrenzung zur kommunalen IT wird in kirchlichen Häusern gern überdehnt. Also der Reihe nach, was tatsächlich anders ist.

Erstens die Rechtsordnung. Für kirchliche Träger gilt nicht die Datenschutz-Grundverordnung unmittelbar, sondern das eigene kirchliche Datenschutzrecht: das DSG-EKD auf evangelischer, das KDG auf katholischer Seite. Beide sind in den letzten anderthalb Jahren novelliert worden. Die Synode der EKD hat das neue DSG-EKD am 13. November 2024 beschlossen, es wurde am 15. Januar 2025 im Amtsblatt veröffentlicht und gilt seit dem 1. Mai 2025; unter anderem wurde die kirchenspezifische Rechtsgrundlage „kirchliches Interesse“ durch das allgemeinere „berechtigte Interesse“ ersetzt. Auf katholischer Seite hat die Vollversammlung des Verbandes der Diözesen Deutschlands die Novellierung von KDG und KDG-Durchführungsverordnung am 24. November 2025 beschlossen; in Kraft getreten ist sie am 1. März 2026. Wer also noch mit einem Datenschutzkonzept von 2022 arbeitet, arbeitet mit einem historischen Dokument.

Zweitens die Aufsicht. Nicht die Landesdatenschutzbehörde ist zuständig, sondern der Beauftragte für den Datenschutz der EKD beziehungsweise die Diözesandatenschutzbeauftragten mit den katholischen Datenschutzzentren. Das ändert nichts an der Sachfrage, aber alles an der Frage, wem du eine Datenpanne meldest und wer bei dir prüft.

Drittens die Mitbestimmung. Statt Personalrat verhandelst du mit der Mitarbeitervertretung, nach MVG-EKD oder MAVO. Das MVG-EKD ordnet die Einführung und Anwendung von Maßnahmen und technischen Einrichtungen, die zur Überwachung von Verhalten oder Leistung geeignet sind, der Mitbestimmung zu (§ 40 MVG-EKD); die MAVO kennt eine inhaltlich entsprechende Regelung samt Möglichkeit der Dienstvereinbarung. Protokollierung, Auditing und DLP-Auswertungen fallen genau in diesen Bereich.

Viertens das Fachverfahren selbst. Eine Kommune führt ihr Melderegister selbst, mit eigener Rechtsgrundlage und eigener Fachanwendung. Ein kirchlicher Träger führt ein abgeleitetes

Verzeichnis, das aus dem staatlichen Register gespeist wird und in eine gesamtkirchliche Austauschstruktur eingebunden ist. Deine Freiheitsgrade sind dadurch kleiner, nicht größer.

Und das war es dann auch schon. Alles andere – Postfächer, Teams, Dateiablage, Telefonie, Endgerätemanagement, bedingter Zugriff – ist ganz normales Microsoft 365, und es wird nicht kirchlicher dadurch, dass man es in Gremien lange genug bespricht.

Wer die beiden Datenschutzgesetze im Detail braucht, findet sie in eigenen Beiträgen: DSG-EKD verständlich: Was das evangelische Datenschutzgesetz für Microsoft 365 konkret bedeutet und KDG verständlich: Microsoft 365 unter dem Kirchlichen Datenschutzgesetz der katholischen Kirche.

Wo die Daten trotzdem in Microsoft 365 auftauchen

Die reine Lehre lautet: Gemeindegliederdaten bleiben im Fachverfahren. Die Praxis lautet: Der Besuchsdienst fährt nicht mit einem Terminalclient zur Geburtstagsgratulation. Irgendwo muss ein Auszug entstehen, und in den allermeisten Häusern entsteht er heute unkontrolliert. Schauen wir uns die vier üblichen Verdächtigen an.

Geburtstagslisten für den Besuchsdienst

Der Klassiker, und zugleich der Fall, der sich am saubersten lösen lässt. Der Besuchsdienst braucht: Anrede, Name, Anschrift, das Datum des Geburtstags und – je nach Gemeindepraxis – die Angabe des runden Jubiläums. Er braucht nicht: das vollständige Geburtsdatum mit Jahrgang, den Familienstand, die Konfession der Angehörigen, das Taufdatum, die Kirchensteuermerkmale oder die Bemerkungsspalte.

Was tatsächlich exportiert wird, ist in neun von zehn Häusern der Vollbericht, weil der schneller zu erzeugen war. Genau hier liegt der größte und billigste Hebel: Lass im Fachverfahren einen Bericht bauen, der ausschließlich die benötigten Felder liefert, monatsweise gefiltert und um alle Sperren bereinigt. Das ist eine Aufgabe von zwei Stunden für das Rechenzentrum und spart dir den halben Rest dieses Beitrags.

Konfirmanden- und Kommunionkinderlisten

Hier wird es heikler, weil es um Minderjährige geht und weil die Listen über Monate in Gebrauch sind: Anmeldung, Gruppeneinteilung, Elternabende, Fahrten, Fotoeinwilligungen, Abwesenheiten. Das ist echte Fallarbeit, und sie findet in Teams statt, ob es dir gefällt oder nicht.

Die Linie verläuft hier zwischen Stammdaten und Arbeitsdaten. Die Stammdaten – wer ist Gemeindeglied, wer ist getauft, welche Anschrift gilt – bleiben im Fachverfahren. Die Arbeitsdaten – wer ist in Gruppe B, wer fährt mit, wer hat die Einwilligung abgegeben – dürfen in Microsoft 365 entstehen und dort leben. Was du verhindern musst, ist die Vermischung: die Liste, die mit fünf Feldern begann und nach dem dritten Copy-and-paste sechzehn hat, darunter das Geburtsdatum der Eltern.

Praktisch heißt das: ein eigenes Team je Jahrgang, mit definiertem Ende, mit Label, mit Aufbewahrungsrichtlinie, und mit einer klaren Ansage an die Hauptamtlichen, dass am Ende des Kurses die Ablage in den Zustand „abgeschlossen“ überführt wird. Für die Strukturfrage lohnt sich ein Blick in den Beitrag zur Informationsarchitektur.

Die Ablagestruktur dafür ist beschrieben in SharePoint-Informationsarchitektur für Kirchengemeinde und Kirchenkreis: Pfarramt, Gremien, Ausschüsse und Gebäude.

Adressexporte für den Gemeindebrief und Serienbriefe

Der Gemeindebrief ist der zweitgrößte Erzeuger von Adressdateien und der größte Erzeuger von Datenpannen mit Außenwirkung, weil hier regelmäßig Dritte beteiligt sind: Lettershops, Druckereien, Postdienstleister. Damit bist du in der Auftragsverarbeitung, und zwar nach kirchlichem Recht – § 30 DSG-EKD beziehungsweise § 29 KDG. Der Vertrag muss die Verarbeitung nach Umfang, Art und Zweck, die Datenarten und den Kreis der Betroffenen festlegen, und die beauftragende kirchliche Stelle muss sich vor Beginn und danach regelmäßig von den technischen und organisatorischen Maßnahmen überzeugen. „Wir kennen die Druckerei seit zwanzig Jahren“ ist keine Überzeugung im Sinne der Vorschrift.

