



Erzdiözese
Freiburg

DATENSCHUTZ



JAHRESBERICHT 2020

REFERAT DATENSCHUTZ IM
ERZBISCHÖFLICHEN ORDINARIAT FREIBURG

Für den Zeitraum 01.11.2019 bis 31.12.2020
Vorgelegt Februar 2021
Redaktionsschluss: 18.01.2021

INHALT

1. Vorwort	2
2. Zuständigkeit	3
3. Arbeitsschwerpunkte	4
3.1. Website des Referates Datenschutz	4
3.2. Prüfung von Videokonferenzsystemen	4
3.3. Vororttermine	4
3.4. Schulungen	8
3.5. Nutzung privater IT-Systeme zu dienstlichen Zwecken	10
3.6. Diözesane IT-Projekte	11
3.7. Rahmen-Dienstvereinbarung IT-Einsatz und kirchlicher Datenschutz	11
4. Einzelne Themen	12
4.1. Veröffentlichungen	12
4.2. Privacy Shield	12
4.3. § 29 KDG Gesetz	13
4.4. Datenpannen	13
5. Ausblick	15
5.1. Datenschutzkonzept	15
5.2. Grundlagenschulungen digital	15

1. VORWORT

Zum 25.05.2018 ist die europaweit geltende Datenschutz-Grundverordnung (DS-GVO) in Kraft getreten. Zum 24.05.2018 wurde für den Bereich der Erzdiözese, der Kirchengemeinden, Kirchenstiftungen, der Caritasverbände sowie weiterer Kirchlicher Einrichtungen das diesem Gesetz weitgehend entsprechende Kirchliche Datenschutzgesetz (KDG) in Kraft gesetzt.

Die DS-GVO und das für den kirchlichen Bereich geltende KDG erhöhten die für den Schutz personenbezogener Daten relevanten Normen und Maßnahmen erheblich. In Folge des Inkrafttretens des Kirchlichen Datenschutzgesetzes (KDG) mit Wirkung vom 24.05.2018 wurde zum 15.07.2018 das Referat Datenschutz im Erzb. Ordinariat errichtet. Dessen Aufgabenstellung ist in aller Kürze wie folgt umschrieben: „Im Bereich der verfassten Kirche den Datenschutz voranbringen“.

Der Zeitraum, über den der zweite Jahresbericht des Referates Datenschutz reicht, beginnt Ende des Jahres 2019. Die Planung von Präsenzs Schulungen mit einem Schwerpunkt für ehrenamtlich Mitarbeitende war bereits realisiert; diese Schulungen waren hauptsächlich für die im Frühjahr 2020 neu zu wählenden Pfarrgemeinde- und Stiftungsräte gedacht.

Aber: Wie für alle anderen geschäftlichen und privaten Lebensbereiche galt auch hier:

Mit Corona und den deswegen erforderlichen Maßnahmen kam vieles anders:

Die bereits terminierten Präsenzs Schulungen mussten abgesagt werden; Keine Vororttermine, keine Präsenzsitzungen in der Lockdownphase ab März 2020.

Vorgesehene Veranstaltungen und Beratungstermine mussten abgesagt werden. Dafür ergaben sich Aufgabenschwerpunkte, die „vor Corona“ in der Form nicht vorstellbar waren:

- Eckpunkte für die Arbeit im Homeoffice mussten geklärt werden.
- Die Notwendigkeit, die fehlende persönliche Präsenz zu kompensieren, bedeutete für die Kommunikation mittels Videokonferenz eine enorme Nachfrage. Für das Referat Datenschutz bedeutete dies eine datenschutzrechtliche Prüfung vieler Videokonferenzsysteme.
- Herausfordernd war auch – wie für alle anderen Einrichtungen auch – die interne Kommunikation und die Kommunikation mit den betreuten Einrichtungen auf die neuen Gegebenheiten umzustellen.
- Die neuen Rahmenbedingungen bedeuteten auch für die Einrichtungen der Erzdiözese, sich umstellen zu müssen, mit neuen Themenschwerpunkten und neuen Arbeitsweisen. Diese Umstellungen führten für das Referat Datenschutz zu neuen Aufgabenstellungen (z.B. datenschutzrechtliche Prüfung von „Ostern digital“ im Bereich der Kirchengemeinden, oder „Homeschooling“ im Bereich der Schulen).

Trotz der Einschränkungen im Zusammenhang mit Corona kann festgehalten werden, dass die „Grundaufgaben“ des Referates Datenschutz mit den Beratungen vor Ort (teilweise mit integrierten Schulungen) erfüllt werden konnten (sh. dazu Ziff. 3.3 und 3.4 dieses Berichtes).

