fotograf.de
GotPhoto

Technische und organisatorische Maßnahmen (TOM) gemäß Art. 32 DSGVO
Fotografen Online Service GmbH (FOS)

1. Einleitung

Die Fotografen Online Service GmbH (FOS) trifft angemessene technische und organisatorische Maßnahmen gemäß Art. 32 Datenschutz-Grundverordnung (DSGVO), um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.

Diese Maßnahmen dienen insbesondere dazu, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten sicherzustellen sowie die Fähigkeit zu gewährleisten, die Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall zeitnah wiederherzustellen.

Die nachfolgend beschriebenen Maßnahmen gelten für sämtliche Systeme und Dienste, die zur Verarbeitung personenbezogener Daten eingesetzt werden.

2. Vertraulichkeit

2.1 Physische Zutrittskontrolle

FOS betreibt für seine Produktivsysteme keine eigene Serverinfrastruktur, sondern nutzt überwiegend zertifizierte Cloud-Infrastruktur-Anbieter.

Die für die Verarbeitung personenbezogener Daten eingesetzten Rechenzentren sind durch moderne physische Sicherheitsmaßnahmen geschützt. Hierzu gehören unter anderem Zutrittskontrollsysteme, Videoüberwachung sowie streng geregelte Zugangsverfahren. Die eingesetzten Cloud-Anbieter verfügen über international anerkannte Sicherheitszertifizierungen (z. B. ISO 27001).

Der Zutritt zu den Büroräumen von FOS ist ausschließlich autorisierten Mitarbeitenden gestattet und wird mittels elektronischer Zutrittsausweise kontrolliert. Zutritte werden elektronisch protokolliert und können bei Bedarf zu Sicherheits- oder Compliance-Zwecken nachvollzogen werden. Besucherinnen und Besucher werden während ihres gesamten Aufenthalts von Mitarbeitenden begleitet, um die Einhaltung der Sicherheits- und Datenschutzstandards von FOS sicherzustellen.

2.2 Logische Zugangskontrolle (Systemzugang)

Der Zugriff auf interne Systeme sowie Produktionsumgebungen wird ausschließlich autorisierten Personen gewährt.

Zu diesem Zweck werden insbesondere folgende Maßnahmen umgesetzt:

- Individuelle Benutzerkonten für alle Mitarbeitenden
- Anforderungen an sichere Passwörter
- Multi-Faktor-Authentifizierung (MFA) für administrative und privilegierte Zugriffe
- Zentrales Identitäts- und Zugriffsmanagement
- Rollenbasierte Zugriffskonzepte
- Unverzügliche Deaktivierung von Benutzerkonten nach Beendigung des Beschäftigungs- oder Vertragsverhältnisses
- Verschlüsselte Kommunikationsprotokolle (z. B. TLS) für den Systemzugriff

Administrative Zugriffe auf Infrastruktur- und Cloud-Dienste erfolgen über ein zentrales Identitätsmanagement unter Anwendung sitzungsbasierter Authentifizierung sowie des Least-Privilege-Prinzips.

2.3 Zugriffskontrolle (Berechtigungskonzept)

Der Zugriff auf personenbezogene Daten erfolgt ausschließlich nach dem Need-to-know-Prinzip.

Hierzu werden insbesondere folgende Maßnahmen umgesetzt:

- Rollenbasierte Berechtigungskonzepte
- Funktionstrennung, soweit erforderlich
- Dokumentierte Verfahren zur Vergabe, Änderung und Entziehung von Zugriffsrechten
- Regelmäßige Überprüfung bestehender Berechtigungen
- Restriktive Vergabe administrativer Rechte
- Eindeutige Benutzerkennungen für alle berechtigten Personen

Der Zugriff auf Quellcode-Repositories, Datenbanken sowie administrative Oberflächen ist ausschließlich autorisierten Personen vorbehalten.

2.4 Trennungsgebot

Personenbezogene Daten verschiedener Verarbeitungszwecke und Kunden werden logisch voneinander getrennt.