Immerhin: Seit der Novelle ist die frühere Pflicht, säkulare Auftragsverarbeiter der kirchlichen Aufsicht zu unterwerfen, im DSG-EKD entfallen. Das macht Verträge mit externen Dienstleistern erheblich leichter verhandelbar – ein Punkt, der in der Praxis mehr Wirkung entfaltet hat als die meisten anderen Änderungen.

Für den Serienbrief selbst gilt: Er ist ein Lauf, kein Zustand. Eine Datei, ein Zweck, ein Termin, danach weg. Wer den Serienbrief-Datensatz „für das nächste Mal“ behält, hat kein Archiv angelegt, sondern ein Risiko mit Verfallsdatum null.

Und die Kirchensteuer? Eine Zone für sich

Beim Kirchensteuerbezug treffen kirchliche und steuerliche Regeln aufeinander. Das Kirchensteuerabzugsmerkmal – ein sechsstelliger Code für Religionszugehörigkeit, Steuersatz und zuständige Religionsgemeinschaft – wird beim Bundeszentralamt für Steuern abgefragt; die Auskunft aus der Regelabfrage gilt grundsätzlich für das folgende Kalenderjahr. Aufbewahrungsseitig landest du in der Abgabenordnung, mit den dort für sonstige Unterlagen vorgesehenen Fristen.

Merke: Steuerdaten sind besonders heikel, weil sie die Religionszugehörigkeit unmittelbar offenlegen und damit eine besondere Kategorie personenbezogener Daten betreffen (§ 13 DSG-EKD, § 11 KDG). Sie gehören in die Finanzverfahren und in die Abstimmung mit der Kirchensteuerstelle, nicht in eine Excel-Auswertung für das Leitungsgremium. Wenn das Presbyterium, der Kirchenvorstand oder der Verwaltungsrat Zahlen braucht, braucht es aggregierte Zahlen. Personenbezug ist dort nie erforderlich.

Warnung: Der Vollexport im OneDrive eines Ehrenamtlichen

Das Szenario, das bei jeder zweiten Bestandsaufnahme auftaucht: Eine ehrenamtliche Person im Besuchsdienst hat ein eigenes Konto im Tenant bekommen – gut so – und im Pfarrbüro hat jemand freundlicherweise „die Liste“ exportiert und per Teams-Chat geschickt. Die Liste enthält sämtliche Gemeindeglieder mit vollständigem Geburtsdatum, Familienstand, Angehörigen und Amtshandlungen. Sie liegt jetzt in einem persönlichen OneDrive.

Was daran im Einzelnen kaputt ist: Die Zweckbindung ist verletzt, weil der Besuchsdienst nur Geburtstage braucht. Die Datenminimierung ist verletzt, weil der komplette Bestand statt einer Monatsauswahl übergeben wurde. Die Sperrvermerke sind wirkungslos, weil ein Export sie nicht mitführt. Die Richtigkeit ist verletzt, weil der Bestand fortlaufend aktualisiert wird und die Kopie nicht. Und die Speicherbegrenzung ist verletzt, weil niemand ein Löschdatum vereinbart hat.

Besonders unangenehm: OneDrive-Inhalte lassen sich nicht per Restricted Content Discovery aus der organisationsweiten Suche und aus Copilot nehmen – diese Funktion gilt ausdrücklich nur für SharePoint-Sites. Wenn später Copilot ausgerollt wird, ist der Vollexport also im Zugriff, sobald jemand mit Berechtigung eine passende Frage stellt.

Und der Teil, an den niemand denkt: Wird das ehrenamtliche Konto irgendwann gelöscht, bleibt das

OneDrive standardmäßig weiter bestehen – der im SharePoint Admin Center einstellbare Zeitraum liegt zwischen 30 und 3.650 Tagen. Zehn Jahre sind ein plausibler Wert für eine Fehlkonfiguration und eine sehr lange Zeit für eine Datei, die es nie hätte geben dürfen.

Die folgende Tabelle ist die Kurzfassung dessen, was du im Haus verbindlich machen musst. Sie funktioniert für die evangelische wie für die katholische Seite; das Fachverfahren heißt nur jeweils anders.