2. ZUSTÄNDIGKEIT

Die Zuständigkeit für den Bereich der verfassten Kirche bedeutet eine Zuständigkeit für die Erzdiözese mit ihren unselbständigen Einrichtungen und für die Kirchengemeinden mit ihren unselbständigen Einrichtungen. Das sind für den Bereich der Erzdiözese z.B. die Erzb. Kurie, das Erzb. Seelsorgeamt, die Kath. Akademie, die Verrechnungsstellen für Kath. Kirchengemeinden, die Erzb. Bauämter und für den Bereich der Kirchengemeinden die 224 Kirchengemeinden mit ihren u.a. Kindergärten, Kirchenchören, Büchereien, soweit nicht mit eigener Rechtspersönlichkeit ausgestattet.

Im Berichtszeitraum war das Referat personell mit dem Referatsleiter und weiteren vier vollzeitbeschäftigten Mitarbeiterinnen und Mitarbeitern ausgestattet. Das entspricht der vorgesehenen personellen Ausstattung.

Die Mitarbeitenden sind in der Funktion von betrieblichen Datenschutzbeauftragten i.S. der §§ 36 ff KDG eingestellt; die Einrichtungen der Erzdiözese und die Kirchengemeinden haben vom Angebot der Benennung vollständig Gebrauch gemacht, sodass von einer vollständigen Versorgung der Einrichtungen der Erzdiözese und der Kirchengemeinden mit betrieblichen Datenschutzbeauftragten gesprochen werden kann.

Zu den betrieblichen Datenschutzbeauftragten und ihren Zuständigkeiten wird auf die nachstehende Übersicht verwiesen. Die Kontaktdaten finden Sie auf der Website, sh. Ziff. 3.1 des Datenschutzberichtes:

Thomas Maier	Schulstiftung der Erzdiözese Freiburg (Verwaltung und Schulen), Kath. Fachschulen für Sozialpädagogik, Schulen im Bildungswerk der Erzdiözese Freiburg
Johannes Ries	Erzb. Kurie, Stiftungsverwaltung, Rechnungshof, Verrechnungsstellen für Kath Kirchengemeinden, Geschäftsstellen der drei Großen Gesamtkirchengemeinden, Bildungswerk der Erzdiözese Freiburg, Erzb. Seelsorgeamt, Ehe-Familien-Lebensberatungsstellen Katholische Hochschulgemeinden, Kirchliche Studienbegleitung, Kath Studierendenwohnheime in der Trägerschaft der Erzdiözese (Thomas-Morus-Burse, Edith-Stein-Haus, Collegium Sapientiae, St. Alban Haus), Sprachenkolleg für ausländische Studierende, Freiburg
Christian Weinmann	Kirchengemeinden in den Dekanaten Tauberbischofsheim, Mosbach-Buchen, Mannheim, Heidelberg-Weinheim, Wiesloch, Kraichgau, Bruchsal, Karlsruhe, Pforzheim; Dekanatsverbände
Elisabeth Adler-Gößmann	Kirchengemeinden in den Dekanaten Rastatt, Baden-Baden, Acher-Renchtal, Offenburg-Kinzigtal, Lahr, Endingen-Waldkirch, Freiburg, Breisach-Neuenburg, Wiesental, Dekanatsverbände
Alexander Kalinasch	Kirchengemeinden in den Dekanaten Schwarzwald-Baar, Neustadt, Waldshut, Hegau, Zollern, Sigmaringen-Meißkirch, Konstanz, Linzgau; Dekanatsverbände

3. ARBEITSSCHWERPUNKTE

3.1. Website des Referates Datenschutz

Die betreuten Einrichtungen sind regional und strukturell breit gestreut. Die Website hat deswegen zentrale Bedeutung für die Kommunikation von Rechtsgrundlagen, Informationen, Mustern und Arbeitshilfen. Das Referat Datenschutz hat großen Wert auf den Aufbau und die Bestückung der Website gelegt. Die Website als Informationsplattform wird regelmäßig aktualisiert und weist unter der Rubrik Aktuelle Informationen u.a. auf neue bzw. aktualisierte Beiträge hin.

www.ebfr.de/datenschutz

3.2. Prüfung von Videokonferenzsystemen

Die Erzdiözese hat im Mai 2020 eine Auswahl empfohlener Systeme für Videokonferenzen zusammengestellt. Diese Auswahl soll Kirchlichen Einrichtungen zur Orientierung dienen. Die empfohlenen Lösungen sind:

- Skype
- Jitsi Meet
- WebEx
- GoToMeeting
- Zoom

Die Empfehlung der Erzdiözese ist ergänzt um allgemeine datenschutzrechtliche Hinweise.

Hinweise zum Abschluss eines Vertrages über die Auftragsverarbeitung und die erforderlichen Datenschutzhinweise sind, jeweils angepasst an die einzelnen Konferenzanbieter, auf der Website des Referates Datenschutz eingestellt; Die Datenschutzhinweise sowie die Empfehlungen der Erzdiözese finden Sie im Register Videokonferenzsysteme:

www.ebfr.de/datenschutz

3.3. Vororttermine

Vororttermine haben eine hervorgehobene Bedeutung für das Sensibilisieren der Verantwortlichen vor Ort in Sachen *Datenschutz* sowie zur Aufnahme der IST-Situation und zum Ableiten von erforderlichen Maßnahmen.

