

Datenschutzrechtliche Bewertung des Einsatzes von Microsoft 365 (insbesondere Microsoft Teams) im BEFG-Kontext

Stellungnahme Bundesbeauftragten für Datenschutz des BEFG

Stand: 06.02.2025

Inhalt

1. Anlass, Ziel und Prüfraumen	2
2. Maßgebliche Normen der DSO-BUND	2
3. Sachliche Einordnung: Was bedeutet „Teams/M365“ datenschutzrechtlich?	3
4. Kernproblem I: Drittlandzugriff (Cloud Act/FISA) trotz EU-Cloud – rechtliche Bedeutung unter DSO-BUND	3
4.1 Aktuelle Erkenntnislage (Gutachten der Universität Köln).....	3
4.2 Cloud Act und DSO-BUND-Dogmatik.....	4
5. Kernproblem II: Aufsichtspositionen (DSGVO-bezogen) als Sachstandsindikator – Übertragung auf DSO-BUND	4
6. Kirchenspezifische Zuspitzung: erhöhte Schutzbedürftigkeit und Ehrenamt als Organisationsrisiko	5
6.1 Religiöse Daten sind im kirchlichen Alltag Regelfall, nicht Ausnahme	5
6.2 „Nur Seelsorgedaten nicht mit M365 nutzen“ ist häufig nicht beherrschbar.....	6
6.3 Ehrenamt: Systemtrennung und Schutzbedarfslogik sind im Alltag fehleranfällig...	6
7. Ergebnis der rechtlichen Bewertung (DSO-BUND)	6
7.1 M365 – ja oder nein?.....	6
7.2 Drittlandzugriff.....	7
8. Empfehlung des Datenschutzbeauftragten	7
8.1 Grundempfehlung: Alternativen sind im BEFG-Kontext regelmäßig vorzugswürdig .	7
8.2 Falls M365/Teams dennoch erwogen wird: Freigabe nur unter striktem, datenkategoriebasiertem Einsatzmodell	8
9. Zusammenfassendes Fazit	8

1. Anlass, Ziel und Prüfraahmen

Verantwortliche Stellen im Bund Evangelisch-Freikirchlicher Gemeinden in Deutschland K.d.ö.R. (BEFG) erwägen den Einsatz von **Microsoft 365 (M365)**, insbesondere **Microsoft Teams**, zur Kommunikation und Zusammenarbeit (Meetings, Chat, ggf. Dateiablage/OneDrive/SharePoint sowie Identitätsverwaltung).

Diese Stellungnahme bewertet, ob und unter welchen Voraussetzungen ein Einsatz **nach der Datenschutzordnung des BEFG – DSO-BUND (Stand 06/2025)** zulässig ist.

Kernproblem: In einer Kirche ist typischerweise von **erhöhtem Schutzbedarf** auszugehen, weil regelmäßig „besondere Daten“ berührt werden (u. a. religiöse Überzeugungen). Hinzu tritt ein strukturelles Organisationsmerkmal: Der BEFG ist in erheblichem Umfang auf die Arbeit **ehrenamtlicher Mitarbeiter** angewiesen. Daraus folgt das praktische Risiko, dass Datenklassifizierung und strikte „Systemtrennung“ im Alltag nicht jederzeit treffsicher gelingen. Diese organisatorische Realität muss zwingender Bestandteil der Risikoabwägung einer jeden verantwortlichen Stelle sein.

2. Maßgebliche Normen der DSO-BUND

Für die rechtliche Bewertung sind insbesondere folgende Normen maßgeblich:

1. **§ 3 Nr. 2 Begriffsbestimmung „besondere Daten“:** Darunter fallen ausdrücklich Daten, aus denen **religiöse oder weltanschauliche Überzeugungen** hervorgehen.
2. **§ 4 Seelsorgegeheimnis und Amtsverschwiegenheit:** Ordinierte Mitarbeitende dürfen für den Seelsorgeauftrag eigene Aufzeichnungen (auch mit besonderen Daten) führen; diese dürfen niemandem zugänglich gemacht werden; dafür sind geeignete technische/organisatorische Maßnahmen zu treffen.
3. **§ 5 Rechtmäßigkeit / Grundsätze:** Datenminimierung, Zweckbindung, Transparenz etc. sowie Erlaubnistatbestände (u. a. Rechtsvorschrift, Einwilligung, Erforderlichkeit für Aufgaben der Stelle einschließlich kirchlicher Aufsicht).
4. **§ 8 Verarbeitung besonderer Daten:** Grundsatz: **untersagt**; Ausnahmen u. a. bei ausdrücklicher Einwilligung oder – für nicht gewinnorientierte Stellen – bei Verarbeitung im Rahmen notwendiger Tätigkeiten **mit geeigneten Garantien (z. B. Verschlüsselung/Pseudonymisierung)** und ohne Offenlegung nach außen ohne Einwilligung.
5. **§ 18 Technische und organisatorische Maßnahmen:** risikoadäquate TOMs, regelmäßige Wirksamkeitsprüfung; Risiko insbesondere durch **unbefugte Offenlegung oder unbefugten Zugang** ist ausdrücklich zu berücksichtigen.