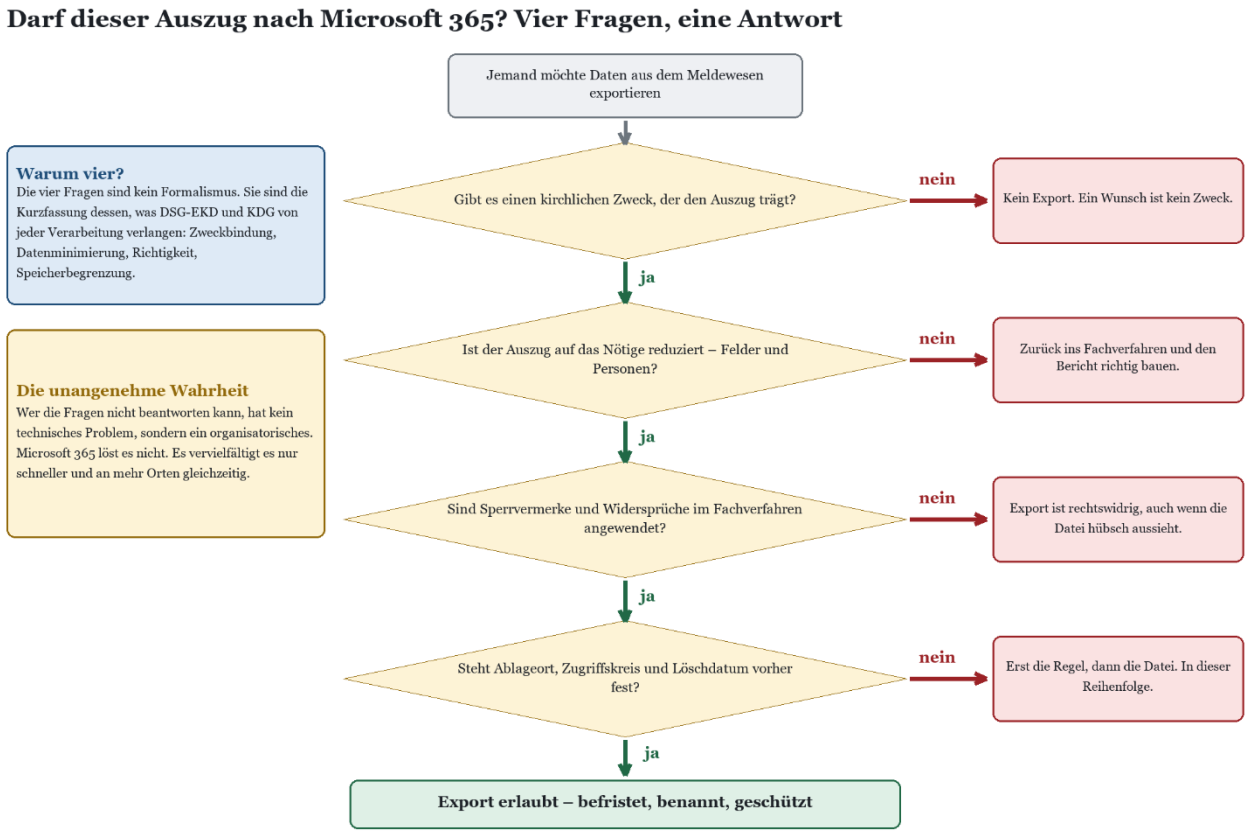
Datenart	Führendes Fachverfahren	Export nach Microsoft 365	Schutzmaßnahme
Gemeindegliederbestand vollständig (Stammdaten, Familienverbund, Amtshandlungen, Sperren)	Meldewesen-Fachverfahren im kirchlichen Rechenzentrum (evangelisch Gemeindegliederverzeichnis, katholisch Pfarrkartei)	Nein. Kein Anwendungsfall rechtfertigt eine Vollkopie.	Exportfunktion für Gemeindebüros technisch beschränken; Vollexporte nur durch das Rechenzentrum auf begründeten Antrag
Geburtstagsliste Besuchsdienst	Meldewesen-Fachverfahren, Bericht mit Sperrfilter	Ja, monatsweise, reduzierter Feldsatz, ohne Geburtsjahr	Eigene SharePoint-Bibliothek im Besuchsdienst-Team, Label mit Verschlüsselung, Aufbewahrungsrichtlinie mit Löschung nach dem Monat
Konfirmanden- und Kommunionkinderdaten	Meldewesen-Fachverfahren für Stammdaten; Kursverwaltung je nach Träger	Stammdaten nur als Startliste; Arbeitsdaten dürfen in Microsoft 365 entstehen	Jahrgangsteam mit festem Ende, Mitgliedschaft geschlossen, Gastzugang ausgeschlossen, Label, Aufbewahrung bis Kursende plus definierte Frist
Adressdatei Gemeindebrief	Meldewesen-Fachverfahren, Versandbericht	Ja, je Versandlauf, nur Anschriftfelder	Auftragsverarbeitungsvertrag mit Lettershop nach § 30 DSG-EKD bzw. § 29 KDG; Übergabe über geschützten Kanal; Löschung nach Auslieferung
Serienbrief an einzelne Zielgruppen (Jubiläen, Einladungen)	Meldewesen-Fachverfahren, Zielgruppenbericht	Ja, einmalig je Anlass	Ablage im Vorgangsordner des Pfarramts, nicht im OneDrive; Löschdatum im Dateinamen oder per Aufbewahrungsbezeichnung
Kirchensteuermerkmale, Kirchensteuerabzugsmerkmal	Finanz- und Kirchensteuerverfahren des Trägers bzw. der Kirchensteuerstelle	Nein, personenbezogen. Für Gremien nur aggregiert.	Besondere Kategorie nach § 13 DSG-EKD bzw. § 11 KDG; DLP-Regel auf das Merkmalsformat; kein Versand per Mail
Spenden- und Kollektendaten mit Personenbezug	Fundraising- oder Finanzverfahren	Nur aggregiert oder pseudonymisiert	Fundraising-Sperren beachten; getrennte Ablage; Zugriff auf die Finanzverwaltung begrenzt
Seelsorgliche Vermerke, Beratungsinhalte, Klientenakten	Seelsorge bleibt außerhalb jeder IT-Ablage; Klientendaten im Fachverfahren der	Nein, unter keinen Umständen	Organisatorisches Verbot, technische Absicherung über Label und DLP, Schulung; im Zweifel Papier und Schrank

	Einrichtung		

Die letzte Zeile ist ein eigenes Thema und in zwei Beiträgen ausführlich behandelt: Seelsorgegeheimnis und Beichtgeheimnis in Microsoft 365: Was nie in Teams, OneNote oder Copilot landen darf sowie Klientendaten in Diakonie und Caritas: Sozialdaten, Schweigepflicht und Schutz mit Microsoft Purview. Wenn du in einem diakonischen oder caritativen Träger arbeitest, lies den zweiten zuerst – Sozialdaten und Schweigepflicht sind noch einmal ein anderer Schärfegrad als Gemeindegliederdaten.

Die Exportregel: vier Fragen, die vor jeder Datei stehen

Du kannst dieses Thema technisch angehen und wirst scheitern. Du kannst es organisatorisch angehen und wirst langsam vorankommen. Du kannst es beides gleichzeitig angehen, in dieser Reihenfolge: erst die Regel, dann die Technik, die sie durchsetzt. Die Regel passt auf eine Seite.



Skizze 2: Der Entscheidungsweg vor jedem Export. Vier Fragen, und bei jedem Nein ist die Antwort dieselbe.

Frage eins: Welcher kirchliche Zweck trägt den Auszug?

Nicht „wofür ist das gut“, sondern „welche kirchliche Aufgabe wird damit erfüllt“. Besuchsdienst, Gemeindebrief, Konfirmandenarbeit, Kirchenvorstandswahl: alles saubere Zwecke. „Der Kollege hätte gern mal einen Überblick“, „für die Statistik“ und „falls wir es brauchen“ sind keine. Notiere den Zweck schriftlich, mit einem Satz, im Verarbeitungsverzeichnis. Wenn du den Satz nicht zustande bringst, hast du deine Antwort.

Frage zwei: Ist der Auszug wirklich reduziert?

Reduziert heißt zweidimensional: weniger Felder und weniger Personen. Der Besuchsdienst braucht den laufenden Monat, nicht das Jahr. Der Gemeindebrief braucht Anschriften, nicht

Geburtsdaten. Die Konfirmandenarbeit braucht den Jahrgang, nicht die Familien der Nachbarschaft.

Der Hebel liegt im Fachverfahren, nicht in Excel. Wer erst exportiert und dann Spalten löscht, hat die Daten trotzdem übergeben – und in Excel gelöschte Spalten sind in älteren Dateiversionen, im Papierkorb und in der Vorversionshistorie noch eine ganze Weile munter.

Frage drei: Sind Sperren und Widersprüche angewendet?

Diese Frage stellt in der Praxis niemand, weil sie unsichtbar ist. Ein Bericht, der Sperren ignoriert, sieht exakt so aus wie einer, der sie berücksichtigt – nur mit ein paar Zeilen mehr. Deshalb muss die Antwort in die Berichtsdefinition, nicht in die Zuständigkeit der Person, die auf „Exportieren“ klickt.