Trotz coronabedingter Einschränkungen hat das Referat Datenschutz seine Planung, bis Ende des Jahres 2020/ bis Frühjahr 2021 einen Ersttermin in 90% der Einrichtungen gehabt zu haben aufrecht gehalten und wie in der nachstehenden Tabelle skizziert, durchgeführt (Die Durchführung eines Ersttermins wird im übrigen nach wie vor in Präsenzform durchgeführt, weil die Begehung der Einrichtung im Blick auf die Zutrittssituation, die Verortung von IT-Technik und Archiv, die Situation der einzelnen Arbeitsplätze usw. unabdingbar ist).

Tatsächlich durchgeführt, bzw. zumindest fest terminiert bis Frühjahr 2021 sind:

Erzdiözese	100%
Schulen	100%
Kirchengemeinden/Dekanatsverbände	60-77% (Korridor in den jeweiligen Zuständigkeiten)
Kindergärten	33%

Vororttermine in den Kindergärten, Schulungen von Kindergartengeschäftsführungen und von Kindergartenleitungen wurden im Berichtszeitraum neu als Aufgabe hinzugenommen.

Feststellungen aus den Vorortterminen:

Grundwissen zum Thema Datenschutz ist in den Einrichtungen vorhanden. Der Datenschutz war auch vor dem Inkrafttreten des KDG bereits Thema in den Einrichtungen und den Verantwortlichen nicht unbekannt.

Dennoch ist sowohl der Wissensstand als auch die Umsetzung von Maßnahmen unterschiedlich ausgeprägt. Die Einrichtungen zeigen sich durchweg im Kontakt mit den betrieblichen Datenschutzbeauftragten aufgeschlossen und interessiert. Auch hier: Bei allen Einrichtungen, unabhängig von der Trägerschaft, erfordern die coronabedingten Maßnahmen eine Umstellung der Arbeitsweise mit Auswirkungen (auch) auf datenschutzrechtliche Fragestellungen; diese sind Fragestellungen z.B. im Hinblick auf die Zulässigkeit und die Rahmenbedingungen von Videokonferenzsystemen oder nach Datenschutzhinweisen für Coronakontaktverfolgungsformulare.

Einrichtungen der Erzdiözese:

Allgemein ist festzustellen, dass in den Bistumseinrichtungen die Sensibilität für die Anforderungen des Datenschutzes seit der Einführung des KDG spürbar zugenommen hat.

In den meisten zentralen Bistumseinrichtungen wurden inzwischen Erstbesuche durchgeführt. Begonnen wurde auch mit sog. Zweitbesuchen, die vor allem dazu dienen, den Status der beim Erstbesuch protokollierten Hinweise und Empfehlungen zu überprüfen und die weitere Vorgehensweise zu besprechen.

Regeltermine (jour fixe) werden inzwischen mit den Verantwortlichen im Bildungswerk, Diözesanstelle IT, EFL-Diözesanstelle, Erzb. Ordinariat (Hauptabteilung 7, Referatsleitung Verrechnungsstellen), Erzb. Seelsorgeamt, Institut für Pastorale Bildung und der Katholischen Akademie durchgeführt. Die Termine dienen dazu, den Verantwortlichen bei der Umsetzung der KDG-Konformität zu beraten und zu unterstützen. Es ist geplant, in weiteren Bereichen Regeltermine einzuführen.

Technische und organisatorische Maßnahmen gem. § 26 KDG sind, soweit diese die Gebäudesicherheit betreffen, in der Regel vorhanden. Da die Bistumseinrichtungen dem ITTAI-Projekt angeschlossen sind, sind auch angemessene technische Maßnahmen zur IT-Sicherheit umgesetzt. Diese Maßnahmen werden im Rahmen der Prüfaufgaben des betrieblichen Datenschutzbeauftragten im Einzelfall bewertet werden, da durch die unterschiedlichen Aufträge und Aufgabe der Einrichtungen auch unterschiedliche Risiken zum Tragen kommen können.

Verträge über Auftragsverarbeitung gem. § 29 KDG, die seit dem 31.12.2019 vorliegen müssen, sind entweder abgeschlossen oder aktuell in Arbeit. Im Rahmen der Beratungsaufgaben unterstützt das Referat Datenschutz die Erstellung und die Änderung bestehender Verzeichnisse.

Das Verzeichnis von Verarbeitungstätigkeiten (§ 31 KDG) wurde in den meisten Einrichtungen erstellt. Das Verzeichnis wird durch die Verantwortlichen geführt. Vereinbart wurde, dass der betriebliche Datenschutzbeauftragte über den Bearbeitungsstand der Verzeichnisse informiert wird.

Schulen (Trägerschaft der Schulstiftung, Fachschulen für Sozialpädagogik, 2. Bildungsweg):

Die Sensibilität für Fragen des Datenschutzes ist im Bereich der Schulen insgesamt recht gut ausgebildet. Datenschutz ist in Schulen „schon immer“ ein Thema gewesen.