Hierzu werden insbesondere folgende Maßnahmen umgesetzt:

- Logische Trennung von Entwicklungs-, Test- und Produktivumgebungen
- Kontrollierter Zugriff auf administrative Funktionen
- Logische Trennung von Kundendaten innerhalb der Anwendungsarchitektur
- Segmentierung von Infrastrukturkomponenten entsprechend ihrer Sicherheitsanforderungen

3. Integrität

3.1 Integrität der Daten und Änderungskontrolle

FOS stellt sicher, dass personenbezogene Daten nicht unbefugt verändert oder gelöscht werden können.

Zu diesem Zweck werden insbesondere folgende Maßnahmen umgesetzt:

- Rollenbasierte Berechtigungskonzepte
- Protokollierung von Zugriffen und sicherheitsrelevanten Systemaktivitäten
- Kontrollierte Bereitstellungsprozesse (Deployment)
- Dokumentierte Freigabe- und Änderungsmanagementverfahren
- Versionsverwaltung für Quellcode
- Sichere Konfigurationsverwaltung

3.2 Sichere Datenübertragung

Die Übertragung personenbezogener Daten über öffentliche Netzwerke erfolgt ausschließlich verschlüsselt.

Zu diesem Zweck werden insbesondere folgende Maßnahmen umgesetzt:

- Verschlüsselte Kommunikation über HTTPS (TLS 1.2 oder höher)
- Verschlüsselte Protokolle für administrative Zugriffe
- Verbot der unverschlüsselten Übertragung personenbezogener Daten

3.3 Eingabekontrolle und Protokollierung

Es kann nachvollzogen werden, ob und durch wen personenbezogene Daten in den Systemen eingegeben, verändert oder gelöscht wurden.

Zu diesem Zweck werden insbesondere folgende Maßnahmen umgesetzt:

- Protokollierung von Authentifizierungsereignissen
- Protokollierung administrativer Tätigkeiten
- Protokollierung relevanter Änderungen auf Anwendungsebene

- Zentrales Log-Management
- Definierte Aufbewahrungsfristen für Protokolldaten

Protokolldaten werden anlassbezogen sowie im Rahmen der Untersuchung von Sicherheitsvorfällen ausgewertet.

4. Verfügbarkeit und Belastbarkeit

4.1 Verfügbarkeitskontrolle

FOS schützt personenbezogene Daten vor zufälliger Zerstörung oder Verlust.

Zu diesem Zweck werden insbesondere folgende Maßnahmen umgesetzt:

- Hosting in zertifizierten Cloud-Umgebungen
- Redundante Infrastrukturkomponenten
- Regelmäßige automatisierte Datensicherungen
- Versionierte Backups
- Regelmäßige Wiederherstellungstests
- Kontinuierliche Systemüberwachung

4.2 Wiederherstellung der Verfügbarkeit

FOS unterhält Verfahren, um die Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen innerhalb angemessener Zeit wiederherzustellen.

Zu diesem Zweck werden insbesondere folgende Maßnahmen umgesetzt:

- Dokumentierte Backup- und Wiederherstellungsverfahren
- Definierte Recovery Time Objectives (RTO) und Recovery Point Objectives (RPO)
- Verfahren für Incident- und Notfallmanagement
- 24/7-Überwachung der Produktivsysteme
- Definierte Eskalationsverfahren

4.3 Business Continuity

FOS verfügt über einen dokumentierten Business-Continuity-Plan (BCP). Mitarbeitende werden über Notfallverfahren informiert. Die Wirksamkeit des Business-Continuity-Managements wird regelmäßig überprüft.

5. Datenschutzmanagement und Governance

5.1 Datenschutzorganisation

FOS hat folgende Funktionen eingerichtet:

- Externe Datenschutzbeauftragte (DSB)
- Interne Informationssicherheitsbeauftragte (ISO)

Darüber hinaus werden dokumentierte Richtlinien und Verfahren vorgehalten, insbesondere:

- Datenschutzrichtlinie
- Informationssicherheitsrichtlinie
- Richtlinie zum Identitäts- und Zugriffsmanagement
- Backup- und Wiederherstellungsrichtlinie
- Incident-Response-Plan
- Richtlinien für mobiles Arbeiten und den Einsatz mobiler Endgeräte
- Richtlinie zur Löschung und Vernichtung von Daten

Alle Mitarbeitenden sind vertraglich zur Vertraulichkeit verpflichtet und nehmen regelmäßig an Schulungen zum Datenschutz sowie zur Informationssicherheit teil.