6. **§ 19 Verarbeitung im Auftrag:** Verantwortliche Stelle bleibt verantwortlich; nur Auftragsverarbeiter mit hinreichenden Garantien; schriftlicher Auftrag; Unterauftragsverarbeiter-Kontrolle; und zentral: **Drittlandbezug** – Sitz/Betriebsstätte im Drittland nur zulässig, wenn EU-Kommission für dieses Land ein angemessenes Datenschutzniveau beschlossen hat.
7. **§ 23 Datenschutz-Folgenabschätzung (DSFA):** DSFA vorab, wenn voraussichtlich hohes Risiko; „insbesondere“ bei **umfangreicher Verarbeitung besonderer Daten**.

3. Sachliche Einordnung: Was bedeutet „Teams/M365“ datenschutzrechtlich?

Microsoft Teams ist in M365 regelmäßig nicht nur Videokonferenz, sondern Kollaborationsplattform mit:

- Inhaltsdaten (Chat/Beiträge/Dateien/Meetings),
- Metadaten (Teilnahmen, Kontakte, Kommunikationsbeziehungen),
- Diagnosedaten/Telemetrie (Betrieb/Sicherheit/Produktverbesserung, je nach Konfiguration und Vertrags-/Dokumentationslage).

Im kirchlichen Kontext können schon Metadaten (z. B. Teilnahme an bestimmten Gruppen, Mitarbeit in Diensten, Seelsorgekontakte) Rückschlüsse auf **religiöse Überzeugungen** und Lebensumstände zulassen. Damit ist § 8 DSO-BUND (besondere Daten) praktisch häufig berührt.

4. Kernproblem I: Drittlandzugriff (Cloud Act/FISA) trotz EU-Cloud – rechtliche Bedeutung unter DSO-BUND

4.1 Aktuelle Erkenntnislage (Gutachten der Universität Köln)

Nach aktueller Berichterstattung (*u. a. heise online, www.heise.de*) zu einem öffentlich gewordenen Gutachten (Universität zu Köln, im Auftrag des BMI; Veröffentlichung im IFG-Kontext) bestehen weitreichende Zugriffsmöglichkeiten von US-Behörden auf Cloud-Daten auch dann, wenn diese in europäischen Rechenzentren gespeichert werden; maßgeblich sei nicht allein der Speicherort, sondern u. a. die Kontrolle durch US-Unternehmen und die Reichweite US-Rechtsgrundlagen (*z. B. CLOUD Act/SCA, FISA 702*).

Diese Erkenntnis ist im BEFG-Kontext von besonderer Bedeutung, weil bei kirchlichen Datenverarbeitungsvorgängen regelmäßig besondere Daten betroffen sein können und Seel-

sorge-/Vertrauenskontexte eine gesteigerte Schutzbedürftigkeit begründen (§ 4, § 8 DSO-BUND).

4.2 Cloud Act und DSO-BUND-Dogmatik

Ein absoluter Schutz vor dem Zugriff staatlicher Behörden oder unbefugter Dritter ist weder technisch realistisch noch normativ der Maßstab der DSO-BUND. Die DSO-BUND verlangt vielmehr ein **dem Risiko angemessenes Sicherheitsniveau** (§ 18) und – bei hohem Risiko – eine zusätzliche Datenschutzfolgenabschätzung (§ 23).

Aber: § 19 Abs. 3 DSO-BUND enthält eine klare Drittland-Schranke: Liegt der Sitz bzw. die Betriebsstätte des Auftragsverarbeiters (oder eine für die Verarbeitung benötigte Betriebsstätte) in einem Drittland, ist die Beauftragung nur zulässig, wenn die EU-Kommission für dieses Land ein angemessenes Datenschutzniveau beschlossen hat.