Hinsichtlich der IT-Architektur, der Anschaffung von Hardware und Software, Benutzermanagement, Passwortrichtlinien usw. sind die Schulen sehr autonom und individuell. Es sind dazu nur wenige Rahmenbedingungen vorgegeben.

Mit der Besetzung einer Stelle *IT/ Digitalisierung* hat die Schulstiftung der Erzdiözese Freiburg einen wichtigen Beitrag zur Professionalisierung der IT in ihren Schulen geleistet.

Einige Schulen (Fachschulen für Sozialpädagogik und 2. Bildungsweg) haben auf ITTAI umgestellt oder sind dabei umzustellen. Die Sicherheitsstandards von ITTAI erhöhen im Zweifel die datenschutzrechtlichen Standards gegenüber dem status quo und sind daher aus Sicht des Datenschutzes zu begrüßen.

Beschreibung von ITTAI:

ITTAI ist eine zentrale Plattform für die Bereitstellung von IT Diensten. Im Gegensatz zur EBO-Cloud wird hierbei dem Anwender jedoch nicht nur ein Desktop per Bildschirmübertragung zur Verfügung gestellt; auch die gesamte weitere IT-Infrastruktur (wie z.B. Drucker, Switches, Firewall, Router, Internetzugang) ist standardisiert. Die Abkürzung von ITTAI steht für IT Transition Application Infrastructure, was übersetzt für die Überführung auf die standardisierte Anwendungs- und IT-Infrastruktur steht.

Kirchengemeinden/ Dekanate:

Aufgrund der Vor-Ort-Besuche von Pfarrbüros und Kindergärten sowie von Dekanatsbüros lässt sich festhalten, dass dem Datenschutz eine große praktische Bedeutung zukommt.

Von Seiten der betrieblichen Datenschutzbeauftragten galt es viele Fragen zu beantworten, Grundlagenwissen zu vermitteln bzw. zu vertiefen und praktische Hilfestellung bei der Umsetzung des neuen Datenschutzrechts in den jeweiligen Einrichtungen zu geben. Diese Hilfe wurde dankbar angenommen.

Wie bei den Schulungen auf Diözesanebene wurden auch bei den Vor-Ort-Besuchen die folgenden Themenschwerpunkte vermittelt: Verzeichnis von Verarbeitungstätigkeiten, Auftragsverarbeitung, Verpflichtungserklärung, Konzept für Mitarbeiterschulungen, technische und organisatorische Maßnahmen.

Diese 5 Punkte sind Prüfungspunkte des Katholischen Datenschutzzentrums Frankfurt a.M. (KDSZ). Daraus lässt sich zum einen die Wichtigkeit der Umsetzung dieser 5 Punkte für den Schutz personenbezogener Daten ableiten. Zum anderen stellen sich Einrichtungen gut auf für den Fall einer Prüfung durch das KDSZ.

Wichtig:

Ein gutes Datenschutzniveau setzt maßgeblich ein hohes Maß an IT-Sicherheit voraus. Für den Bereich der Kirchengemeinden bietet die Erzdiözese hierzu die EBO-Cloud an. Den Kirchengemeinden wird empfohlen, diesen IT-Standard zu nutzen.

Festzuhalten ist allerdings, dass EBO-Cloud nicht alle Themen der IT-Sicherheit abdeckt.

Abgedeckt ist z.B.:

- Der Einsatz einer hochverfügbaren Server-Farm (Exchange-Server, File-Server, etc.).
- Die zentrale Administration und das zentrale Monitoring der Server-Farm.
- Die zentrale und sichere Dateiablage auf dem EBO-File-Server.
- Der gesicherte Zugriff auf die Daten von unterschiedlichsten Standorten und Geräten.
- Eine tägliche Datensicherung.
- Der Einsatz aktueller Sicherheitstechnik (zentral überwachte Antiviren-Lösung, Firewall und Patch-Management, etc.) für die Kommunikation und zum Schutz der Daten innerhalb der EBO-Cloud.
- Ein zentraler Spamschutz.
- Die Erstellung und Umsetzung eines Benutzer- und Berechtigungskonzepts.
- Die Einbindung neuer IT-Systeme in das vorhandene, einrichtungseigene Netzwerk.
- Die Basis-Installation der Programme für den EBO-Cloud-Zugriff und die Einrichtung der Antivirus und Mail-Security auf den IT-Systemen.

