

BERICHT 2024/2025

DES DATENSCHUTZBEAUFTRAGTEN DES BUNDES FREIKIRCHLICHER PFINGSTGEMEINDEN KDÖR



Erzhausen, im Frühjahr 2026

1. Vorbemerkungen

Kommunikation, Organisation und Zusammenarbeit erfolgen auch in Gemeinden des Bundes Freikirchlicher Pfingstgemeinden zunehmend über digitale Werkzeuge und Plattformen. Cloud-Dienste, kollaborative Arbeitsumgebungen und soziale Medien sind vielerorts zu selbstverständlichen Hilfsmitteln geworden und erleichtern die Zusammenarbeit zwischen haupt- und ehrenamtlich Mitarbeiterinnen und Mitarbeitern.

Gleichzeitig entstehen dadurch neue Fragen im Umgang mit personenbezogenen Daten. Datenschutz ist kein statisches Regelwerk, sondern ein fortlaufender Prozess, der sich an technische und organisatorische Entwicklungen anpassen muss. Gerade im kirchlichen Kontext geht es dabei nicht nur um rechtliche Vorgaben, sondern auch um einen verantwortungsvollen Umgang mit den persönlichen Informationen der Menschen, die sich Gemeinden anvertrauen.

Im Berichtszeitraum rückte der Einsatz Künstlicher Intelligenz (KI) stärker in den Blick. Anwendungen zur Texterstellung, Bildbearbeitung oder Informationsverarbeitung sind inzwischen weit verbreitet und werden auch im kirchlichen Arbeitsumfeld genutzt. Damit verbunden sind neue datenschutzrechtliche Fragen, etwa zur Herkunft von Trainingsdaten, zur Transparenz automatisierter Prozesse oder zur Verantwortung bei der Nutzung solcher Systeme. Diese Entwicklung spiegelt sich auch in der europäischen Gesetzgebung wider, insbesondere im 2024 in Kraft getretenen AI Act.

Darüber hinaus war der Datenschutz durch zahlreiche Entwicklungen auf nationaler und europäischer Ebene geprägt. Neue Regelungen zur digitalen Infrastruktur, zu Plattformdiensten und zur IT-Sicherheit sowie Orientierungshilfen der Aufsichtsbehörden tragen dazu bei, die datenschutzrechtlichen Anforderungen weiter zu konkretisieren.

Für viele Gemeinden im Bund Freikirchlicher Pfingstgemeinden ist es jedoch nicht immer leicht, diese Entwicklungen im Blick zu behalten. Die Gemeindegarbeit wird in hohem Maß durch ehrenamtliches Engagement getragen, während datenschutzrechtliche Fragestellungen häufig neben

viele andere praktische Aufgaben treten. Umso wichtiger bleibt die beratende Unterstützung durch die Datenschutzaufsicht, um praktikable Lösungen zu finden, die sowohl den Anforderungen des Datenschutzes als auch den Bedürfnissen der Gemeindegarbeit gerecht werden.

Der vorliegende Tätigkeitsbericht gibt einen Überblick über die Entwicklung des Datenschutzes im Berichtszeitraum sowie über die Tätigkeit der Datenschutzaufsicht im Bund Freikirchlicher Pfingstgemeinden. Neben rechtlichen und technischen Entwicklungen werden auch typische Fragestellungen aus der Beratungspraxis aufgegriffen, um die praktische Umsetzung des Datenschutzes in Gemeinden und Einrichtungen zu verdeutlichen. Die BFP-Datenschutzordnung (BFP-DSO) bleibt dabei die zentrale Grundlage, um den kirchlichen Datenschutz im Einklang mit der Datenschutz-Grundverordnung (DSGVO) zu gewährleisten.