Aktuell existiert ein solcher Angemessenheitsbeschluss für die USA durch das **EU-US Data Privacy Framework (DPF)** der Kommission (*Durchführungsbeschluss (EU) 2023/1795*). Die Datenschutzkonferenz der Länder hat hierzu Anwendungshinweise veröffentlicht, die Reichweite und praktische Nutzung einordnen.

Konsequenz im DSO-BUND-Kontext:

- Cloud Act/FISA-Risiken führen nicht automatisch zu einem „Per-se-Verbot“.
- Sie bergen aber ein **erhebliches Restrisiko**, das in § 18-TOMs und § 23-DSFA zwingend zu adressieren ist – und das bei besonderen Daten/Seelsorgekontexten schnell die Schwelle zur **Unvertretbarkeit** erreichen kann.

5. Kernproblem II: Aufsichtspositionen (DSGVO-bezogen) als Sachstandsindikator – Übertragung auf DSO-BUND

Staatliche Datenschutzaufsichtsbehörden äußern sich naturgemäß zur DSGVO und nicht zur DSO-BUND. Diese Positionen sind daher für den BEFG nicht unmittelbar maßgeblich, sie bilden jedoch einen **relevanten Tatsachen- und Bewertungsrahmen** (Transparenz, Rollenverteilung, Telemetrie, Vertragslage, Drittlandrisiken), der unter der DSO-BUND analog zu prüfen ist (insb. § 18, § 19, § 23).

- Die **Datenschutzkonferenz (DSK)** hat in ihrer Festlegung vom 24.11.2022 zur damaligen Vertrags-/Dokumentationslage ausgeführt, dass Verantwortliche einen datenschutzgerechten Einsatz auf dieser Grundlage nicht nachweisen konnten (Transparenz- und Vertragsprobleme u. a.).
- Der **LfD Niedersachsen** hat für den öffentlichen Bereich erklärt, das Verhandlungsergebnis zur AV-Ausgestaltung für Teams sei „akzeptabel“, betont aber fortbeste-

hende Prüfpflichten, DSFA-Bedarf, Konfigurationsanforderungen sowie die fort-dauernde Prüfung von Alternativen (u. a. zur Vermeidung von Herstellerabhängigkeiten im Hinblick auf Software und Daten).

- Der **Hessische Beauftragte für Datenschutz und Informationssicherheit (HBDI)** hat am 15.11.2025 einen Bericht veröffentlicht, nach dem M365 unter bestimmten Voraussetzungen datenschutzkonform genutzt werden könne (allerdings innerhalb eng definierter Rahmenrichtlinien und innerhalb derer nur unter strengen Bedingungen).

Im Kontext des BEFG bzw. der DSO-BUND bedeutet dies: Selbst wenn einzelne Aufsichten (DSGVO-bezogen) inzwischen einen bedingten „Machbarkeitspfad“ sehen, bleibt für BEFG-Stellen zwingend: **Einzelfallprüfung, DSFA bei hohem Risiko, TOM-Härtung, belastbare Auftragsverarbeitung und Drittlandprüfung** (§§ 18, 19, 23 DSO-BUND) insbesondere unter Berücksichtigung der Verarbeitung personenbezogener Daten im religiösen Kontext (besondere Daten).

6. Kirchenspezifische Zuspitzung: erhöhte Schutzbedürftigkeit und Ehrenamt als Organisationsrisiko

6.1 Religiöse Daten sind im kirchlichen Alltag Regelfall, nicht Ausnahme

Die DSO-BUND qualifiziert analog zur DSGVO religiöse Überzeugungen als besondere Daten.

Praktisch können bereits Mitgliedschaftsbezüge, Gruppenmitarbeit, Mitarbeit in Diensten, interne Seelsorge- und Unterstützungsstrukturen oder Schutzkonzept-Kontexte zu einer Verarbeitung besonderer Daten führen. **Damit ist § 8 DSO-BUND nicht „Randnorm“, sondern bei nahezu jedem Datenverarbeitungsvorgang von zentraler Bedeutung.**

6.2 „Nur Seelsorgedaten nicht mit M365 nutzen“ ist häufig nicht beherrschbar

§ 4 DSO-BUND verlangt die besondere Abschottung seelsorgerlicher Aufzeichnungen; diese dürfen niemandem zugänglich gemacht werden und sind technisch/organisatorisch zu sichern.