Nach wie vor vor Ort zu lösen sind z.B.:

- Die Planung und Beschaffung neuer IT-Systeme (z.B. PCs, Laptops, Peripherie, Netzwerk, etc.).
- Die Grundkonfiguration neuer IT-Systeme (insbesondere Sicherheitseinstellungen, Datenschutz-Einstellungen der lokalen Betriebssysteme).
- Die Administration und das Monitoring der lokalen IT-Systeme, gemeint sind die Bestandteile außerhalb der EBO-Cloud.
- Die Erstellung eines gesamtheitlichen IT-Sicherheitskonzepts für die Einrichtung (Dokumentation der getroffenen IT-Sicherheitsmaßnahmen).
- Die Erstellung von Systemplänen, Hardwarelisten, etc. für die Einrichtung.
- Die Implementierung einer E-Mail Verschlüsselungslösung [§ 6 Abs. 1 b) KDG-DVO].
- Die Umsetzung einer Datenträgerverschlüsselung auf den IT-Systemen [§ 6 Abs. 1 b) KDG-DVO].
- Die Planung und Durchführung regelmäßiger IT-Sicherheitsschulungen (Informationssicherheit) für die Mitarbeiter der Einrichtung [§ 15 Abs. 3 KDG-DVO].
- Die regelmäßige Überprüfung der getroffenen technischen und organisatorischen Maßnahmen bzgl. IT-Sicherheit [§ 7 KDG-DVO].
- Die regelmäßige Prüfung der beauftragten örtlichen IT-Dienstleister (Auftragsverarbeiter) [§ 15 Abs. 5 KDG-DVO].
- Die Umsetzung von Maßnahmen zur „sicheren“ Datenträgerlöschung und Datenträgerentsorgung.
- Die Planung und Umsetzung einer, im Sinne § 20 KDG-DVO, datenschutzkonformen IT-Lösung für die ehrenamtlichen Mitarbeiter der Einrichtung.

3.4. Schulungen

Die Durchführung von Schulungen ist zentral für die Aufgabenstellung des Referates Datenschutz: „...den Datenschutz voranbringen“.

Mit Schulungen soll die Logik und die Sinnhaftigkeit von datenschutzrechtlichen Regelungen vermittelt werden. Deren Kenntnis ist Voraussetzung dafür, dass der Datenschutz Eingang findet in die alltäglichen Handlungen. Das Referat Datenschutz geht den Schulungsbereich aktiv an; gleichzeitig werden gerne aber auch Schulungen bei Anfragen von Einrichtungen durchgeführt.

Online-Schulung für den kirchlichen Datenschutz

Unter dem Label oskd (Online-Schulung für den kirchlichen Datenschutz) wurde in den Berichtszeiträumen 2019 und 2020 für 3.250 Mitarbeitende der Erzdiözese (u.a. Mitarbeitende der Erzb. Kurie, des Erzb. Seelsorgeamtes, der Verrechnungsstellen für Kath. Kirchengemeinden und die Priester) eine online-Schulung angeboten.

Der größte Teil der Mitarbeitenden der Erzdiözese Freiburg hatte damit die Möglichkeit einer digitalen Grundlagenschulung im Bereich *Datenschutz*.

Die Möglichkeit der online-Schulung steht neuen Mitarbeitenden nach wie vor zur Verfügung.

Präsenzs Schulungen:

Die bereits geplanten 6 Grundlagenschulungen, verteilt über die gesamte Erzdiözese, mussten, wie im Vorwort erwähnt, abgesagt werden. Vergleichbare, breit aufgestellte Schulungsformate konnten im Berichtszeitraum nicht durchgeführt werden.

Dennoch konnten spezifische Schulungen, z.B. berufsgruppen- oder einrichtungsbezogen durchgeführt werden.

Schulungsformate mit reduzierter Teilnehmerzahl wurden auch nach Anfrage durch die verantwortlichen Ansprechpersonen von den betrieblichen Datenschutzbeauftragten vor Ort durchgeführt.

Das Schulen und Sensibilisieren gehört zu den Kernaufgaben der betrieblichen Datenschutzbeauftragten. Deswegen wird unter den nachfolgenden Gliederungsziffern nochmals auf Schulungen in den einzelnen Bereichen eingegangen:

3.4.1. Schulungen Bistumseinrichtungen

Durch die Corona-Einschränkungen wurde nur eine Schulung vor Ort (Verrechnungsstelle) durchgeführt. Alle weiteren Sensibilisierungsmaßnahmen erfolgten digital. Auf Anfrage der Bundesarbeitsgemeinschaft Familie und Betrieb e.V. wurde bei deren Jahrestagung über Videokonferenz ein Fachreferat „Datenschutz in der landwirtschaftlichen Familienberatung“ gehalten. Der Erstkontakt war über das Erzb. Seelsorgeamt erfolgt.