2. Auswahl rechtlicher Vorgaben und Veränderungen zum Datenschutz (2024–2025)

AI Act – KI-Verordnung

Der „AI Act“ ist die europäische KI-Verordnung (Regulation [EU] 2024/1689) und gilt als erster umfassender Rechtsrahmen der EU für künstliche Intelligenz.¹ Sie ist am 1. August 2024 in Kraft getreten, wirkt aber in der Praxis über gestaffelte Anwendungszeitpunkte: Nicht alles gilt sofort, sondern je nach Themenblock zu späteren Terminen. Der Ansatz im Kern ist eine Risikologik: KI-Systeme werden danach beurteilt, wie stark sie Grundrechte, Sicherheit oder wichtige Lebensbereiche beeinflussen. Systeme, die in sensiblen Bereichen eingesetzt werden (z. B. Beschäftigung, Bildung, kritische Infrastruktur) und daher strenge Anforderungen erfüllen müssen, werden als „Hochrisiko“-Anwendungen eingestuft. Die Verordnung enthält zudem Transparenzpflichten, etwa wenn Menschen mit KI interagieren oder Inhalte synthetisch erzeugt werden, damit Nutzerinnen und Nutzer nicht getäuscht werden. Insgesamt verschiebt der „AI Act“ den Fokus von (erhoffter) „Selbstregulierung“ hin zu verbindlichen Anforderungen an Anbieter und in Teilen auch an Betreiber, je nach Rolle und Risikoklasse.

Datentransfers in die USA – Entwicklung und Entscheidung zum Data Privacy Framework

Das „EU-U.S. Data Privacy Framework“ (DPF) ist ein Mechanismus für Datenübermittlungen personenbezogener Daten aus der EU in die USA, basierend auf einem Angemessenheitsbeschluss der EU-Kommission. In der Praxis ist das DPF vor allem relevant, weil Unternehmen Daten an DPF-zertifizierte US-Organisationen übertragen können, ohne für jede Übermittlung zusätzliche Standardmechanismen verhandeln zu müssen (wobei natürlich weiterhin Datenschutzpflichten bestehen, nur die Transfer-Rechtsgrundlage ist erleichtert). 2024 stand das Framework u. a. im Zeichen der Überprüfung und der anhaltenden juristischen und politischen Debatte, ob die US-Schutzmechanismen gegenüber staatlichem Zugriff ausreichen.

Eine zentrale Entwicklung im Berichtszeitraum war die gerichtliche Auseinandersetzung: Am 3. September 2025 bestätigte das Gericht der Europäischen Union (EuGH) die Wirksamkeit des DPF, indem es eine Klage auf Nichtigerklärung des Angemessenheitsbeschlusses abwies (Rechtssache T-553/23).² Praktisch bedeutet das, dass der aktuelle Angemessenheitsbeschluss zum EU-US Data Privacy Framework derzeit Rechtssicherheit für Datenübermittlungen an zertifizierte US-Anbieter wie Microsoft, Amazon oder Google bietet. Gleichzeitig sollten Verantwortliche ihren Datenaustausch

¹ <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai>

² <https://www.reuters.com/sustainability/boards-policy-regulation/eu-court-backs-latest-data-transfer-deal-agreed-by-us-eu-2025-09-03>

weiter rechtlich absichern, etwa durch Dokumentation der eingesetzten Dienste, vorbereitete Standardvertragsklauseln sowie technische Maßnahmen (z. B. Verschlüsselung oder EU-Hosting), falls der Beschluss künftig vom EuGH aufgehoben wird.³

Ausblick: „Digital Omnibus“ der EU-Kommission

Der von der Europäischen Kommission veröffentlichte „Digital Omnibus“ vom 19. November 2025⁴ zielt auf eine Vereinfachung und teilweise Deregulierung der europäischen Digitalgesetzgebung, insbesondere in den Bereichen Datenschutz, Cybersicherheit und Künstliche Intelligenz. Vorgesehen sind Änderungen an elf bestehenden Rechtsakten – darunter der DSGVO, dem Data Act und der NIS-2-Richtlinie – sowie eine stärkere Zusammenführung einzelner Datenregelwerke in einem reformierten Data Act. Parallel dazu soll der AI Act angepasst werden, insbesondere durch eine abgeschwächte Anwendung der Hochrisiko-KI-Vorgaben für kleine und mittlere Unternehmen sowie eine spätere Umsetzungsfrist. Ergänzend hat die Kommission Strategiepapier, weitere Verordnungsvorschläge (u. a. zur europäischen „Unternehmensbrieftasche“) und mehrere öffentliche Konsultationen gestartet, um zusätzliche Vereinfachungsmaßnahmen in der europäischen Digitalgesetzgebung zu prüfen.⁵

