# Bilderladen GmbH

# Technische und organisatorische Maßnahmen (TOMs)

## gemäß Art. 32 DSGVO

Version: 1.3 (26.05.2026)
Status: Abgenommen

---

# Inhaltsverzeichnis

---

# Einleitung

Die Bilderladen GmbH trifft geeignete technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO, um ein dem Risiko angemessenes Schutzniveau für personenbezogene Daten sicherzustellen.

Die nachfolgend beschriebenen Maßnahmen dienen insbesondere der Gewährleistung von:

- Vertraulichkeit,
- Integrität,
- Verfügbarkeit,
- Belastbarkeit der Systeme und Dienste,
- sowie der Fähigkeit, die Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall zeitnah wiederherzustellen.

Die Maßnahmen gelten für alle Systeme, Dienste und Prozesse der Bilderladen GmbH, die zur Verarbeitung personenbezogener Daten eingesetzt werden.

Bilderladen betreibt eine cloudbasierte SaaS-Plattform für Schul- und Kindergartenfotografie, einschließlich Bildverwaltung, Online-Shops, Bestellprozessen und damit verbundenen Dienstleistungen.

---

# 1. Pseudonymisierung (Art. 32 Abs. 1 lit. a DSGVO)

Die folgenden Maßnahmen sind implementiert:

- Logische Trennung von Mandanten und Kundendaten
- Verwendung interner Identifikationsnummern und technischer IDs
- Datenminimierung bei Verarbeitungsvorgängen
- Pseudonymisierte Verarbeitung sofern technisch und organisatorisch sinnvoll

- Einschränkung personenbezogener Anzeigen in administrativen Bereichen

---

# 2. Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)

Maßnahmen umfassen insbesondere:

- Verschlüsselte Kommunikation über HTTPS/TLS
- Verschlüsselung administrativer Zugriffe
- Verschlüsselte Speicherung sensibler Zugangsdaten und Secrets
- Nutzung verschlüsselter Cloud-Dienste
- Verschlüsselte Übertragung von Dateien und Bilddaten
- Einsatz sicherer Authentifizierungsverfahren

---

# 3. Gewährleistung der Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

## 3.1 Zutrittskontrolle

Bilderladen nutzt überwiegend zertifizierte Cloud-Infrastruktur-Anbieter für den Betrieb produktiver Systeme. Eigene lokale Produktionsserver werden für Kerndienste der Plattform grundsätzlich nicht betrieben.

Die genutzten Rechenzentren verfügen über moderne physische Sicherheitsmaßnahmen, insbesondere:

- Zugangskontrollsysteme,
- Videoüberwachung,
- eingeschränkte Zutrittsverfahren,
- Umwelt- und Sicherheitsmonitoring,
- sowie zertifizierte Sicherheits- und Betriebsprozesse.

Die eingesetzten Cloud-Anbieter verfügen über anerkannte Sicherheitszertifizierungen wie beispielsweise ISO 27001 oder vergleichbare Standards.

Der Zugang zu Büroräumen der Bilderladen GmbH ist auf autorisierte Personen beschränkt.

Maßnahmen umfassen insbesondere:

- Elektronische oder physische Zugangskontrollen
- Beschränkung des Zutritts auf autorisierte Mitarbeiter
- Begleitung von Besuchern sofern erforderlich
- Sperrung von Arbeitsplätzen außerhalb der Nutzung
- Clean-Desk-Prinzipien für sensible Informationen

---

## 3.2 Zugangskontrolle

Der Zugriff auf interne Systeme und Produktionsumgebungen wird ausschließlich autorisierten Personen nach dem Prinzip der minimalen Rechtevergabe gewährt.

Maßnahmen umfassen insbesondere:

- Individuelle Benutzerkonten
- Sichere Passwortanforderungen
- Multi-Faktor-Authentifizierung (MFA) für privilegierte Zugriffe
- Rollenbasierte Zugriffskonzepte
- Sofortige Deaktivierung von Zugängen bei Austritt oder Rollenwechsel
- Verschlüsselte Kommunikationsprotokolle (TLS)
- Geschützte Remote-Zugriffe und VPN-Verbindungen sofern erforderlich
- Eingeschränkter Zugriff auf Produktionssysteme

Administrative Zugriffe auf Cloud- und Infrastruktursysteme sind ausschließlich autorisierten Personen vorbehalten.

---

## 3.3 Zugriffskontrolle

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

Maßnahmen umfassen insbesondere:

- Rollen- und berechtigungsbasierte Zugriffskonzepte
- Restriktive Vergabe administrativer Rechte
- Geregelte Prozesse zur Vergabe, Änderung und Entziehung von Berechtigungen
- Regelmäßige Überprüfung von Zugriffsrechten
- Protokollierung administrativer Tätigkeiten
- Einschränkung des Zugriffs auf Datenbanken, Speicher und Administrationsoberflächen
- Schutz vor unbefugtem Export oder Offenlegung personenbezogener Daten

Der Zugriff auf Kunden-, Bestell- und Bilddaten ist auf berechtigte Personen mit betrieblicher Notwendigkeit beschränkt.