3.4.2. Schulungen für den Bereich der Schulen

Schulen in der Trägerschaft der Schulstiftung:

Fachtag Datenschutz	Aufbauschulung Datenschutz	Nov. 2019
Gesamt MAV aller Stiftungsschulen	Grundlagen/ spezifische Themen	Nov. 2019
Schulsekretärinnen	Grundlagen/ spezifische Themen	Okt. 2020

Sachthemen:

- Datenpannen
- E-Mail-Kommunikation mit Eltern
- Weitergabe von Adressen (an Eltern/ Elternbeiräte/ Kirchengemeinden)
- Umgang mit dem Fotografieren

3.4.3. Schulungen Kirchengemeinden/ Dekanate

Kirchengemeinden/ Pfarrbüros/ Dekanatsbüros

3 x Schulungseinheit Datenschutz beim Aufbaukurs für Pfarrsekretärinnen des Institutes für Pastorale Bildung (IPB)	Grundlagen
--	------------

Vors. Stiftungsrat, Pfarrsekretärinnen, teilw. Pastorale MA), Dekane, Dekanatssekretärinnen, teilw. Dekanatsreferenten	Grundinformation; Themenschwerpunkte: Verzeichnis von Verarbeitungstätigkeiten, Auftragsverarbeitung, Verpflichtungserklärung, Konzept für Mitarbeiterschulungen, Technische und organisatorische Maßnahmen Erläuterung von Fristen gem. KDG-DVO
--	--

Sachthemen:

- Rechtsgrundlagen und Informationspflicht u.a. bei Amtshandlungen, im Besuchsdienst, bei Trauergesprächen, im Bewerbungsverfahren, bei Vermietung Gemeindehaus
- Umgang mit Auskunftersuchen
- Erstellung und Veröffentlichung von Fotos im Gottesdienst, bei kirchlichen Veranstaltungen, bei Ferienfreizeiten, etc.
- Verschiedene IT-technische Fragestellungen
- Nutzung der Privat-IT für geschäftliche Zwecke durch ehrenamtliche Mitarbeiter (BYOD, Bring Your Own Device)
- Umgang mit Datenpannen
- Beratung bei Datenschutzfolgeabschätzungen (insbesondere Videoüberwachung)
- Erläuterung von Datenschutzklassen und damit verbundenen IT-Sicherheitsaspekten gem. KDG-DVO

Kirchengemeinden/ Kindertagesstätten

Kindergartengeschäftsführungen, Kindergartenleitungen	Grundinformation; Themenschwerpunkte: Verzeichnis von Verarbeitungstätigkeiten, Auftragsverarbeitung, Verpflichtungserklärung, Technische und organisatorische Maßnahmen Erläuterung von Fristen gem. KDG-DVO
---	--

Sachthemen:

- Weitergabe von personenbezogenen Daten an Ämter, Kommunen, Eltern, Elternbeirat, etc.
- Erstellung von Listen, z.B. Geburtstagslisten, Telefonlisten, etc.
- Aufnahmevertrag
- Einsatz spezieller Kita-Software (Kid-Kita, Kita-Info-App, etc.)
- Umgang mit Datenpannen
- Erstellung und Veröffentlichung von Fotos im Kindergarten, bei
- Veranstaltungen, etc.
- Verschiedene IT-technische Fragestellungen
- Erläuterung von Datenschutzklassen und damit verbundenen IT-Sicherheitsaspekten gem. KDG-DVO

3.5. Nutzung privater IT-Systeme zu dienstlichen Zwecken

Die Verarbeitung personenbezogener Daten auf privaten IT-Systemen zu dienstlichen Zwecken ist gem. § 20 Abs. 1 der Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO) grundsätzlich verboten. Die Voraussetzungen für eine Zulassung im Einzelfall durch den Verantwortlichen sind sehr hoch (§ 20 Abs. 2 KDG-DVO), so dass davon auszugehen ist, dass in der Praxis eine rechtskonforme Verarbeitung personenbezogener Daten auf privaten IT-Systemen eher nicht erfolgt.

Hinweise auf die Rechtslage in Schulungen und in Vorortterminen erfolgen durch das Referat Datenschutz. Zur Auflösung dieses Dilemmas wird aber parallel darauf hingewirkt, dieses aufzulösen. Hierbei sind Ansätze:

- Die Anschaffung dienstlicher Laptops (mit professioneller technischer Betreuung)
- Eine technische Lösung, die es ermöglicht, die Datenverarbeitung auf einem „virtuellen Desktop“ vorzunehmen, sodass die Verarbeitung von vornherein (zwar mit) aber nicht auf dem privaten Gerät erfolgt.

Die Entscheidungen/ Umsetzungen liegen hierbei nicht im Verantwortungsbereich des Referates Datenschutz; es ist jedoch ein großes Anliegen, dieses „Datenschutzdilemma“ aufzulösen. Das Referat Datenschutz unterstützt deswegen die Verantwortlichen bei Anstrengungen, die in die oben skizzierte Richtung gehen.

Im Zusammenhang mit der Bearbeitung dieser Thematik ist auch eine Neufassung der *Verpflichtungserklärung Ehrenamt* erfolgt (sh. Ziff. 4.1).

Ohne größere inhaltliche Veränderungen vorzunehmen wurde getrennt zwischen allgemeingültigen Bestimmungen und Bestimmungen, die zusätzlich für ehrenamtlich Mitarbeitende gelten, die personenbezogene Daten digital verarbeiten.