Novellierung des Bundesdatenschutzgesetzes

Im Frühjahr 2024 hat der Deutsche Bundestag in einer ersten Lesung über die „Novellierung des Bundesdatenschutzgesetzes“ (BDSG) beraten. Inhaltlich zielt der Entwurf u. a. darauf, die Datenschutzkonferenz (DSK) gesetzlich im BDSG zu institutionalisieren (also ihre Rolle und Arbeitsgrundlage im Gesetz zu verankern). Außerdem wurden im Entwurf Anpassungen bei Auskunfts-/Betroffenenrechten und weiteren Detailfragen des nationalen Datenschutzrechts adressiert.⁶

Umsetzung des DSA in nationales Recht

Der Digital Services Act (DSA) ist eine EU-Verordnung für digitale Dienste (Plattformen, Hosting-Dienste, Marktplätze usw.) und gilt EU-weit unmittelbar.⁷ Trotz dieser unmittelbaren Gültigkeit sind die EU-Mitgliedstaaten in der Verantwortung, die Zuständigkeiten, Verfahren und Aufsichtsinstrumente auf nationaler Ebene zu regeln. In Deutschland erfolgte dies über das Digitale-Dienste-

³ <https://www.heuking.de/de/news-events/newsletter-fachbeitraege/artikel/eug-bestaetigt-wirksamkeit-des-eu-us-data-privacy-framework.html>

⁴ https://germany.representation.ec.europa.eu/news/vereinfachung-der-digitalgesetzgebung-kommission-legt-paket-vor-2025-11-19_de

⁵ <https://www.brak.de/newsroom/newsletter/nachrichten-aus-bruessel/2025/ausgabe-21-2025-v-05122025/vereinfachungs-paket-fuer-den-digitalbereich-digitaler-omnibus-kom/>

⁶ <https://www.bundestag.de/dokumente/textarchiv/2024/kw20-de-bundesdatenschutzgesetz-1000382>.

Das BDSG ergänzt und konkretisiert die europäische Datenschutzgrundverordnung (DSGVO) an verschiedenen Stellen. U. a. enthält es eine Reihe von sogenannten Öffnungsklauseln, die eine nationale Spezifizierung bestimmter Vorschriften ermöglichen – zum Beispiel den Datenschutz im Beschäftigungsverhältnis und die Fälle, in denen eine Pflicht zur Benennung eines Datenschutzbeauftragten besteht.

⁷ Vgl. hierzu auch den Tätigkeitsbericht des BFP-Datenschutzbeauftragten 2022/2023.

Gesetz (DDG)⁸, das am 14. Mai 2024 in Kraft getreten ist und die nationale Umsetzung bzw. Ausgestaltung der DSA-Strukturen regelt. Inhaltlich geht es bei dieser „Umsetzung“ um Fragen wie: Welche Behörde ist Koordinator (z. B. „Digital Services Coordinator“), wie laufen Meldungen/Anordnungen, welche Sanktionsmöglichkeiten gibt es und wie wird die Zusammenarbeit mit EU-Stellen organisiert? Das DGG hat sowohl das Telemediengesetz (TMG) als auch das Netzdurchsetzungsgesetz (NetzDG) abgelöst und führt zudem ergänzende Gesetze für Bereiche ein, die vom DSA nicht abgedeckt werden.

⁸ <https://gesetz-digitale-dienste.de/>.

Relevant ist das DDG u. a. für den Webauftritt von Gemeinden und Einrichtungen des BFP. Statt auf § 5 TMG ist jetzt auf § 5 DDG zu verweisen.

3. Anwendung des Datenschutzes im BFP

Organisation der Datenschutzaufsicht

Die Datenschutzaufsicht im Sinne einer unabhängigen kirchlichen Aufsichtsbehörde⁹ wird im Bund Freikirchlicher Pfingstgemeinden durch den Datenschutzbeauftragten des Bundes wahrgenommen. Er leitet die Datenschutzaufsicht und vertritt diese auch nach außen. Seit dem Jahr 2015 nimmt Daniel Aderhold, der durch das BFP-Präsidium bestellt wurde, diese Aufgabe wahr. Die Tätigkeit wird in Teilzeit ausgeübt; der Dienstsitz befindet sich in der Geschäftsstelle des BFP in Erzhausen.