Lass dir vom Rechenzentrum bestätigen, welche Berichte Sperrvermerke auswerten, und beschrifte die anderen. Wenn ein Bericht Sperren nicht auswertet, gehört er nicht in die Hand der Gemeinde.

Frage vier: Steht der Rahmen fest, bevor die Datei existiert?

Ablageort, Zugriffskreis, Löschdatum. Drei Angaben, die vor dem Export feststehen müssen, weil sie danach niemand mehr nachträgt. Ein Export ohne Löschdatum ist eine dauerhafte Speicherung, und eine dauerhafte Speicherung von Meldedaten außerhalb des Fachverfahrens hat keine Rechtsgrundlage.

Tipp: Die Exportrichtlinie in zehn Sätzen

1. Führendes System für alle Gemeindegliederdaten ist das Meldewesen-Fachverfahren im kirchlichen Rechenzentrum.
2. Exporte sind Auszüge für einen benannten Zweck, niemals Kopien des Bestands.
3. Es gibt eine abschließende Liste zugelassener Berichte; andere Exporte sind unzulässig.
4. Jeder Bericht wertet Sperrvermerke und Widersprüche aus; das ist schriftlich bestätigt.
5. Ablageort ist immer eine benannte SharePoint-Bibliothek oder ein benanntes Team, niemals OneDrive, Chat oder Mailanhang.
6. Jeder Export trägt ein Sensitivity Label und damit Verschlüsselung, Zugriffsbeschränkung und Kennzeichnung.
7. Jeder Export hat ein Löschdatum, das technisch durchgesetzt wird.
8. Ehrenamtliche erhalten Auszüge nur mit eigenem Konto, nach Verpflichtung auf das Datengeheimnis und nach Einweisung.
9. Die Übergabe an externe Dienstleister erfolgt nur mit Auftragsverarbeitungsvertrag nach kirchlichem Recht.
10. Wer einen Export benötigt, der hier nicht vorgesehen ist, stellt einen Antrag – und bekommt eine Antwort, keine Duldung.

Zugriff durch Ehrenamtliche: der eigentliche Knackpunkt

In der Dienstgemeinschaft arbeiten Hauptamt und Ehrenamt nebeneinander, und das ist gut so. Datenschutzrechtlich sind beide nicht gleich. Ehrenamtliche stehen in keinem Dienstverhältnis, unterliegen keiner arbeitsrechtlichen Sanktion, und wenn sie aufhören, hört auch der Zugriff auf ihre Geräte auf – nur nicht der Zugriff auf die Dateien, die sie mitgenommen haben.

Praktisch brauchst du drei Dinge. Erstens eigene Konten statt geteilter Anmeldungen; ein Sammelkonto „besuchsdienst@“ mag bequem sein, macht aber jede Protokollierung wertlos und

jede Löschung unmöglich. Zweitens eine schriftliche Verpflichtung auf das Datengeheimnis – das DSG-EKD regelt sie ausdrücklich (§ 26), das KDG fordert Entsprechendes. Drittens eine Einweisung, die nicht aus einem PDF besteht, sondern aus zwanzig Minuten mit echten Beispielen aus der eigenen Gemeinde.

Und dann die unpopuläre Konsequenz: Wer keinen Zugang bekommt, bekommt auch keine Datei. Die Umgehung „dann drucke ich es eben aus und gebe es mit" ist nicht die Lösung, sondern dieselbe Datenübermittlung mit schlechterer Protokollierung.

Wie du Ehrenamtliche technisch sauber anbindest – eigenes Konto, Gastzugang oder bewusst gar nichts –, steht in Ehrenamtliche in Microsoft 365: Gastzugang, eigene Konten, geteilte Postfächer oder besser gar nichts?.

Wichtig: Aufbewahrung ist nicht dasselbe wie Datenschutz

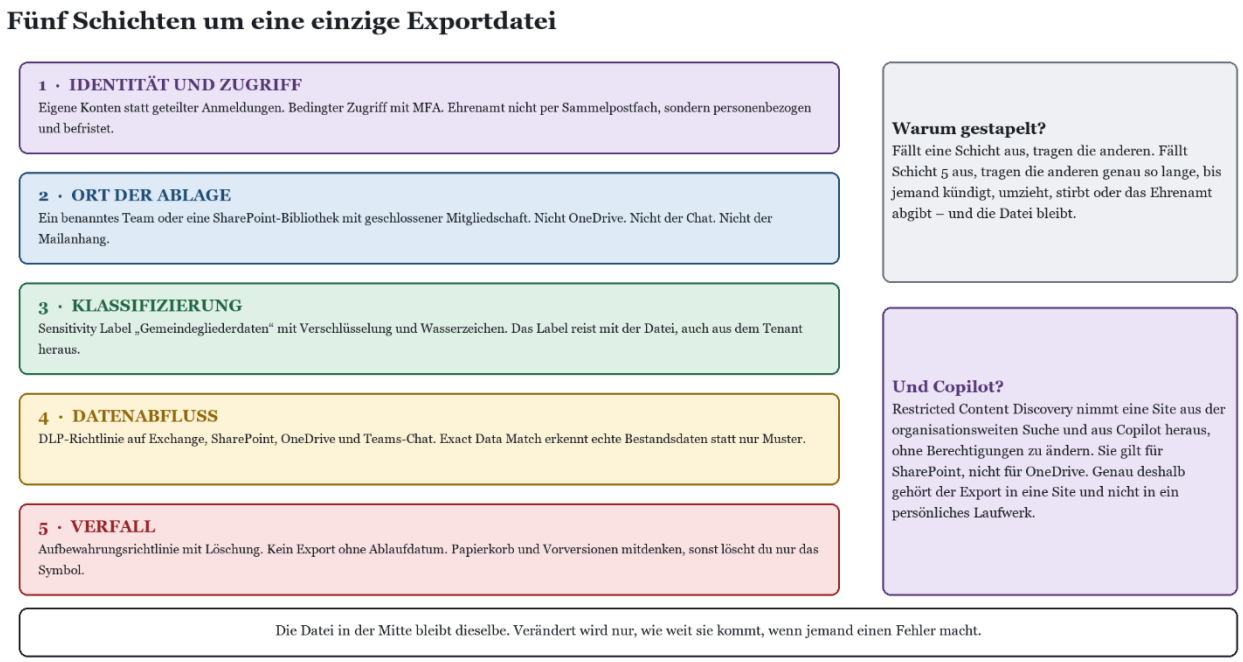
Kirchliche Träger unterliegen eigenen Archiv- und Kassationsordnungen. Kirchenbücher und bestimmte Amtshandlungsnachweise sind dauerhaft aufzubewahren – das ist kein Widerspruch zur Löschpflicht, sondern eine andere Datenart in einem anderen System.