3.6. Diözesane IT-Projekte

Mit der Einführung neuer IT-Systeme sind immer Folgen für den Schutz personenbezogener Daten zu berücksichtigen. Dafür steht neben dem Instrument der Datenschutz-Folgenabschätzung der betriebliche Datenschutzbeauftragte zur Beratung zur Verfügung. In diesem Zusammenhang wurde der Verantwortliche im Berichtszeitraum unter anderem in folgenden Projekten beraten:

- KIDICAP Neo und Personal Office in Nachfolge des SAP-Projektes
- IBO – Neue Prüfsoftware Rechnungshof
- SemiQ - Software für Seminarverwaltung mit integriertem Hotelmanagement in Bildungs- und Übernachtungseinrichtungen
- Dienstmartphones für Seelsorger
 - In Zusammenarbeit mit der Diözesanstelle IT Erstellung der IT-Sicherheitsanforderungen

3.7. Rahmen-Dienstvereinbarung IT-Einsatz und kirchlicher Datenschutz

Das Erzbischöfliche Ordinariat hat im April 2020 an die Kirchengemeinden und selbständigen Einrichtungen der Erzdiözese die Rahmendienstvereinbarung IT-Einsatz *und* *Datenschutz* versandt verbunden mit der Bitte, diese mit der jeweiligen MAV abzuschließen.

Die Rahmendienstvereinbarung dient als Grundlage für den Abschluss von Einzeldienstvereinbarungen zur Einführung mitbestimmungspflichtiger IT-Systeme.

Die Rahmendienstvereinbarung ist auf der Homepage der Erzdiözese Freiburg unter www.ebfr.de/mdv-sap zu finden.

Die Rahmendienstvereinbarung ist komplex und umfangreich.

Das Referat Datenschutz hat die Erarbeitung der Dienstvereinbarung begleitet und unterstützt die Kirchengemeinden/ Einrichtungen bei Rückfragen zu datenschutzbezogenen Themen.

4. EINZELNE THEMEN

4.1. Veröffentlichungen

Mit dem Verweis auf die Website und die verschiedenen Dokumente, die dort hinterlegt sind, wird an dieser Stelle vor allem auf folgende Veröffentlichung hingewiesen:

Im Register *Muster und Arbeitshilfen unter Verpflichtungserklärung das Dokument Verpflichtungserklärung Datengeheimnis:Ehrenamt.*

Dieses Dokument bitte für neue Verpflichtungen verwenden; die Wirksamkeit von Verpflichtungen mit dem bisherigen Dokument bleibt jedoch bestehen.

4.2. Privacy Shield

Die Verarbeitung personenbezogener Daten innerhalb der EU ist auf der Grundlage der Datenschutz-Grundverordnung (DS-GVO) zulässig. Eine Übermittlung in ein Drittland (das sind alle Länder außerhalb der EU) bedarf einer gesonderten Rechtsgrundlage. Für die USA wurde diese Rechtsgrundlage mit dem sog. Privacy Shield geschaffen.

Mit Urteil vom 16.07.2020 (Schrems II) hat der Europäische Gerichtshof (EuGH) das Privacy Shield als Rechtsgrundlage für die Übermittlung von Daten in die USA und die Verarbeitung von Daten in den USA für nicht zulässig erklärt.

Damit liegt zunächst einmal keine Rechtsgrundlage mehr vor für die Übermittlung und Verarbeitung von Daten in den USA.

Die Server von ITTAI und EBO-Cloud oder auch der Kirchlichen Meldestelle stehen in Baden-Württemberg. Die Verarbeitung der Daten des „Kerngeschäftes“ ist damit von diesem Urteil des EuGH nicht berührt.

Relevant ist dieses Urteil und die Rechtsfolgen jedoch für den Bereich von social media und anderen Bereichen der Übermittlung und Verarbeitung von personenbezogenen Daten in die/ den USA:

Facebook, Twitter, Instagramm, YouTube, Google Analytics, Videokonferenzsysteme aller amerikanischen Anbieter (soweit die Daten nicht in der EU bleiben).

Die Schaffung einer (neuen) Rechtsgrundlage erfolgt durch den Abschluss sog. Standardvertragsklauseln. Diese Standardvertragsklauseln – von der EU-Kommission 2010 beschlossen – sind nach wie vor gültig. Durch beiderseitige Unterzeichnung der Standardvertragsklauseln kommt ein Vertrag zwischen Datenexporteur und Datenimporteur zustande, der dann die Rechtsgrundlage für die Verarbeitung personenbezogener Daten darstellt.

Es wird wenig überraschen, dass auch diese Rechtsgrundlage durch Experten als beginnend tragfähig bewertet wird; derzeit besteht aber keine andere Möglichkeit zur Schaffung einer Rechtsgrundlage.

4.3. § 29 KDG Gesetz

Bei der Verarbeitung personenbezogener Daten durch Dritte muss ein sogenannter Vertrag über die Auftragsverarbeitung (AV-Vertrag) abgeschlossen werden. Das ist auch der Fall, wenn der Dritte eine andere kirchliche Rechtsperson ist; also dann, wenn z.B. die Verrechnungsstelle für eine Kirchengemeinde, die Personalabteilung für eine Kirchengemeinde, die Diözesanstelle IT für eine Kirchengemeinde usw. Daten verarbeitet.