Zur Unterstützung der Gemeinden und Einrichtungen stellt der Bund über das Infoportal „datenschutz.bfp.de“ umfangreiche Materialien zur Verfügung. Die Plattform hat sich in den vergangenen Jahren als zentrale Anlaufstelle für Merkblätter, Vorlagen sowie kurze Informations- und Schulungsvideos etabliert und bietet den verantwortlichen Stellen eine praktische Hilfestellung bei der Umsetzung datenschutzrechtlicher Anforderungen.

Für die praktische Umsetzung des Datenschutzes vor Ort werden durch die jeweils Verantwortlichen in den Gemeinden und Einrichtungen örtlich Beauftragte für den Datenschutz bestellt. Diese werden der aufsichtsführenden Stelle gemäß § 23 Abs. 6 BFP-DSO gemeldet und unterstützen die Verantwortlichen bei der Umsetzung der datenschutzrechtlichen Vorgaben im jeweiligen Verantwortungsbereich.

Beratung und Unterstützung der Gemeinden

Ein wesentlicher Teil der Tätigkeit der Datenschutzaufsicht bestand im Berichtszeitraum erneut in der Beratung von Gemeinden, Werken und Einrichtungen des Bundes Freikirchlicher Pfingstgemeinden.¹⁰ Die eingehenden Anfragen spiegeln dabei die Vielfalt der datenschutzrechtlichen Fragestellungen wider, die sich aus der praktischen Gemeindegearbeit ergeben. Besonders häufig ging es um Fragen zum Umgang mit personenbezogenen Daten in der täglichen Kommunikation und Verwaltung der Gemeinden.

Mehrere Gemeinden wandten sich mit Fragen zur Übermittlung von Spendenbescheinigungen beziehungsweise Zuwendungsbestätigungen per E-Mail an die Datenschutzaufsicht. Dabei standen insbesondere die rechtlichen Voraussetzungen, mögliche Risiken sowie praktische Umsetzungsmöglichkeiten im Mittelpunkt. Ebenso häufig wurde nach der Gestaltung von Datenschutzhinweisen für Gemeindeglieder gefragt. Hier ging es u. a. um die Frage, welche Informationen

⁹ Vgl. Art. 91 Abs. 1 DSGVO i.V.m. §§ 26ff BFP-DSO.

¹⁰ Wie bereits in den letzten Berichten ausgeführt, gibt es in der Datenschutzordnung des BFP eine Opt-Out-Regelung (§ 1, Abs. 3, BFP-DSO) für rechtlich selbstständige Gemeinden und Einrichtungen. Allerdings hat keine der inzwischen über 1.095 Mitgliedsgemeinden des BFP im Berichtszeitraum davon Gebrauch gemacht.

Gemeinden bereitstellen müssen und in welchen Fällen eine Einwilligung der betroffenen Personen erforderlich ist.

Ein weiterer Schwerpunkt der Beratung betraf den Umgang mit Foto-, Video- und Bildmaterial. Gemeinden baten insbesondere um Unterstützung bei der Formulierung von Hinweisen auf Kontaktkarten oder Anmeldeformularen sowie um eine Einschätzung, unter welchen Voraussetzungen Fotos und Videos von Veranstaltungen – etwa in sozialen Netzwerken – veröffentlicht werden dürfen. In diesem Zusammenhang wurde wiederholt gefragt, ob und in welchen Fällen Veröffentlichungen auch ohne ausdrückliche Einwilligung einzelner abgebildeter Personen möglich sind und welche Rolle hierbei die Regelungen des Kunsturhebergesetzes spielen. Ebenfalls thematisiert wurden Löschfristen für Bildmaterial sowie Fragen zur Einholung und Dokumentation von Einwilligungen zum Recht am eigenen Bild.

Mehrfach gingen außerdem Anfragen zum Einsatz technischer Systeme und digitaler Dienste ein. Dazu gehörten Fragen zur Nutzung von Cloud-Diensten, insbesondere Office 365 und Microsoft Teams, zur Verwendung von Newsletter-Diensten wie Mailchimp sowie zur Auswahl datenschutzkonformer Messenger-Dienste als Alternative zu WhatsApp. Weitere Gemeinden baten um eine datenschutzrechtliche Einschätzung zum Einsatz von Künstlicher Intelligenz, zur Einführung eines papierlosen Büros oder zur Umsetzung eines IT-Sicherheitskonzepts. In diesem Zusammenhang wurden auch Empfehlungen zu grundlegenden Maßnahmen der Datensicherheit, etwa zur Nutzung von Antivirenprogrammen, Firewalls oder sicheren Kommunikationswegen, erbeten.