Was du niemals tun darfst: eine Exceltabelle im Team als „Archiv" deklarieren, weil in ihr Amtshandlungen stehen. Die Archivwürdigkeit liegt beim Kirchenbuch und beim Fachverfahren, nicht bei deinem Arbeitsauszug. Der Auszug wird gelöscht. Immer.

Wie du Fristen und Kassationsregeln technisch abbildest, steht in Kirchliche Aufbewahrungsfristen, Kassationsordnungen und Archivgesetze in Microsoft Purview abbilden.

Technische Leitplanken in Microsoft 365

Jetzt zur Technik. Die gute Nachricht: Du brauchst nichts Exotisches. Die schlechte: Du brauchst mehrere Bausteine gleichzeitig, weil jeder einzelne umgangen werden kann.



Skizze 3: Fünf Schutzschichten um eine einzige Exportdatei. Keine einzelne Schicht trägt allein.

Klassifizierung: ein eigenes Label für Gemeindegliederdaten

Ein Sensitivity Label ist der einzige Schutz, der die Datei begleitet, wenn sie den Tenant verlässt. Richte ein Label ein, das konkret heißt, was es schützt – „Gemeindegliederdaten“ und nicht „Vertraulich 3“ –, verschlüssele damit, beschränke die Berechtigung auf eine benannte Gruppe und setze eine sichtbare Kennzeichnung. Die Kennzeichnung ist wichtiger, als IT-Leute glauben: Sie ist das Einzige, was eine ehrenamtliche Person sieht, bevor sie auf „Weiterleiten“ klickt.

Das Label gehört nicht isoliert eingeführt, sondern als Teil eines Konzepts, das vom Gemeindebrief bis zur Beratungsakte reicht – mit so wenigen Stufen wie möglich, weil jede zusätzliche Stufe die Trefferquote senkt.

Ein durchgearbeitetes Label-Konzept für kirchliche Träger findest du in Sensitivity Labels für kirchliche Träger: Ein Label-Konzept vom Gemeindebrief bis zur Beratungsakte.

Datenabfluss: DLP mit echten Bestandsdaten statt nur Mustern

Eine DLP-Richtlinie über Exchange Online, SharePoint, OneDrive und den Teams-Chat fängt die häufigsten Unfälle ab: die Liste im Mailanhang an eine private Adresse, die Weitergabe im Chat an jemanden außerhalb der Gemeinde, den Freigabelink „für alle im Internet“.

Für Gemeindegliederdaten ist die Mustererkennung allerdings schwach – ein Name mit Adresse sieht aus wie jeder andere Name mit Adresse. Hier hilft Exact Data Match: Du lädst nicht die Daten selbst hoch, sondern deren gehashte Werte samt Salt, und die Richtlinie erkennt exakt deine Bestandsdaten statt irgendwelcher Muster. Die Quelltabelle darf bis zu 100 Millionen Zeilen umfassen und lässt sich täglich aktualisieren – für eine Landeskirche oder ein Bistum reicht das mit erheblichem Abstand. Unterstützt wird Exact Data Match unter anderem in DLP für SharePoint, OneDrive, Teams-Chat, Exchange Online und Endgeräte sowie in der automatischen Klassifizierung.

In der Praxis heißt das: Ein Träger kann eine Regel bauen, die anschlägt, wenn in einer Datei mehr als eine bestimmte Anzahl echter Gemeindegliederdatensätze steht. Ein Besuchsdienstauszug mit dreißig Zeilen läuft durch, ein Vollexport mit achttausend wird blockiert. Das ist genau die Unterscheidung, die du organisatorisch triffst – nur eben automatisch.

Ablageort und Copilot: warum SharePoint und nicht OneDrive

OneDrive ist persönlicher Speicher. Persönlicher Speicher hat keinen Eigentümerwechsel, keine Gremienzuständigkeit und keine Nachfolge. Wenn die Person geht, geht die Zuständigkeit, nicht die Datei.

Hinzu kommt ein sehr konkretes Argument aus der Copilot-Welt. Restricted Content Discovery nimmt Inhalte einer SharePoint-Site aus der organisationsweiten Suche und aus Copilot-Antworten heraus und blendet gleichzeitig die KI-Einstiegspunkte auf diesen Sites aus, ohne Berechtigungen zu verändern. Es lässt sich auf bis zu 20.000 Sites anwenden, setzt eine Copilot-Lizenz und SharePoint Advanced Management voraus – und es funktioniert ausdrücklich nicht für OneDrive. Wer seine sensiblen Auszüge in persönlichen Laufwerken liegen hat, kann sie also genau dann nicht mehr einfangen, wenn es darauf ankommt.

Ein Hinweis für die Erwartungssteuerung: Die Umstellung wirkt nicht sofort. Bei Sites mit mehr als 500.000 Elementen kann es laut Microsoft über eine Woche dauern, bis sich die Änderung vollständig in Suche und Copilot niederschlägt. Und Purview-Funktionen wie eDiscovery und automatische Klassifizierung arbeiten weiter, weil der Inhalt nicht aus dem Suchindex entfernt wird. Das ist beabsichtigt – Aufsicht und Rechtsverfolgung sollen ja funktionieren.

Die Dokumentation zu dieser Funktion findet sich bei Microsoft unter Restrict discovery of SharePoint sites and content.

Was das für einen Copilot-Rollout insgesamt bedeutet, steht in Copilot in Kirche und Diakonie: Nutzen, Grenzen, Oversharing und die Copilot-Überprüfung vor dem Rollout.

Verfall: Löschung ist ein Prozess, kein Klick

Eine Aufbewahrungsrichtlinie in Purview, die auf die Bibliothek mit den Auszügen wirkt und nach Ablauf löscht, ist der einzige Mechanismus, der unabhängig von menschlicher Disziplin funktioniert. Richte sie so ein, dass sie auf Grundlage des Erstellungsdatums löscht, und prüfe, ob der Papierkorb zweiter Stufe und die Versionshistorie mit abgeräumt werden. Sonst löschst du das Symbol und behältst den Inhalt.

Der zweite Mechanismus betrifft Konten. Wird ein Benutzerkonto gelöscht, bleibt das zugehörige OneDrive standardmäßig erhalten; der Zeitraum ist im SharePoint Admin Center zwischen 30 und 3.650 Tagen einstellbar. Prüfe diesen Wert. In vielen kirchlichen Tenants steht dort eine Zahl, die jemand 2021 „erst mal großzügig“ gesetzt hat, und seitdem sammeln sich die Laufwerke ehemaliger Ehrenamtlicher.

Identität und Zugriff

Zum Schluss die Schicht, die alles darunter trägt. Eigene Konten für Ehrenamtliche, mehrstufige Anmeldung ohne Ausnahme, bedingter Zugriff mit Regeln, die zwischen Pfarrbüro, Verwaltung, Pflegedienst und Ehrenamt unterscheiden. Für den Zugriff auf Auszüge mit Gemeindegliederdaten ist eine eigene, kleine Gruppe die richtige Antwort – nicht „alle in der Gemeinde“, und schon gar nicht „jeder mit dem Link“.