Das KDG sieht dabei die Möglichkeit vor, anstelle (einer großen Zahl von AV-Verträgen), ein anderes *Rechtsinstrument* zu wählen. Das Referat Datenschutz hat zu diesem Zweck ein sogenanntes § 29 KDG-Gesetz erarbeitet und zur Veröffentlichung vorbereitet.

Mit Verabschiedung dieses Gesetz wird ein wichtiger Schritt zur Erhöhung der Rechtskonformität von Regelungen in der Erzdiözese erfolgen.

4.4. Datenpannen

Gem. § 33 Abs. 1 KDG meldet der Verantwortliche der Datenschutzaufsicht unverzüglich die Verletzung des Schutzes personenbezogener Daten, wenn diese Verletzung eine Gefahr für die Rechte und Freiheiten natürlicher Personen darstellt. Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung (§ 34 Abs. 1 KDG).

Im Berichtszeitraum sind **37 Datenpannen**, davon **17 meldepflichtig** aufgetreten, die sich auf die verschiedenen Einrichtungen der Erzdiözese und der Kirchengemeinden wie folgt verteilen:

Datenpannen	Anzahl	davon meldepflichtig
Einrichtungen der Erzdiözese	22	11
Kirchengemeinden	15	6
Gesamt	37	17

Vergleich zu den Zahlen aus dem Berichtszeitraum 2019:

Datenpannen	2019		2020	
	Anzahl	davon meldepflichtig	Anzahl	davon meldepflichtig
Einrichtungen der Erzdiözese	1	1	22	11
Kirchengemeinden	6	1	15	6
Gesamt	7	2	37	17

Im Vergleich zum Berichtszeitraum 2019 ist für 2020 eine deutliche Steigerung der Datenpannen und der davon meldepflichtigen Fälle festzustellen.

Eine abschließende Erklärung dieser Steigerung ist nicht möglich.

Das Referat Datenschutz informiert und schult (insbesondere auch) zum Thema der Datenpanne. Möglicherweise führt dies zu einer Sensibilisierung der Einrichtungen, die erst ein Erkennen einer Datenpanne und deren Meldung ermöglicht.

Die Erhöhung der Zahlen selbst ist aber auch Grund, das Thema ernst zu nehmen und durch Sorgfalt im täglichen Handeln Datenpannen zu vermeiden.

5. AUSBLICK

5.1 Datenschutzkonzept

Nach § 15 Abs. 4 der Durchführungsverordnung zum Gesetz über den Kirchlichen Datenschutz (KDG-DVO) stellt der Verantwortliche sicher, dass ein Konzept zur datenschutzrechtlichen Ausgestaltung der IT-Systeme (Datenschutzkonzept) erstellt und umgesetzt wird.

Das Referat Datenschutz ist dabei, zur Unterstützung der Verantwortlichen bei der Erfüllung der gesetzlichen Verpflichtungen ein Muster für die Erarbeitung eines konkreten Datenschutzkonzeptes zu erarbeiten.

Das Datenschutzkonzept dient den Verantwortlichen dabei, für ihre Einrichtung den IST-Zustand zu erheben und bei einem Abweichen im Vergleich zu den Rahmenbedingungen/ Empfehlungen einen Handlungsbedarf zu ermitteln. Hierzu enthält das Datenschutzkonzept konkrete Aussagen zum *Sollzustand*.

Das Datenschutzkonzept dient somit der Standortbestimmung und unterstützt die Angleichung an einen Sollzustand. Die Umsetzung des Datenschutzkonzeptes erhöht die datenschutzrechtliche Qualität einer Einrichtung; Breite und Tiefe der im Datenschutzkonzept enthaltenen Themen lassen eine ausreichende Umsetzung von maßgeblichen Anforderungen erwarten.

Ein bearbeitetes Datenschutzkonzept dient primär der Einrichtung selbst bei der Erfüllung ihrer rechtlichen Verpflichtungen; es hilft, die maßgeblichen Themen und den aktuellen Bearbeitungsstand im Überblick zu haben; zusätzlich reduziert ein solches Konzept im Falle einer Prüfung durch das Katholische Datenschutzzentrum dann entstehenden Aufwand für die Einrichtung.

5.2 Grundlagenschulungen digital

Für das erste Halbjahr 2021 werden 6 Grundlagenschulungen für ehrenamtliche Mitarbeitende geplant. Diese Schulungen adaptieren das für 2020 in Präsenzform vorgesehene Schulungskonzept für digitale Schulungen.



Thomas Maier

Leiter des Referates Datenschutz im Erzbischöflichen Ordinariat Freiburg

Herausgeber:

Erzbischöfliches Ordinariat Freiburg
Referat Datenschutz
Schoferstraße 2
79098 Freiburg
datenschutz@ordinariat-freiburg.de

www.ebfr.de/Datenschutz