Auch organisatorische und rechtliche Fragen spielten eine wichtige Rolle. Verschiedentlich wurde nach den Voraussetzungen für die Bestellung eines örtlich Beauftragten für den Datenschutz gefragt, nach möglichen Personenkreisen für dieses Amt sowie nach der Vereinbarkeit dieser Aufgabe mit anderen Funktionen innerhalb der Gemeindeleitung. Ebenso wurden Fragen zur Rechtsgrundlage der Datenverarbeitung innerhalb der BFP-Gemeinden, zum Geltungsbereich der Datenschutzordnung, zu Auftragsverarbeitungsverträgen (AVV) sowie zu datenschutzkonformen Mitgliedsanträgen und Einwilligungserklärungen gestellt.

Weitere Fragestellungen betrafen etwa den zulässigen Personenkreis mit Zugriff auf Finanzinformationen, den datenschutzkonformen Versand von Sitzungsprotokollen, den Umgang mit Geburtstagslisten im Kindergottesdienst, die Erhebung von Daten von Kindern sowie die datenschutzrechtliche Bewertung von Mitgliederversammlungen im Livestream.

Darüber hinaus baten Gemeinden regelmäßig um eine Überprüfung ihrer Webseiten hinsichtlich der Einhaltung datenschutzrechtlicher Vorgaben. Auch Schulungsanfragen nahmen im Berichtszeitraum zu. Dabei ging es sowohl um allgemeine Datenschutzbildungen für örtlich Beauftragte als auch um spezifische Fragestellungen im Zusammenhang mit Gemeindesoftware, beispielsweise ChurchTools.

Aufsichtliche Maßnahmen und gemeldete Datenschutzvorfälle

Im Berichtszeitraum erreichten die Datenschutzaufsicht mehrere Meldungen über Datenschutzvorfälle sowie einzelne Beschwerden und Anfragen zu datenschutzrechtlichen Sachverhalten. Darüber hinaus wurde die Aufsicht in einzelnen Fällen auch von sich aus tätig. Die folgenden Beispiele geben einen Überblick über ausgewählte Vorgänge.

Im Oktober 2024 wurde der Datenschutzaufsicht eine Datenschutzpanne im Zusammenhang mit einem Newsletterversand gemeldet. Dabei wurden versehentlich 466 E-Mail-Adressen im CC-Feld statt im BCC-Feld eingefügt und damit für alle Empfänger sichtbar gemacht. Die verantwortliche Stelle informierte zeitnah über den Vorfall und setzte in Abstimmung mit der Datenschutzaufsicht geeignete organisatorische Maßnahmen um, um ähnliche Fehler künftig zu vermeiden.

Im November 2024 wurde ein Auskunftersuchen einer betroffenen Person bearbeitet und die verantwortliche Stelle bei der rechtmäßigen Beantwortung unterstützt.

Im Juni 2025 beanstandete die Datenschutzaufsicht ein Anmeldeformular für ein Jugend-Sommercamp, nachdem bei der Prüfung datenschutzrechtliche Mängel festgestellt worden waren. Dabei wurden gegenüber der verantwortlichen Stelle Maßnahmen zur Anpassung der Datenerhebung sowie zur Verbesserung der Transparenz ausgesprochen.

Im Juli 2025 erreichte die Datenschutzaufsicht eine Beschwerde wegen eines angeblichen Verstoßes gegen die Verschwiegenheitspflicht. Nach Prüfung des Sachverhalts stellte sich der Vorwurf als unbegründet heraus, sodass kein aufsichtsrechtliches Verfahren eingeleitet werden musste.

Ein weiterer gemeldeter Vorfall betraf im September 2025 das unberechtigte Verschieben und Löschen von rund 5.000 E-Mails durch eine Mitarbeiterin einer BFP-Einrichtung. Der Vorfall wurde gemeinsam mit der verantwortlichen Stelle aufgearbeitet. Dabei zeigte sich eine hohe Bereitschaft zur Zusammenarbeit und zur transparenten Aufklärung. Die E-Mails konnten durch einen Dienstleister wiederhergestellt werden. Durch organisatorische und technische Maßnahmen wurde sichergestellt, dass vergleichbare Datenverluste künftig verhindert werden können. Aufgrund der Umstände wurde von weiteren aufsichtsrechtlichen Maßnahmen abgesehen.