Und ja: Das bedeutet Verwaltungsaufwand. Ein Träger, der siebzig Ehrenamtliche im Besuchsdienst hat, muss siebzig Konten pflegen, einweisen und wieder abschalten. Das ist der Preis dafür, dass man personenbezogene Daten aus einem staatlichen Melderegister verarbeiten darf. Wer den Preis nicht zahlen will, arbeitet mit Papierlisten aus dem Pfarrbüro, die abends zurückkommen. Auch eine Lösung, und in kleinen Gemeinden ehrlich gesagt die bessere.

Baustein	Was er löst	Was er nicht löst
Sensitivity Label mit Verschlüsselung	Schutz reist mit der Datei, auch außerhalb des Tenants; sichtbare Kennzeichnung vor dem Weiterleiten	Verhindert nicht, dass ein Berechtigter den Inhalt abtippt oder fotografiert
DLP mit Exact Data Match	Erkennt echte Bestandsdaten statt Muster; blockiert Massenexporte in Mail, Chat und Freigaben	Greift nicht bei Papier und nicht bei Daten, die nie in die Quelltabelle aufgenommen wurden
Restricted Content Discovery	Nimmt SharePoint-Sites aus organisationsweiter Suche und Copilot; blendet KI-Einstiegspunkte aus	Ändert keine Berechtigungen, wirkt nicht für OneDrive, braucht Copilot und SharePoint Advanced Management
Aufbewahrungsrichtlinie mit Löschung	Setzt das Verfallsdatum technisch durch, unabhängig von Disziplin	Ersetzt nicht die Kassationsordnung und nicht die Archivzuständigkeit
Bedingter Zugriff und mehrstufige Anmeldung	Verhindert Fremdzugriff auf Konten, differenziert nach Rolle und Gerät	Schützt nicht vor dem berechtigten Nutzer, der zu viel bekommen hat
Berichtsdefinition im Fachverfahren	Reduziert Felder und Personen an der Quelle, wendet Sperren an	Nützt nichts, wenn daneben eine freie Exportfunktion offen bleibt

Rollen, Gremien und der Weg zur verbindlichen Regel

Eine Exportregel, die nur in der IT existiert, ist eine Meinung. Verbindlich wird sie durch die Gremien, und die sind in kirchlichen Trägern zahlreicher als anderswo.

Wer was entscheidet

Verantwortliche Stelle im Sinne des kirchlichen Datenschutzrechts ist der Träger, nicht die IT und nicht das Rechenzentrum. In der Kirchengemeinde ist das evangelisch das Presbyterium beziehungsweise der Kirchenvorstand, katholisch der Kirchenvorstand oder die Kirchenverwaltung – der Pfarrgemeinderat ist das pastorale Gremium und in dieser Frage nicht das entscheidende. Im Kirchenkreis, im Dekanat, im Landeskirchenamt und im Generalvikariat gelten die jeweiligen Geschäftsordnungen.

Praktisch bedeutet das: Die Exportrichtlinie wird von der IT entworfen, vom örtlich Beauftragten für den Datenschutz geprüft, mit der Mitarbeitervertretung abgestimmt, soweit Beschäftigte betroffen sind, und vom zuständigen Leitungsgremium beschlossen. Ohne diesen Beschluss ist die Regel im Konfliktfall nichts wert, und Konfliktfälle gibt es genau dann, wenn jemand seine Liste nicht hergeben möchte.

Mitarbeitervertretung: Protokollierung ist mitbestimmt

Die Exportregel selbst berührt in erster Linie Betroffenenrechte, nicht Beschäftigtenrechte. Ihre technische Durchsetzung tut es sehr wohl: DLP-Auswertungen, Auditprotokolle, Berichte darüber, wer welchen Export erzeugt hat. Das MVG-EKD ordnet Maßnahmen und technische Einrichtungen, die zur Überwachung von Verhalten oder Leistung geeignet sind, der Mitbestimmung zu (§ 40 MVG-EKD); die MAVO enthält eine entsprechende Regelung und sieht dafür ebenfalls Dienstvereinbarungen vor.

Der pragmatische Weg: Nimm die MAV früh mit hinein und schreibe in die Dienstvereinbarung hinein, wozu die Auswertungen dienen und wozu ausdrücklich nicht. Eine MAV, die versteht, dass DLP-Meldungen dem Schutz der Gemeindeglieder dienen und nicht der Leistungskontrolle des Pfarrsekretariats, ist in aller Regel kooperativ. Eine MAV, die vom fertigen System überrascht wird, ist es nie.

Die Mitbestimmungsfragen rund um Teams, Copilot und Protokollierung sind gesammelt in Mitarbeitervertretung und Microsoft 365: MVG-EKD, MAVO, Dienstvereinbarung und Mitbestimmung bei Teams, Copilot und Protokollierung.

Datenschutzaufsicht: was geprüft wird

Der Beauftragte für den Datenschutz der EKD und die Diözesandatenschutzbeauftragten beziehungsweise die katholischen Datenschutzzentren fragen bei diesem Thema erfahrungsgemäß nach drei Dingen: dem Verarbeitungsverzeichnis mit den tatsächlich gelebten Exporten, der Auftragsverarbeitung mit Rechenzentrum und externen Dienstleistern, und der Frage, wie Ehrenamtliche eingebunden und verpflichtet sind.

Wenn die Verarbeitung ein hohes Risiko birgt, kommt die Datenschutz-Folgenabschätzung hinzu – § 34 DSG-EKD, § 35 KDG. Für Microsoft 365 insgesamt wirst du sie ohnehin brauchen; die Verarbeitung von Gemeindegliederdaten gehört dann als eigener Verarbeitungsvorgang hinein, mit einer ehrlichen Beschreibung dessen, was exportiert wird.

