FMK | FileMaker Konferenz

Sicherheit in der Low-Code-Entwicklung

Ein Vortrag von

Rechtsanwalt Christoph Kluss

Über den Sprecher

- **Christoph Kluss**
- Geburtsjahr 1962
- Tätigkeit für Deutsch-Amerikanische Handelskammer in Los Angeles, USA.
- Rechtsanwalt seit 1991 überwiegend für technische Unternehmen / IT Branche im Bereich gewerblicher Rechtsschutz u. Urheberrecht, Arbeitsrecht und Inkasso und Dateschutzbeauftragter.
- Dozent und Prüfer IHK für Bankfachwirte
- 4 Currywurstbuden „Best Worscht In Town“ BESTWORSCHT IN TOWN 😀

1. Einführung

- Warum sind rechtliche Datenschutzaspekte für Entwickler relevant ?

Praxisbeispiel: „Entwicklung einer FileMaker-App mit Patientendaten – was passiert bei ungesicherter Cloud-Verbindung?“

1. Einführung

- Warum sind rechtliche Aspekte für Entwickler relevant ?
  - **Datenbanken = Herzstück vieler Geschäftsprozesse**

1. Einführung

- Warum sind rechtliche Aspekte für Entwickler relevant ?
  - Datenbanken = Herzstück vieler Geschäftsprozesse
  - **Entwickler tragen Mitverantwortung ➡️**
  - **Design-Entscheidungen haben rechtliche Folgen**

1. Einführung

- Warum sind rechtliche Aspekte für Entwickler relevant ?
  - Datenbanken = Herzstück vieler Geschäftsprozesse
  - Entwickler tragen Mitverantwortung → Design-Entscheidungen haben rechtliche Folgen
  - **Ziel**: Überblick über rechtliche Rahmenbedingungen und praktische Umsetzung in FileMaker

2. Rechtsrahmen

- EU-Ebene: DSGVO,
- **Deutschland**: BDSG, IT-Sicherheitsgesetz, branchenspezifische Vorschriften (StGB § 203, BRAO, SGB).
- **Österreich**: DSG Österreich
- **Schweiz**: DSG Schweiz
- Internationale Relevanz: Cloud-Hosting außerhalb EU → Drittstaatentransfer (Art. 44 ff. DSGVO)

2. Rechtsrahmen

- Klare Trennung
  - **Datenschutz** (personenbezogene Daten) vs.
  - **IT-Sicherheit** (Integrität, Verfügbarkeit, Vertraulichkeit)

3. DSGVO-Grundprinzipien

- Rechtmäßigkeit,
- Transparenz,
- Zweckbindung,
- Datenminimierung

3. DSGVO-Grundprinzipien

- Integrität & Vertraulichkeit (Art. 32 DSGVO) = zentrale Anforderung an Datenbanken

ACHTUNG: Art. 32 DSGVO ist „Pflichtnorm“ für Entwickler – technische & organisatorische Maßnahmen (TOMs).

3. DSGVO-Grundprinzipien

- Rechenschaftspflicht (Art. 5 Abs. 2 DSGVO): Nachweis, nicht nur Einhaltung.

4. IT-Sicherheitsgesetz & BSI

- IT-Sicherheitsgesetz: Schutz kritischer Infrastrukturen (teilweise auch Kanzleien/Medizin betroffen.

- Informationssicherheitsgesetz in **Österreich**

- Bundesgesetz über die Informationssicherheit in der **Schweiz**

4. IT-Sicherheitsgesetz & BSI

- BSI-Grundschutzkataloge als anerkannte Maßstäbe (Bundesamt für Sicherheit in der Informationstechnik)

- In **Österreich** ist das **Bundeskanzleramt** (BKA) die zentrale Stelle für Cybersicherheit auf nationaler Ebene.

- In der **Schweiz** übernimmt das Nationale **Zentrum für Cybersicherheit (NCSC)** die zentrale Rolle in der nationalen Cybersicher-heitsarchitektur.

4. IT-Sicherheitsgesetz & BSI

ACHTUNG:

Auch wenn nicht direkt adressiert, gelten BSI-Standards als „Stand der Technik“ i.S.d. Art. 32 DSGVO.