Allein die Möglichkeit, dass seelsorgerliche Inhalte in Chat/Meeting-Chat/Dateiablage „landen“, stellt ein erhebliches Risiko dar. Ein Verbot, solche (besonderen) Daten in Microsoft 365 zu speichern kann jedoch nur dann wirksam sein, wenn es organisatorisch durchgesetzt und praktisch eingehalten wird (Kontrollen/Prozesse/Alternativwege). Dies ist realistisch betrachtet im Alltag nicht praktikabel.

6.3 Ehrenamt: Systemtrennung und Schutzbedarfslogik sind im Alltag fehleranfällig

Der oben beschriebene Ansatz: „Teams nur für Unkritisches, Sensibles in System X.“ birgt in einer Organisation mit hoher Ehrenamtsquote zudem ein unkalkulierbares Risiko. Es ist ernsthaft zu bezweifeln, dass Ehrenamtliche dauerhaft sicher einschätzen, wann welche Datenkategorie vorliegt und welches System zu verwenden ist. Dieser Umstand ist nicht zwingend auf ein „Schulungsdefizit“ zurückzuführen, sondern auch angesichts hoher Ehrenamtsfluktuation schlicht strukturelle Realität.

§ 18 DSO-BUND ist auch in diesem Kontext von besonderer Relevanz: Das Risiko unbefugter Offenlegung/unbefugten Zugangs ist im Rahmen der Erstellung ordnungsgemäßer TOMs ausdrücklich zu adressieren.

Wenn die Organisation die Einhaltung der Systemtrennung realistischerweise nicht sicherstellen kann, steigt jedoch die Wahrscheinlichkeit, dass besondere Daten (§ 8) in ein System geraten, dessen Drittlandzugriffs-Restrisiko nicht hinreichend beherrschbar ist.

7. Ergebnis der rechtlichen Bewertung (DSO-BUND)

7.1 M365 – ja oder nein?

Ein geplanter M365/Teams-Einsatz ist im Kontext der DSO-BUND **nicht automatisch verboten**, aber auch **nicht pauschal freigabefähig**. Maßgeblich ist eine szenarien- und schutzbedarfsbezogene Bewertung anhand von:

- **Rechtmäßigkeit/Zweck/Erforderlichkeit** (§ 5),
- **besondere Daten** (§ 8) und dafür erforderliche Garantien,
- **TOM-Niveau** (§ 18) einschließlich Minimierung und Schutz vor Offenlegung/Zugriff,
- **Auftragsverarbeitung/Drittland** (§ 19),
- **DSFA-Pflicht** (§ 23), insbesondere bei umfangreichen besonderen Daten.

7.2 Drittlandzugriff

Wie ausgeführt, kommt die Universität Köln in ihrem Gutachten zu dem Schluss, dass staatlicher US-Zugriff trotz EU-Hostings nicht sicher ausgeschlossen werden kann. Damit verbleibt ein Restrisiko, das bei kirchlichen Kerninhalten (Seelsorge, Konflikt-/Schutzkonzeptfälle, sensible Mitgliederangelegenheiten) regelmäßig **nicht** mehr als „tolerierbar“ bewertet werden kann – jedenfalls dann nicht, wenn nicht nachweisbar wirk-

same zusätzliche Schutzmechanismen (insbesondere echte Schlüssel-/Kryptokontrolle außerhalb der Anbieterhoheit) implementiert sind.

8. Empfehlung des Datenschutzbeauftragten

8.1 Grundempfehlung: Alternativen sind im BEFG-Kontext regelmäßig vorzugswürdig

Aufgrund (a) der hohen Wahrscheinlichkeit besonderer Datenverarbeitung (§ 8), (b) seelsorgerlicher Vertrauenskontexte (§ 4), (c) des Drittlandzugriffs-Restrisikos (Heise/Gutachten Universität Köln) und (d) der Ehrenamtsrealität (fehlertolerante Praxis nötig), empfehle ich, **zuerst** eine ernsthafte Prüfung **von Alternativen mit eigener Datenhoheit** vorzunehmen, z. B. Kollaborationslösungen mit EU/EWR-Betrieb und -Betreiber sowie eigenständiger Administrations- und Schlüsselhoheit. Eine „einheitliche“, kontrollierbare Lösung ist im Ehrenamtsbetrieb oft sicherer als eine sonst zwingende komplexe Zwei-System-Logik, die in Grenzfällen fehleranfällig ist.