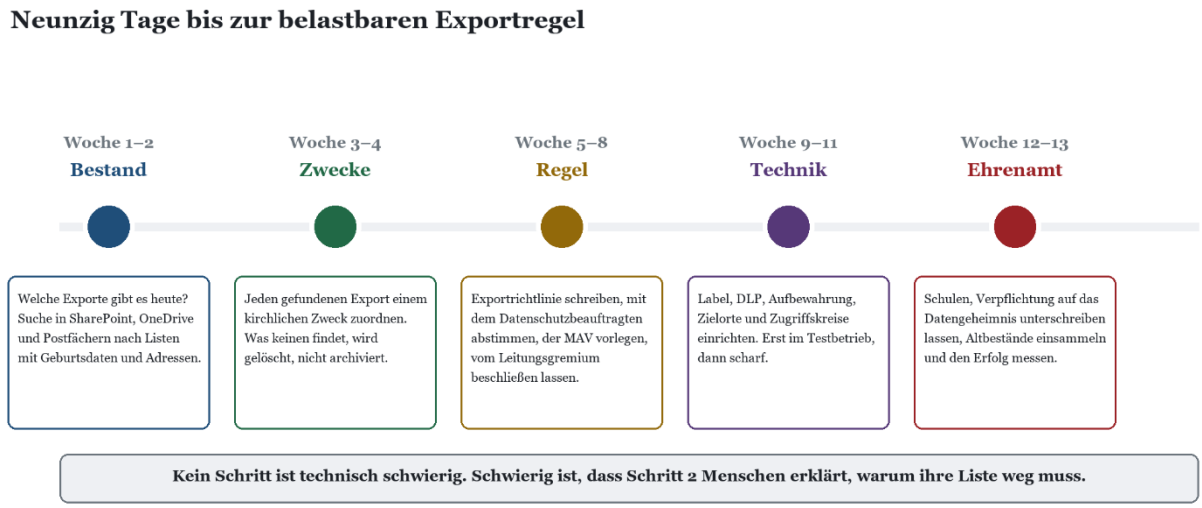
Worauf die Aufsichten im Detail schauen, steht in Kirchliche Datenschutzaufsicht in der Praxis: Was BfD EKD und Diözesandatenschutzbeauftragte von einem Microsoft-365-Tenant erwarten.

Und das Rechenzentrum?

Das kirchliche Rechenzentrum ist in aller Regel dein Auftragsverarbeiter für das Meldewesen, und zwar mit einem Vertrag, der schon existiert. Nutze ihn: Die Exportberichte, die du brauchst, sind eine Leistung, die du dort bestellen kannst. In vielen Häusern wird stattdessen improvisiert, weil niemand fragen wollte.

Ein diakonisches Werk in einer Großstadt hat das durchgerechnet und festgestellt, dass die Beauftragung von vier zusätzlichen Berichten günstiger war als der Aufwand für die Nachbearbeitung freier Exporte in den Gemeinden – noch bevor irgendein Datenschutzrisiko eingepreist war. Ein Caritasverband auf Kreisebene kam zum selben Ergebnis, nur über den Umweg einer Datenpanne.

Wie sich Microsoft 365 und kirchliche Rechenzentren zueinander verhalten, ist Thema in Die Cloud-Frage in der Kirche: Kirchliche Rechenzentren, Microsoft 365 und die Ehrlichkeit über Datenstandorte.



Skizze 4: Ein realistischer Fahrplan. Der schwierigste Schritt ist nicht die Technik, sondern Woche 3 und 4.

Der Bestandsaufnahme-Trick

Bevor du irgendetwas regelst, musst du wissen, was da ist. Drei Wege haben sich bewährt und lassen sich kombinieren.

- Inhaltssuche über den Tenant nach typischen Feldbezeichnungen: „Geburtsdatum“, „Gemeindeglied“, „Taufdatum“, „Konfession“, „Kirchenaustritt“ in Tabellenformaten. Das findet erstaunlich viel.
- Berichte aus der Zugriffssteuerung über Sites und Bibliotheken mit weit gefassten Freigaben – dort liegen die Altbestände.
- Und die unterschätzte Methode: eine Rundmail an alle Hauptamtlichen mit der Bitte, vorhandene Listen zu melden, verbunden mit einer Amnestie. Wer meldet, bekommt Unterstützung beim Aufräumen und keine Rückfragen. Das funktioniert in der Dienstgemeinschaft besser als jedes Werkzeug – vorausgesetzt, die Amnestie wird eingehalten.

Eine Landeskirche hat auf diesem Weg in sechs Wochen mehr Gemeindegliederlisten eingesammelt als in zwei Jahren technischer Suche. Der Preis war, dass die IT-Leitung tatsächlich niemandem etwas vorhielt, auch nicht der Person mit dem Vollexport von 2017 auf einem privaten Notebook. Das war unangenehm und richtig.

Wichtig: Wenn es doch passiert ist

Ein abgeflossener Gemeindegliederbestand ist eine meldepflichtige Verletzung des Schutzes personenbezogener Daten. Gemeldet wird nicht an die Landesdatenschutzbehörde, sondern an die kirchliche Aufsicht: den Beauftragten für den Datenschutz der EKD oder den zuständigen Diözesandatenschutzbeauftragten. Das KDG sieht dafür eine Meldung binnen 72 Stunden vor (§ 33 KDG); das DSG-EKD regelt die Meldung an die Aufsichtsbehörde in § 32 und die Benachrichtigung der betroffenen Personen in § 33.

Halte die Kontaktdaten der zuständigen Aufsicht dort bereit, wo sie im Ernstfall gebraucht werden – nicht im Intranet, das nach einem Verschlüsselungsvorfall gerade nicht erreichbar ist.

Häufige Fragen

Dürfen wir das Meldewesen nicht einfach in SharePoint abbilden, wenn wir es gut absichern?

Nein, und die Sicherheitsfrage ist dabei nicht einmal das Hauptargument. Das kirchliche Meldewesen ist in eine gesamtkirchliche Austauschstruktur eingebunden: Daten kommen aus den Melderegistern, sie werden beim Umzug zwischen kirchlichen Stellen weitergegeben, und der Austausch läuft über den Standard XKirche. Eine SharePoint-Liste kann daran nicht teilnehmen. Du würdest also nicht ein System ersetzen, sondern ein zweites, abgekoppeltes danebenstellen – und genau das ist der Zustand, den du beseitigen willst.

Wir sind eine kleine Kirchengemeinde ohne eigene IT. Gilt das alles trotzdem?

Ja, rechtlich uneingeschränkt. Praktisch heißt es aber etwas anderes als in einem Landeskirchenamt. Für eine kleine Gemeinde ist die richtige Antwort oft: keine Exporte, sondern Zugriff auf das Fachverfahren für die zwei Personen im Pfarramt, und für den Besuchsdienst eine Papierliste für den laufenden Monat, die zurückkommt. Das ist kein Rückschritt, sondern eine angemessene Maßnahme. Der Aufwand für Label, DLP und Kontoverwaltung lohnt sich erst ab einer gewissen Größe.

Darf der Besuchsdienst das Geburtsjahr erfahren?

Für die Aufgabe „Geburtstagsbesuch“ braucht es Tag und Monat sowie die Information, ob ein rundes oder hohes Jubiläum ansteht. Das vollständige Geburtsjahr ist dafür nicht erforderlich; es lässt sich bei Bedarf durch ein Kennzeichen ersetzen. Ob deine Gemeinde es trotzdem übergibt, ist eine Abwägung, die der Träger treffen und begründen muss. Sie einfach nur mitzuexportieren, weil das Feld im Bericht steht, ist keine Abwägung.