5. Berufsgeheimnisse

- Anwälte, Ärzte, Steuerberater: § 203 StGB – Schweigepflichtverletzungen auch durch IT-Fehler **strafbar** (auch in Österreich/Schweiz)
- Entwickler haften bei Mitwirkung (fahrlässig/ funktional unzureichend)
- Erhöhte Anforderungen: Verschlüsselung, Zugriffskontrolle, Logging

6. FileMaker Pro-Architektur

- **Betrifft** FileMaker Pro / FileMaker Server / FileMaker Cloud

6. FileMaker Pro-Architektur

- Betrifft FileMaker Pro / FileMaker Server / FileMaker Cloud
- **Daten liegen in .fmp12-Dateien → Verschlüs-selung auf File-Ebene möglich**

6. FileMaker Pro-Architektur

- Betrifft FileMaker Pro / FileMaker Server / FileMaker Cloud
- Daten liegen in .fmp12-Dateien → Verschlüs-selung auf File-Ebene möglich
- **Zugriff meist Client-Server oder WebDirect - Transportverschlüsselung (SSL/TLS) notwendig**

6. FileMaker Pro-Architektur

- Betrifft FileMaker Pro / FileMaker Server / FileMaker Cloud
- Daten liegen in .fmp12-Dateien → Verschlüs-selung auf File-Ebene möglich
- **Zugriff meist Client-Server oder WebDirect - Transportverschlüsselung (SSL/TLS) notwendig**

  ACHTUNG: Nicht nur „App-Logik“ zählt, sondern auch Server-Setup.

7. Authentifizierung & Autorisierung

- FileMaker interne Konten & Passwörter
- Externe Authentifizierung: Active Directory, LDAP, OAuth/OIDC (z. B. Google, Microsoft)
- Zertifikatsbasierte Anmeldung als Sicherheitsplus

Beispiel: Passwort „1234“ = DSGVO-Verstoß ➡️ Haftungsfall.

8. Verschlüsselung

- **AES-256-Verschlüsselung** für Ruhedaten (FileMaker Server / Pro Advanced)

  AES-256 ist Variante des **Advanced Encryption Standard** (AES), einem symmetrischen Verschlüsselungsalgorithmus, der weltweit als sicherer Standard für den Schutz sensibler Daten anerkannt ist. Die Zahl 256 bezieht sich auf die Länge des verwendeten Schlüssels in Bit.

- **SSL/TLS** für Übertragung (Zertifikate verpflichtend!)

- **Backups**: ebenfalls verschlüsseln, Zugriffskontrolle sicherstellen

9. Privacy by Design (Art. 25 DSGVO)

- **Minimalprinzip**: nur benötigte Daten speichern
- **Rollenbasierte Zugriffsrechte** in FileMaker nutzen
- **Löschkonzepte** integrieren (z. B. automatische Archivierung/Löschung - soll über Voreinstellungen definiert werden)

TIPP: Entwicklerpraxis: Checkbox „aktive Kunden“ statt riesiger Historie → Minimierung.

10. Dokumentationspflichten

- Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO)
- Dokumentation der TOMs (Art. 32 DSGVO)
- Nachweisfähigkeit bei Behördenprüfungen
- **TIPP**: Entwickler sollten Auftraggebern standardisierte Dokumentationen bereitstellen.

11. Haftung & Verantwortlichkeit

- **Auftraggeber** = Verantwortlicher (Art. 4 Nr. 7 DSGVO)
- **Entwickler** = Auftragsverarbeiter / Dienstleister (§§ Werkvertrag)
- **Haftung bei Pflichtverletzung** → vertragliche Gestaltung wichtig (Haftungsbegrenzung, TOM-Pflichten)

11. Haftung & Verantwortlichkeit

- **Haftung bei Pflichtverletzung** → vertragliche Gestaltung wichtig (Haftungsbegrenzung, TOM-Pflichten)

- **TIPP**: in Verträgen klare Rollen definieren (Art. 28 DSGVO).

12. Q & A

- **Beispiel 1**: FileMaker-Cloud in den USA – Drittstaatentransfer zulässig?
- **Beispiel 2**: Mitarbeiterzugriff auf Personalakte ohne Berechtigung - Datenschutzverletzung - Meldung Art. 33 DSGVO.
- Offene Fragen & Diskussion.

Vielen Dank unseren Sponsoren und Konferenz-Partnern

MonkeyBread Software

Claris

FileMaker Magazin

24U SOFTWARE

CamelCase
camelcase.com

CAOS
culture agency office software