---

## 3.4 Trennungskontrolle

Daten verschiedener Kunden, Mandanten und Verarbeitungszwecke werden logisch voneinander getrennt verarbeitet.

Maßnahmen umfassen insbesondere:

- Trennung von Entwicklungs-, Test- und Produktivumgebungen
- Mandantentrennung innerhalb der SaaS-Plattform
- Logische Trennung von Kundendaten innerhalb der Systemarchitektur
- Eingeschränkter Zugriff auf Testumgebungen
- Verwendung anonymisierter oder reduzierter Testdaten sofern möglich
- Trennung von Infrastrukturkomponenten entsprechend der Sicherheitsanforderungen

---

# 4. Gewährleistung der Integrität (Art. 32 Abs. 1 lit. b DSGVO)

## 4.1 Weitergabekontrolle

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

Maßnahmen umfassen insbesondere:

- Rollenbasierte Berechtigungskonzepte
- Protokollierung relevanter Systemaktivitäten
- Kontrollierte Deployment- und Release-Prozesse
- Versionsverwaltung für Quellcode
- Sichere Konfigurationsverwaltung
- Kontrollierte administrative Prozesse
- Prinzip der minimalen Rechtevergabe

---

## 4.2 Eingabekontrolle

Personenbezogene Daten werden bei der Übertragung über öffentliche Netzwerke durch Verschlüsselung geschützt.

Maßnahmen umfassen insbesondere:

- Verschlüsselte Kommunikation über HTTPS/TLS
- Verschlüsselte administrative Zugriffe
- Sichere APIs und authentifizierte Kommunikationswege
- Vermeidung unverschlüsselter Übertragungen personenbezogener Daten
- Sichere Upload-Mechanismen für Dateien und Bilder

---

## 2.3 Eingabekontrolle und Protokollierung

Es kann nachvollzogen werden, ob und von wem personenbezogene Daten in Systemen eingegeben, verändert oder gelöscht wurden.

Maßnahmen umfassen insbesondere:

- Protokollierung von Authentifizierungsereignissen durch den Cloud-Anbieter
- Protokollierung administrativer Tätigkeiten durch den Cloud-Anbieter
- Systemseitiges Log-Management durch den Cloud-Anbieter und Anwendungslogs
- Definierte Aufbewahrungsfristen für Protokolle durch den Cloud-Anbieter sowie innerhalb der Anwendung.
- Kontrollierter Zugriff auf Protokolldaten
- Überwachung sicherheitsrelevanter Ereignisse

Protokolle werden insbesondere im Rahmen von Fehleranalysen, Betriebsüberwachung und Sicherheitsvorfällen ausgewertet.

---

# 5. Gewährleistung der Verfügbarkeit und Belastbarkeit der Systeme (Art. 32 Abs. 1 lit. b DSGVO)

## Maßnahmen

Bilderladen schützt personenbezogene Daten vor zufälliger Zerstörung, Verlust oder Nichtverfügbarkeit.

Maßnahmen umfassen insbesondere:

- Betrieb in professionell verwalteten Cloud-Umgebungen
- Redundante Infrastrukturkomponenten sofern erforderlich
- Automatisierte Backups
- Versionierte Sicherungen sofern unterstützt
- Kontinuierliches Monitoring produktiver Systeme

- Alarmierungs- und Überwachungssysteme
- Schutz vor unbeabsichtigtem oder unbefugtem Löschen
- Nutzung von Cloud-Diensten mit integrierten Hochverfügbarkeitsmechanismen

---

# 6. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DSGVO)

Maßnahmen umfassen insbesondere:

Bilderladen unterhält Prozesse zur zeitnahen Wiederherstellung der Verfügbarkeit personenbezogener Daten.

Maßnahmen umfassen insbesondere:

- Backup- und Wiederherstellungsverfahren des Cloud-Anbieters
- Regelmäßige Prüfung von Wiederherstellungsverfahren sofern praktikabel
- Nutzung von Disaster-Recovery-Funktionen der Cloud-Anbieter sofern geeignet

---

# 7. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DSGVO)

## 7.1 Datenschutzmanagement

Bilderladen unterhält organisatorische und technische Prozesse zur Behandlung betrieblicher Störungen und Sicherheitsvorfälle.

Maßnahmen umfassen insbesondere:

- Betriebs- und Systemmonitoring
- Eskalationswege für kritische Vorfälle
- Regelmäßige Bewertung betrieblicher Risiken

---

## 7.2 Incident-Response-Management

## 4.1 Datenschutzorganisation

Bilderladen unterhält organisatorische und technische Regelungen im Bereich Datenschutz und Informationssicherheit.

Maßnahmen umfassen insbesondere:

- Benennung eines Datenschutzbeauftragten sofern gesetzlich erforderlich
- Interne Verantwortlichkeiten für Datenschutz und Informationssicherheit
- Datenschutz- und Sicherheitsrichtlinien
- Vertraulichkeitsverpflichtungen für Mitarbeiter
- Regelmäßige Sensibilisierung und Schulungen
- Dokumentation von Verarbeitungstätigkeiten sofern erforderlich
- Prozesse zur Bearbeitung von Betroffenenanfragen (Ticketsystem)
- Prozesse zur Behandlung von Datenschutzvorfällen (Ticketsystem)

---

## 4.2 Incident-Response-Management

Bilderladen unterhält Prozesse zur Erkennung, Meldung und Behandlung von Sicherheits- und Datenschutzvorfällen.

