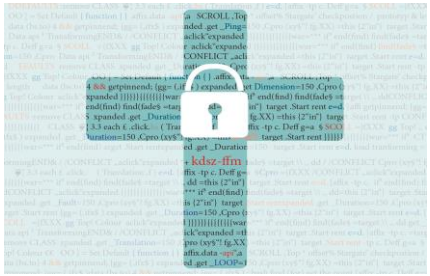


Kath. Datenschutzzentrum Frankfurt/M.KdöR
Roßmarkt 23 • 60311 Frankfurt
www.kdsz-ffm.de - info@kdsz-ffm.de

Gemeinsame Datenschutzaufsicht für die (Erz-)Diözesen
Freiburg, Fulda, Limburg, Mainz, Rottenburg-Stuttgart, Speyer und Trier

Datenschutz bei Websites

Beobachtungen und Sensibilisierung

Bei automatisierten Prüfungen von Websites katholischer Schulen hat das Kath. Datenschutzzentrum Frankfurt/M. untenstehende Beobachtungen gemacht. Teilweise weisen diese Beobachtungen auf Mängel hinsichtlich des Datenschutzes hin, in anderen Fällen ist zumindest unklar, ob alle Anforderungen des Datenschutzes erfüllt sind.

Personenbezogene Daten bei Websites

Gemäß § 4 Nr. 1 KDG sind „‚personenbezogene Daten' alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden ‚betroffene Person') beziehen". Beispiele für personenbezogene Daten im Kontext von Websites sind IP-Adressen, Web-Browser-Fingerprints, in Formularen eingegebene Daten, Inhalte von Cookies, Bestandteile von URLs, Aktivitäten einer betroffenen Person auf einer Website.

Rechtsgrundlagen

Das KDG sieht mehrere mögliche Rechtsgrundlagen für die Verarbeitung personenbezogener Daten vor. Insbesondere an Einwilligungen als Rechtsgrundlage gem. § 6 lit. b) KDG werden hohe Anforderungen gestellt, z.B. in Bezug auf die Transparenz, die in der Praxis oft nur schwer einzuhalten sind. Das Kath. Datenschutzzentrum Frankfurt/M. empfiehlt daher im Bereich von Websites, nur in Ausnahmefällen personenbezogene Daten auf Grundlage einer Einwilligung zu verarbeiten.

Sollen personenbezogene Daten dennoch auf Basis einer Einwilligung verarbeitet werden, ist darauf zu achten, dass die entsprechenden Verarbeitungen erst nach dem Erteilen einer Einwilligung stattfinden. Insbesondere sollten externe Komponenten, die nicht benötigt werden, falls eine betroffene Person keine Einwilligung erteilen möchte, erst dann von externen Servern geladen werden, wenn die entsprechende Einwilligung erteilt wurde.

Eine Verarbeitung auf der Grundlage des § 6 Abs. 1 lit. g) KDG (berechtigte Interessen, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere

Roßmarkt 23 Tel +49 69 5899755 10 Bank: Pax-Bank Köln info@kdsz-ffm.de
60311 Frankfurt/M. Fax+49 69 5899755 11 IBAN: DE78 3706 0193 5007 1810 10 www.kdsz-ffm.de
BIC: GENODED1PAX

dann, wenn es sich bei der betroffenen Person um einen Minderjährigen handelt) sollte nur nach einer positiven dreistufigen Prüfung des Verantwortlichen erfolgen:

- 1. Stufe: Vorliegen eines berechtigten Interesses des Verantwortlichen oder eines Dritten
- 2. Stufe: Erforderlichkeit der Datenverarbeitung zur Wahrung dieses Interesses
- 3. Stufe: Abwägung mit den Interessen, Grundrechten und Grundfreiheiten der betroffenen Person im konkreten Einzelfall

(Quelle: Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021 der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder)

Ein Nachweis dieser Prüfung ist der Aufsicht auf Verlangen vorzuzeigen. Eine Verarbeitung auf der Grundlage des § 6 Abs. 1 lit. g) KDG ist für die von öffentlich-rechtlich organisierten kirchlichen Stellen in Erfüllung ihrer Aufgaben vorgenommene Verarbeitung unzulässig.

Einbindung externer Komponenten

Bei der Einbindung externer Komponenten wird vom Web-Browser des Besuchers/der Besucherin eine zusätzliche Verbindung zu weiteren Servern aufgebaut, was in der Regel mit der Verarbeitung personenbezogener Daten einhergeht. Nach den Grundsätzen der Datenminimierung und des Datenschutzes durch Technikgestaltung empfiehlt es sich, Komponenten grundsätzlich intern einzubinden und nur nötigenfalls extern. Für die folgenden, im Rahmen der diesseits durchgeführten Prüfung beobachteten Einbindungen besteht unter Umständen keine Rechtsgrundlage bzw. bestehen Zweifel, dass sie dem Grundsatz der Datenminimierung und des Datenschutzes durch Technikgestaltung genügen:

- Google Tagmanager und Google Analytics
- Google reCaptcha
- Google Maps
- Google Youtube
- Google Fonts
- statische Dateien wie Schriftarten, CSS-Dateien, JavaScript-Dateien, z.B. jQuery
- Altruja
- collect.chat
- Consentmanager

Roßmarkt 23 Tel +49 69 5899755 10 Bank: Pax-Bank Köln info@kdsz-ffm.de
60311 Frankfurt/M. Fax+49 69 5899755 11 IBAN: DE78 3706 0193 5007 1810 10 www.kdsz-ffm.de
BIC: GENODED1PAX

- Cookiebot
- etracker
- Matomo
- Easy Reading
- Usercentrics
- piwik-sesam.w-commerce.de
- zwei14.app
- Musterhausen
- Carinet

Bei diesen Einbindungen sollte geprüft werden, ob eine Auftragsverarbeitung vorliegt und ein entsprechender Auftragsverarbeitungsvertrag abgeschlossen wurde (ggf. über § 29 Abs. 3 KDG), eine Rechtsgrundlage für die Verarbeitung besteht und die Grundsätze der Datenminimierung und des Datenschutzes durch Technikgestaltung eingehalten werden.