Wie lange darf ein Export im Team liegen bleiben?

So lange, wie der Zweck dauert, und keinen Tag länger. Für den Besuchsdienst ist das ein Monat, für den Gemeindebriefversand der Zeitraum bis zur Auslieferung, für einen Konfirmandenjahrgang der Kurs zuzüglich einer definierten Nachlauffrist, die dein Träger festlegt. Verlasse dich nicht auf Kalendereinträge, sondern auf eine Aufbewahrungsrichtlinie mit automatischer Löschung.

Kann Copilot auf Gemeindegliederdaten zugreifen?

Copilot arbeitet mit den Berechtigungen der anfragenden Person. Wenn eine Person auf einen Vollexport Zugriff hat, kann Copilot ihn für sie auswerten. Copilot erzeugt also kein neues Datenschutzproblem, sondern macht ein bestehendes sichtbar und schnell abrufbar. Genau deshalb gehört die Bereinigung der Altbestände vor den Rollout, nicht danach – und genau dafür

gibt es Restricted Content Discovery als befristetes Hilfsmittel, das allerdings nur für SharePoint-Sites gilt.

Brauchen wir für den Lettershop wirklich einen Vertrag?

Ja. Sobald ein externer Dienstleister personenbezogene Daten in deinem Auftrag verarbeitet – und Adressen für einen Versand sind genau das –, brauchst du eine Vereinbarung zur Auftragsverarbeitung nach § 30 DSG-EKD beziehungsweise § 29 KDG, mit Festlegung von Umfang, Art und Zweck der Verarbeitung, Datenarten und Betroffenenkreis. Die gute Nachricht: Seit der DSG-EKD-Novelle ist die Pflicht entfallen, säkulare Dienstleister der kirchlichen Aufsicht zu unterwerfen. Das war der Punkt, an dem früher die meisten Verhandlungen scheiterten.

Wir haben mehrere Tenants – Kirchenkreis, Gemeinden, diakonischer Träger. Ändert das etwas?

An der Rechtslage nichts, am Aufwand eine Menge. Jeder Tenant braucht eigene Label, eigene DLP-Richtlinien und eigene Aufbewahrung, und Exporte wandern zwischen Tenants besonders gern unkontrolliert hin und her. Wenn du die Tenant-Frage noch offen hast, entscheide sie vor der Exportregel und nicht danach.

Die Argumente dazu stehen in Ein Tenant oder viele? Kirchengemeinde, Kirchenkreis, Landeskirche, Bistum und die Frage der Tenant-Architektur.

Dürfen Gremienmitglieder Gemeindegliederdaten bekommen?

Nur, soweit es für die konkrete Gremienaufgabe erforderlich ist – etwa bei einer Wahl mit Wählerverzeichnis. Für die laufende Gremienarbeit reichen aggregierte Zahlen fast immer aus. Und Gremienmitglieder sind datenschutzrechtlich wie Ehrenamtliche zu behandeln: eigene Konten, Verpflichtung auf das Datengeheimnis, definierte Ablage, definiertes Ende der Amtszeit mit definiertem Entzug der Berechtigung.

Wie Gremienarbeit in Teams sauber aufgesetzt wird, steht in Gremienarbeit in Microsoft Teams: Presbyterium, Kirchenvorstand, Pfarrgemeinderat und Synode digital.

Was ist mit Daten, die wir selbst erhoben haben?

Die sind eine andere Kategorie und unterliegen nicht der Meldewesen-Logik. Wer sich für den Newsletter anmeldet, in den Chor eintritt oder sich für eine Freizeit anmeldet, gibt seine Daten unmittelbar der Gemeinde. Diese Daten dürfen in Microsoft 365 leben, sofern Rechtsgrundlage, Zweckbindung und Löschung geklärt sind. Der Fehler beginnt dort, wo selbst erhobene und aus dem Meldewesen stammende Daten in derselben Tabelle landen – dann gilt für die gesamte Tabelle das strengere Regime, und zwar dauerhaft.

Fazit

Das kirchliche Meldewesen gehört ins Fachverfahren des Rechenzentrums, und zwar nicht aus Traditionspflege, sondern weil es dort an eine Rechtskette angeschlossen ist, die Microsoft 365 nicht ersetzen kann: die Lieferung aus den Melderegistern nach § 42 Bundesmeldegesetz, den Austausch zwischen kirchlichen Stellen über XKirche, die Wirksamkeit von Sperrvermerken und Widersprüchen, die fortlaufende Aktualisierung.

Was in Microsoft 365 stattfindet, sind Auszüge. Und für Auszüge gilt eine Regel, die du auf eine Seite bekommst: benannter Zweck, reduzierter Feldsatz, angewendete Sperren, festgelegter Ablageort, begrenzter Zugriffskreis, technisch durchgesetztes Löschdatum. Die Technik dazu steht bereit – Sensitivity Labels, DLP mit Exact Data Match, Aufbewahrungsrichtlinien, bedingter Zugriff, für die Copilot-Phase Restricted Content Discovery. Nichts davon ist exotisch.

Der schwierige Teil ist der andere: die Bestandsaufnahme, die zutage fördert, was in fünfzehn Jahren gewachsen ist, und das Gespräch mit den Menschen, deren Liste verschwinden soll. Diese Menschen handeln nicht aus Nachlässigkeit, sondern weil sie ihre Arbeit machen wollten und das Fachverfahren ihnen nicht geholfen hat. Wenn du ihnen einen ordentlichen Bericht gibst, der in dreißig Sekunden die richtige Liste erzeugt, brauchst du überraschend wenig Überzeugungsarbeit.

Und wenn du dabei nur eine einzige Sache umsetzt, dann diese: Lass dir vom Rechenzentrum bestätigen, welche Exportberichte es gibt und welche davon Sperrvermerke auswerten. Der Rest ergibt sich aus der Antwort – manchmal schneller, als dir lieb ist.

Weiter lesen: Zum Weiterlesen

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

› 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

› Kirchliche Aufbewahrungsfristen, Kassationsordnungen und Archivgesetze in Microsoft Purview abbilden

› Copilot in Kirche und Diakonie: Nutzen, Grenzen, Oversharing und die Copilot-Überprüfung vor dem Rollout

› Die Cloud-Frage in der Kirche: Kirchliche Rechenzentren, Microsoft 365 und die Ehrlichkeit über Datenstandorte

› Microsoft 365 in Kirche, Diakonie und Caritas: Was wirklich anders ist als in Kommune und Mittelstand

Wenn du die Exportregel, das Label-Konzept und die Bestandsaufnahme nicht nebenbei stemmen willst: Wir begleiten kirchliche Träger dabei – Näheres unter Microsoft-365-Beratung für kirchliche Träger, und für die Einweisung von Haupt- und Ehrenamt gibt es Microsoft-365-Schulung für kirchliche Träger.