Darüber hinaus begleitete die Datenschutzaufsicht im Berichtszeitraum die Umstellung des Hosters für die Mailpostfächer des Bundes. In diesem Zusammenhang wurden unter anderem der neue Anbieter datenschutzrechtlich geprüft, Abstimmungen mit dem IT-Dienstleister vorgenommen sowie die Funktionsfähigkeit der technischen Umsetzung am Ende des Migrationsprozesses überprüft.

Im Datenschutzbeirat des Bundes wurden im Berichtszeitraum unter anderem Merkblätter zum Einsatz von Cloud-Diensten, zu Office 365 sowie zum Datenschutz in der Seelsorge erarbeitet. Darüber hinaus wurde mit der Überarbeitung und Evaluierung der derzeit geltenden BFP-Datenschutzordnung begonnen.

4. Ausblick

Die Vielzahl der Anfragen an die Datenschutzaufsicht im Bund Freikirchlicher Pfingstgemeinden zeigt, dass Datenschutz im Alltag der Gemeinden angekommen ist. Fragen zum Umgang mit personenbezogenen Daten, zu digitalen Diensten oder zu organisatorischen Abläufen werden zunehmend bewusst gestellt. Diese Entwicklung ist erfreulich, insbesondere vor dem Hintergrund des weiterhin wachsenden Bundes mit neuen Gemeinden, Projekten und Arbeitsbereichen.

Gleichzeitig bleibt die fortschreitende Digitalisierung eine Herausforderung. Viele digitale Werkzeuge und Plattformen sind heute leicht zugänglich und werden selbstverständlich in der Gemeindegemeinschaft eingesetzt. Dabei gilt jedoch weiterhin: Nicht alles, was technisch möglich ist, ist auch sinnvoll – und erst recht nicht automatisch datenschutzrechtlich zulässig. Gerade bei der Nutzung neuer digitaler Dienste ist daher eine sorgfältige Prüfung erforderlich.

Neben klassischen Themen wie Cloud-Diensten, Social Media oder digitalen Kommunikationsplattformen wird insbesondere der Einsatz Künstlicher Intelligenz (KI) in den kommenden Jahren an Bedeutung gewinnen. KI-Anwendungen werden bereits heute für Texterstellung, Bildbearbeitung, Übersetzungen oder organisatorische Aufgaben genutzt. Gleichzeitig wirft ihr Einsatz neue Fragen zum Umgang mit personenbezogenen Daten, zur Transparenz von Datenverarbeitungen sowie zur Verantwortung der jeweiligen Anwender auf.

Digitale Technologien können die Arbeit mit und für Menschen in vielerlei Hinsicht bereichern und erleichtern. Gleichzeitig bleibt es eine zentrale Aufgabe, bei der Auswahl und Nutzung solcher Systeme darauf zu achten, dass ein angemessenes Datenschutzniveau gewährleistet ist. Technische Innovationen dürfen nicht dazu führen, dass der Schutz persönlicher Daten aus dem Blick gerät.

Gerade in kirchlichen Kontexten ist der Schutz der Privatsphäre von besonderer Bedeutung. Menschen vertrauen sich Gemeinden häufig mit sehr persönlichen Anliegen an – etwa im seelsorgerlichen Gespräch, im Gebet oder im Rahmen gemeinschaftlichen Lebens. Dieses Vertrauen setzt voraus, dass personenbezogene Informationen verantwortungsvoll behandelt und geschützt werden.

Der Datenschutz kann daher auch künftig ein sichtbares Zeichen für einen respektvollen und verantwortlichen Umgang mit persönlichen Daten sein. Es bleibt das Ziel, Gemeinden und Einrichtungen des Bundes weiterhin zu informieren, zu beraten und für einen verantwortungsvollen Umgang mit personenbezogenen Daten zu sensibilisieren, damit ein hohes Datenschutzniveau im BFP auch in Zukunft gewährleistet ist.