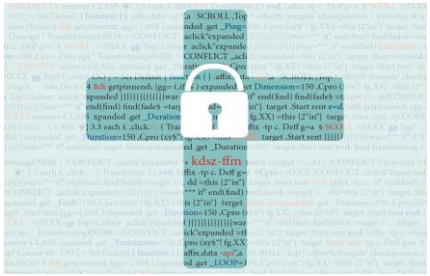
Hosting

Bei der Auswahl eines externen Dienstleisters für das Hosting der Website wird empfohlen, einen Anbieter innerhalb der EU bzw. des EWR zu wählen und darauf zu achten, dass dieser keiner Verpflichtung zur Herausgabe von Daten an Behörden außerhalb des EWR unterliegt (z.B. US-CLOUD-Act). Dies war in mehreren beobachteten Fällen nicht gegeben. Kann auf eine Drittlandsübermittlung nicht verzichtet werden, sind die erhöhten Anforderungen aus Kapitel 5 (§§ 39–41) KDG zu erfüllen. Für das Hosting bei einem externen Dienstleister ist ein Auftragsverarbeitungsvertrag abzuschließen (ggf. über § 29 Abs. 3 KDG).

Teilweise wird die Nutzung der geprüften Websites blockiert, wenn Besuchende einen Proxy (z.B. VPN, Tor etc.) verwenden, ohne dass hierfür ein besonderer Grund erkennbar ist. Da diese Maßnahme der Datenminimierung dienen kann, sollte die Nutzung von Proxies ermöglicht werden.

Es sollte auf eine sichere und datensparsame TLS-Konfiguration des Web-Servers geachtet werden, also beispielsweise die Verwendung nur als sicher geltender Cipher-Suites und von OCSP-Stapling.

Roßmarkt 23 Tel +49 69 5899755 10 Bank: Pax-Bank Köln info@kdsz-ffm.de
60311 Frankfurt/M. Fax+49 69 5899755 11 IBAN: DE78 3706 0193 5007 1810 10 www.kdsz-ffm.de
BIC: GENODED1PAX



Kath. Datenschutzzentrum Frankfurt/M.KdöR
Roßmarkt 23 • 60311 Frankfurt
www.kdsz-ffm.de - info@kdsz-ffm.de

Gemeinsame Datenschutzaufsicht für die (Erz-)Diözesen
Freiburg, Fulda, Limburg, Mainz, Rottenburg-Stuttgart, Speyer und Trier

Speicherung von Informationen im Endgerät

Je nach Gestaltung einer Website werden Cookies und andere Objekte im Web-Browser des Besuchers/der Besucherin gespeichert. Neben der enthaltenen Information, dass in der Vergangenheit bereits ein Aufruf der entsprechenden Website stattgefunden hat, können weitere, oft personenbezogene Daten enthalten sein. Hierfür bedarf es einer Rechtsgrundlage, die nicht immer festgestellt werden konnte.

Analytics

Bei der Erfassung des Besucherverhaltens sollte geprüft werden, welche der erfassten Daten tatsächlich ausgewertet werden. Nicht benötigte Daten dürfen nicht erfasst werden.

Datenschutzerklärung

Einige katholische Schulen, die unter den Anwendungsbereich des KDG fallen, referenzieren in der Datenschutzerklärung ihrer Website auf die Datenschutzgrundverordnung (DSGVO). Dabei muss darauf geachtet werden, dass aus der Formulierung der Datenschutzerklärung eindeutig die Anwendung des KDG hervorgeht. Bei der Formulierung der Datenschutzerklärung sollte auf eine Übereinstimmung mit den vorhandenen technischen Gegebenheiten der Website geachtet werden, insbesondere, wenn allgemeine Vorlagen verwendet werden. Darüber hinaus wird empfohlen, die zuständige Datenschutzaufsicht mit den aktuellen Kontaktdaten zu nennen; ggf. sind diese zu aktualisieren.

Weitere Informationen

Weitere Informationen zu Anforderungen des Datenschutzes können auch der „Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021" der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder entnommen werden:

https://www.datenschutzkonferenz-online.de/media/oh/20221205_oh_Telemedien_2021_Version_1_1_Vorlage_104_DSK_final.pdf

Frankfurt am Main, im Oktober 2024

Roßmarkt 23 | Tel +49 69 5899755 10 | Bank: Pax-Bank Köln | info@kdsz-ffm.de
60311 Frankfurt/M. | Fax+49 69 5899755 11 | IBAN: DE78 3706 0193 5007 1810 10 | www.kdsz-ffm.de
BIC: GENODED1PAX