Maßnahmen umfassen insbesondere:

- Monitoring sicherheitsrelevanter Ereignisse
- Interne Meldewege für Vorfälle
- Dokumentation und Nachverfolgung von Sicherheitsvorfällen
- Zusammenarbeit mit externen Dienstleistern sofern erforderlich

---

# 5. Sichere Softwareentwicklung

Bilderladen berücksichtigt Sicherheits- und Datenschutzanforderungen bei Entwicklung und Betrieb der Plattform.

Maßnahmen umfassen insbesondere:

- Trennung von Entwicklungs-, Test- und Produktivumgebungen
- Verwendung von Versionsverwaltungssystemen
- Kontrollierte Deployment-Prozesse
- Sichere Entwicklungsstandards
- Sichere Verwaltung von Secrets und Zugangsdaten
- Eingeschränkter Zugriff auf Quellcode-Repositories
- Sicherheitsrelevante Prüfungen und Reviews sofern angemessen

- Prinzip der minimalen Rechtevergabe
- Logging und Monitoring produktiver Systeme

Cloud-Infrastruktur und Deployment-Pipelines werden mit modernen Entwicklungs- und DevOps-Prozessen betrieben.

---

## 7.4 Auftragskontrolle (Art. 28 DSGVO)

Sofern Auftragsverarbeiter oder Unterauftragnehmer eingesetzt werden, stellt Bilderladen sicher, dass personenbezogene Daten ausschließlich auf dokumentierte Weisung und unter Einhaltung der geltenden Datenschutzvorgaben verarbeitet werden.

Maßnahmen umfassen insbesondere:

- Sorgfältige Auswahl von Dienstleistern unter Datenschutz- und Sicherheitsgesichtspunkten
- Abschluss von Auftragsverarbeitungsverträgen gemäß Art. 28 DSGVO sofern erforderlich
- Dokumentation eingesetzter Subunternehmer
- Prüfung verfügbarer Sicherheitsdokumentationen der Dienstleister
- Vertragliche Vertraulichkeitsverpflichtungen
- Verwaltung und regelmäßige Überprüfung von Dienstleisterbeziehungen
- Einsatz von EU-Standardvertragsklauseln sofern erforderlich

---

## 7.3 Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DSGVO)

Bilderladen überprüft und bewertet regelmäßig die Wirksamkeit der technischen und organisatorischen Maßnahmen.

Maßnahmen umfassen insbesondere:

- Regelmäßige Überprüfung von Zugriffsrechten
- Überprüfung organisatorischer und technischer Prozesse
- Bewertung technischer Entwicklungen und Risiken
- Anpassung von Maßnahmen bei Bedarf
- Dokumentation relevanter Sicherheitsmaßnahmen

---

## Zusätzliche SaaS- und Cloud-Maßnahmen

Bilderladen berücksichtigt die Grundsätze „Privacy by Design“ und „Privacy by Default“.

Maßnahmen umfassen insbesondere:

- Erhebung personenbezogener Daten nur im erforderlichen Umfang
- Berücksichtigung datenschutzrechtlicher Anforderungen bereits während Entwicklung und Architekturplanung
- Datenschutzfreundliche Standardeinstellungen sofern praktikabel
- Unterstützung von Lösch- und Aufbewahrungsprozessen
- Unterstützung der Wahrnehmung von Betroffenenrechten
- Umsetzung von Datenminimierungsprinzipien

---

# 9. Zusätzliche Maßnahmen für SaaS- und Cloud-Betrieb

Als cloudnative SaaS-Plattform setzt Bilderladen ergänzend weitere technische und organisatorische Maßnahmen ein.

Dazu gehören insbesondere:

- Nutzung verwalteter Cloud-Infrastrukturdienste
- Verschlüsselte Übertragung
- Kontrollierte CI/CD- und Deployment-Pipelines
- Audit-Logging administrativer Tätigkeiten sofern praktikabel
- Mandantentrennung innerhalb der Plattformarchitektur
- Kontrollierter Zugriff auf Produktivsysteme
- Sichere Verarbeitung von Datei- und Bild-Uploads
- Nutzung automatischer Skalierungs- und Resilienzmechanismen der Cloud-Infrastruktur

---

# Hinweise

Dieses Dokument beschreibt allgemeine technische und organisatorische Maßnahmen der Bilderladen GmbH gemäß Art. 32 DSGVO.

Einzelne Maßnahmen können abhängig von:

- dem jeweiligen System,
- der konkreten Verarbeitung,
- gesetzlichen Anforderungen,
- vertraglichen Verpflichtungen,
- sowie dem Stand der Technik

angepasst oder erweitert werden.

Das Dokument wird regelmäßig überprüft und bei organisatorischen, technischen oder rechtlichen Änderungen aktualisiert.