# Anlage 2: Checkliste technische und organisatorische Maßnahmen im Rahmen der Auftragsverarbeitung

Stand: 17.03.2026

Die nachfolgende Checkliste umfasst technische und organisatorische Maßnahmen, die im Rahmen der Auftragsverarbeitung umgesetzt werden können. Die Auswahl und Umsetzung der Maßnahmen erfolgt unter Berücksichtigung der spezifischen Anforderungen und Gegebenheiten des Auftraggebers und Auftragnehmers.

Kontakt Datenschutzbeauftragte:

Tel.: +49 421 40887928
E-Mail: <datenschutz@jaai-group.com>

Die in diesem Dokument beschriebenen technischen und organisatorischen Maßnahmen beziehen sich ausschließlich auf die Datenverarbeitung durch lector.ai und gelten nicht für externe Dienstleister, insbesondere Cloud-Dienstleister.

Bei der Beantwortung der Fragen wird in der Spalte “Erfüllt?” aus folgenden Werten gewählt:

- “Ja”, “Ja (gem. Zertifikat)” oder “Nein” entsprechend des aktuellen Umsetzungsstandes,
- “n/a”, wenn diese Maßnahme nicht zutrifft oder nicht sinnvoll ist
- ein Umsetzungsdatum, wenn die Maßnahme zwar als sinnvoll angesehen wird, aber erst zum angegebenen Datum umgesetzt wird.

# 1 Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

## 1.1 Zutrittskontrolle

| Maßnahme | Erfüllt? |
|---|---|
| Ausweistragepflicht für Besucher | Ja |
| Ausweistragepflicht für Mitarbeiter | Ja |
| Personenkontrolle am Eingang | Ja |
| Protokollierung der Besucher (Besucherbuch) | Ja |

| Maßnahme | Erfüllt? |
|---|---|
| Protokollierung der Schlüsselausgabe (Schlüsselbuch) | Ja |
| Sorgfältige Auswahl des Reinigungspersonals | Ja |
| Einrichtung von Schutz- und Sicherheitszonen | Ja |
| Festlegung der zugangsberechtigten Personen | Ja |
| Absicherung von Gebäudeschächten | n/a |
| Alarmanlage | Ja |
| Automatisches Zugangskontrollsystem | Nein |
| Bewegungsmelder | Ja |
| Manuelles Schließsystem | Ja |
| Schließsystem mit Zugangscode | Nein |
| Sicherheitsschlösser | Ja |
| Videoüberwachung der Zugänge | Ja |
| Protokollierung der Zu- und Abgänge | Nein |

## 1.2 Zugangskontrolle

| Maßnahme | Erfüllt? |
|---|---|
| Revisionsfähigkeit der Zugangsberechtigungen | Ja |
| Passwortrichtlinie (Regelung von Passwortregeln und Wechsel) | Ja |
| Multi-Faktor-Authentifizierung | Ja |
| Zertifizierte Dienstleister für Akten- und Datenvernichtung | Ja |
| Regelungen zur Verlustmeldung und Reaktionen auf Datenträgerverlust | Ja |
| Netzwerksegmentierung | Nein |
| NAC - Network Access Control | Ja |
| Automatische Bildschirmsperre | Ja |
| Cloud-Zugangskontrolle über IAM | Ja |

## 1.3 Zugriffskontrolle

| Maßnahme | Erfüllt? |
|---|---|
| Minimierte Anzahl von Administratoren | Ja |
| Sichere Aufbewahrung von Datenträgern | Ja |
| Sichere Verwaltung von Benutzerrechten | Ja |
| Regelmäßige Überprüfung der Berechtigungen | Ja |
| Revisionsfähiges Rollen-, Berechtigungs- und Nutzerkonzept | Ja |
| Datenträger-Vernichtung nach DIN 66399 | Ja |
| Externer Aktenvernichter (DIN 32757) | Ja |
| Physische Löschung von Datenträgern vor Wiederverwendung | Nein |
| Protokollierung der Datenvernichtung | Ja |
| Protokollierung der Eingabe, Veränderung und Löschung von Daten | Ja |
| Verschlüsselung von Datenträgern | Ja |
| Verschlüsselung von mobilen Geräten | Ja |
| Beschränkung der freien Abfragemöglichkeiten von Datenbanken | Ja |
| Zeitliche Begrenzung der Zugriffsmöglichkeiten | Ja |

## 1.4 Trennbarkeit von Daten

| Maßnahme | Erfüllt? |
|---|---|
| Trennung von Datenbanken durch Berechtigungen | Ja |
| Berechtigungskonzept für Anwendungen, Laufwerke und Dateien | Ja |
| Organisatorische Berücksichtigung der Mandantentrennung | Ja |
| Datensätze sind mit Zweckattributen versehen | Ja |
| Trennung von Produktiv- und Testsystem | Ja |
| Mandantenfähigkeit relevanter Anwendungen, inkl. Cloud-Ressourcen | Ja |
| Physikalisch getrennte Systeme | Nein |
| Logische Trennung der Cloud-Instanzen | Ja |
| Trennung durch getrennte Verschlüsselung | Ja |

| Maßnahme | Erfüllt? |
|---|---|
| Verwendung von Software, die eine buchhalterische Mandantentrennung ermöglicht | Ja |

## 1.5 Pseudonymisierung

| Maßnahme | Erfüllt? |
|---|---|
| Interne Anweisung, personenbezogene Daten im Falle der Weitergabe oder nach Ablauf der gesetzlichen Löschfrist möglichst zu anonymisieren/pseudonymisieren | Ja |
| Trennung der Zuordnungsdaten und Aufbewahrung in getrenntem und abgesicherten System | Nein |