5.2 Incident-Response-Management

FOS verfügt über dokumentierte Verfahren zur Erkennung, Meldung und Behandlung von Sicherheits- und Datenschutzvorfällen.

Zu diesem Zweck werden insbesondere folgende Maßnahmen umgesetzt:

- Überwachungssysteme zur Erkennung sicherheitsrelevanter Ereignisse
- Dokumentierte interne Meldeverfahren für Sicherheitsvorfälle
- Einbindung der Datenschutzbeauftragten bei Datenschutzvorfällen
- Dokumentation und Nachbereitung von Vorfällen
- Verfahren zur Bewertung gesetzlicher Meldepflichten

6. Sichere Softwareentwicklung

FOS wendet anerkannte Grundsätze der sicheren Softwareentwicklung an.

Zu diesem Zweck werden insbesondere folgende Maßnahmen umgesetzt:

- Sichere Systemarchitektur und Engineering-Prinzipien
- Trennung von Entwicklungs-, Test- und Produktivumgebungen
- Anwendung sicherer Programmierstandards

- Peer-Review-Verfahren für Quellcode
- Verbot der Verwendung fest im Quellcode hinterlegter Passwörter
- Kontrollierter Einsatz von Drittanbieter-Komponenten
- Sichere Verwaltung von Quellcode-Repositories
- Zugriff auf Quellcode ausschließlich nach dem Need-to-know-Prinzip
- Continuous Integration und Continuous Deployment (CI/CD) einschließlich Sicherheitsprüfungen
- Sichere Verwaltung von Geheimnissen und Zugangsdaten (Secrets Management)
- Anwendung des Least-Privilege- und Zero-Trust-Prinzips, soweit angemessen

Sicherheitsprüfungen, beispielsweise Schwachstellenanalysen und Penetrationstests, werden regelmäßig durchgeführt.

7. Steuerung von Auftragsverarbeitern

Soweit FOS Auftragsverarbeiter einsetzt, wird sichergestellt, dass die Verarbeitung personenbezogener Daten ausschließlich auf dokumentierte Weisung erfolgt.

Zu diesem Zweck werden insbesondere folgende Maßnahmen umgesetzt:

- Sorgfältige Auswahl von Auftragsverarbeitern anhand von Datenschutz- und Sicherheitskriterien
- Abschluss von Auftragsverarbeitungsverträgen gemäß Art. 28 DSGVO
- Einsatz der EU-Standardvertragsklauseln, soweit erforderlich
- Überprüfung der technischen und organisatorischen Maßnahmen der Auftragsverarbeiter
- Vertragliche Verpflichtung der Mitarbeitenden der Auftragsverarbeiter zur Vertraulichkeit
- Laufende Überwachung der Einhaltung datenschutzrechtlicher Anforderungen durch die Auftragsverarbeiter

8. Regelmäßige Überprüfung und Bewertung

FOS überprüft und bewertet die Wirksamkeit seiner technischen und organisatorischen Maßnahmen regelmäßig.

Dies umfasst insbesondere:

- Regelmäßige interne Bewertungen
- Überprüfung bestehender Zugriffsberechtigungen
- Überprüfung von Richtlinien und Verfahren

- Anpassung der Maßnahmen an technologische Entwicklungen
- Dokumentation relevanter Sicherheitsmaßnahmen

9. Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen

FOS setzt die Grundsätze des Datenschutzes durch Technikgestaltung sowie datenschutzfreundlicher Voreinstellungen gemäß Art. 25 DSGVO um.

Zu diesem Zweck werden insbesondere folgende Maßnahmen umgesetzt:

- Erhebung personenbezogener Daten ausschließlich im für den jeweiligen Verarbeitungszweck erforderlichen Umfang
- Systemkonfigurationen zur Unterstützung der Datenminimierung
- Technische Unterstützung bei der Wahrnehmung der Rechte betroffener Personen
- Berücksichtigung datenschutzrechtlicher Anforderungen bereits bei der Konzeption und Entwicklung von Systemen

Stand: Juli 2026