Diese Empfehlung wird als „Sachstandsimpuls“ auch durch staatliche Aufsichtslinien gestützt, die – trotz teilweiser Annäherung – weiterhin Alternativenprüfung und Minimierung betonen (z. B. LfD Niedersachsen).

8.2 Falls M365/Teams dennoch erwogen wird: Freigabe nur unter striktem, datenkategoriebasiertem Einsatzmodell

Sofern aus zwingenden organisatorischen Gründen M365/Teams weiter in Betracht gezogen wird, ist aus DSO-BUND-Sicht mindestens Folgendes erforderlich:

1. **Vorab-DSFA nach § 23 DSO-BUND** (Pflichtfall naheliegend, da besondere Daten im kirchlichen Kontext typischerweise berührt werden).
2. **Auftragsverarbeitung nach § 19 DSO-BUND**: belastbare schriftliche Beauftragung, Unterauftragsverarbeiter-Kontrolle, Garantien und Dokumentationspflichten; Drittlandfrage nach § 19 Abs. 3 ausdrücklich prüfen und dokumentieren.
3. **TOM-Härtung nach § 18 DSO-BUND** (inkl. Wirksamkeitsprüfung): restriktive Default-Einstellungen, Datenminimierung, Zugriffskontrolle, Logging, Gast-/Sharing-Regeln, Verhinderung unbeabsichtigter Offenlegung.
4. **Inhaltliche Nutzungsgrenzen (Schutzbedarfsmodell)**:
 - **Kategorie A (vertretbar, wenn strikt gehärtet)**: rein organisatorische Kommunikation ohne sensible Inhalte; Termin-/Gremienkoordination ohne personenbezogene Problemlagen; allgemeine Information.

- **Kategorie B (nur mit zusätzlichen Sicherungen):** personenbezogene Vorgänge mit erhöhtem Diskretionsbedarf, jedoch ohne seelsorgerlichen bzw. religiösen Kern/Kontext; nur bei klaren Prozessen und minimaler Datenteilung.
 - **Kategorie C (auszuschließen):** Seelsorgeinhalte, besondere Konflikt-/Schutzkonzept-Sachverhalte, personenbezogene Fallarbeit mit erkennbarer religiöser/gesundheitlicher/sensibler Dimension, soweit nicht technisch eine Anbieter-unabhängige Schlüsselkontrolle/Abschirmung tatsächlich sichergestellt ist (§ 4, § 8, § 18 DSO-BUND).
5. **Ehrenamtsgerechte Governance:** Wenn Kategorien/Trennregeln eingeführt werden, müssen sie **fehlertolerant** sein. Ist realistischerweise nicht zu gewährleisten, dass Ehrenamtliche Grenzfälle korrekt entscheiden, spricht dies **gegen** eine Systemtrennung und **für** den Umstieg auf eine Lösung, die auch im „Fehlbedienungsfall“ das Risiko unbefugter Offenlegung minimiert (§ 18 Abs. 3 DSO-BUND).

9. Zusammenfassendes Fazit

1. In einer Kirche ist typischerweise von einem **erhöhten Schutzbedarf** auszugehen, weil regelmäßig „besondere Daten“ berührt werden (u. a. religiöse Überzeugungen).
2. M365/Teams ist im kirchlichen Umfeld typischerweise ein **Hochrisiko-Szenario**, weil besondere Daten und seelsorgerliche Kontexte nicht zuverlässig auszuschließen sind (§ 4, § 8).
3. Das aktuelle Gutachten der Universität Köln unterstreicht: **US-Behördenzugriff kann auch bei EU-Hosting praktisch nicht sicher ausgeschlossen werden**, sofern ein US-amerikanisches Unternehmen Betreiber der Cloudlösung ist.
4. Selbst wenn Drittlandmechanismen (EU-US Data Privacy Framework) formal einen Angemessenheitsrahmen bieten, bleibt unter DSO-BUND die **Pflicht, Restrisiken über § 18/§ 23 zu bewerten und ggf. bestimmte Verarbeitungen auszuschließen**.
5. Aufgrund der **Ehrenamtsstruktur** ist eine **komplexe Schutzbedarfs-/Systemtrennung im Alltag besonders fehleranfällig**; daher ist in vielen BEFG-Szenarien eine **strategische Präferenz für Alternativen** (z. B. EU/EWR-basierte, eigenkontrollierte Lösungen) die sachgerechtere Empfehlung. **Lösungen wie Nextcloud, Owncloud oder Open-XChange dürfte aus datenschutzrechtlicher Sicht der Vorzug zu geben sein.**