---

# 2 Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

## 2.1 Weitergabekontrolle

| Maßnahme | Erfüllt? |
|---|---|
| Festlegung der Übermittlungswege und der Datenempfänger | Ja |
| Organisatorische Regelungen zur Einrichtung und Befristung von Fernzugriffen (z. B. VPN) | Ja |
| Regelungen zum datenschutzgerechten Einsatz mobiler Datenträger | Ja |
| Regelungen zum datenschutzgerechten E-Mail-Versand | Ja |
| Nutzung von Cloud-Anbietern (z. B. Office365, Google Cloud) | Ja |
| Nutzung der OVH Cloud als primäre Hosting-Infrastruktur | Ja |
| Nutzung einer eigenen Serverinfrastruktur | Nein |
| Nutzung von hosted Servern eines Dienstleisters | Ja |
| Dokumentation der Abruf- und Übermittlungsvorgänge | Ja |
| Dokumentation der Datenempfänger, Überlassungs- und Löschfristen | Ja |
| Automatisierte Überwachung nach außen offener Ports, Protokolle und Dienste | Ja |
| Protokollierung der Datenübermittlung inkl. Abrufe und Empfänger | Ja |
| Einrichtung von VPN-Tunneln | Ja |
| E-Mail-Verschlüsselung | Nein |
| Sicheres Löschen | Ja |

| Maßnahme | Erfüllt? |
|---|---|
| Überprüfung von Datenträgern auf Virenbefall | Ja |
| Zeitbegrenzung von Zugriffsmöglichkeiten | Ja |
| Protokollierung der autorisierten Weitergabe und Entfernung von Datenträgern | Ja |
| Protokollierung der Kopie von Datenträgern | Ja |
| Datenschutzgerechte Entsorgung nicht mehr benötigter Datenträger | Ja |

## 2.2 Datenintegrität

| Maßnahme | Erfüllt? |
|---|---|
| Sicherung der Software durch digitale Signaturen oder Hashwerte | Ja |
| Verschlüsselung der Datenträger | Ja |
| Verschlüsselung der internen Übertragungswege | Ja |
| Verschlüsselung von Dateien und Datenbanken | Ja |
| Kontrolle und Trennung von System- und User-Aktivitäten | Ja |

---

# 3 Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

## 3.1 Verfügbarkeitskontrolle

| Maßnahme | Erfüllt? |
|---|---|
| Notfallplan für die eingesetzten Systeme | Ja |
| Backup- und Recovery-Konzept | Ja |
| Kontrolle des Sicherungsvorgangs | Ja |
| Test der Datenwiederherstellung | Ja |
| Automatisierte Systemüberwachung und Alarmierung | Ja |
| Feuer- und Rauchmeldeanlagen | Ja |
| USV - Unterbrechungsfreie Stromversorgung | Ja |
| Trennung von Produktiv- und Testsystem | Ja |
| Nutzung der OVH Cloud-Infrastruktur mit SLA für Hochverfügbarkeit | Ja |

| Maßnahme | Erfüllt? |
|---|---|
| Geografisch verteilte Rechenzentren des Cloud-Anbieters | Ja |
| Cloud-basiertes Backup- und Recovery-Konzept | Ja |
| Datenverarbeitung ausschließlich in EU-Rechenzentren | Ja |

---

# 4 Wiederherstellbarkeit und Zuverlässigkeit (Art. 32 Abs. 1 lit. c DS-GVO)

## 4.1 Wiederherstellbarkeit

*Die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen*

| Maßnahme | Erfüllt? |
|---|---|
| Notfallplan | Ja |
| Mehrstufiges Backup- und Restorekonzept | Ja |
| Sicherheits-Vorfall-Management | Ja |
| Notfallkonzept | Ja |
| Backup- und Restoreautomatisierung | Ja |
| Nutzung der Cloud-Anbieter-Disaster-Recovery-Funktionen | Ja |
| Regelmäßige Tests der Wiederherstellungsprozesse in der Cloud-Umgebung | Ja |

## 4.2 Zuverlässigkeit

*Gewährleistet das zuverlässige Funktionieren der Datenverarbeitungssysteme*

| Maßnahme | Erfüllt? |
|---|---|
| Mindestens jährliche und dokumentierte Überprüfung der TOM | Ja |
| Regelung zur Reaktion auf Störungen | Ja |
| SLA für IT-Leistungen | Ja |
| Zentrale Beschaffung von Hard- und Software | Nein |
| Virenschutz | Ja |
| Malwarescan | Ja |

| Maßnahme | Erfüllt? |
|---|---|
| Penetrationstests | Nein |
| Regelmäßiges und zeitnahes Patch-Management | Ja |
| MDM (Mobile Device Management) - Umfassendes System zur zentralen Verwaltung, Sicherung und Überwachung von mobilen Endgeräten inklusive Durchsetzung von Sicherheitsrichtlinien, Fernlöschung, Verschlüsselungsmanagement und Anwendungskontrolle | Ja |

---

# 5 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

## 5.1 Auftragskontrolle

*Gewährleistet, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.*

| Maßnahme | Erfüllt? |
|---|---|
| Auftragsverarbeitungsvertrag (AVV) | Ja |
| Laufende Überprüfung des Auftragnehmers | Ja |
| Prüfung der TOM des Auftragnehmers vor erstmaliger Datenübertragung | Ja |
| Sichere Datenvernichtung nach Auftragsende | Ja |
| Vereinbarung von Kontrollrechten | Ja |
| Vereinbarung von Kontrollrechten für lector.ai | Ja |
| Vereinbarung von Vertragsstrafen | Nein |
| Verpflichtung der Mitarbeiter des Auftragnehmers auf die Vertraulichkeit nach DSGVO | Ja |
| Sorgfältige Auswahl des Auftragnehmers | Ja |
| Sorgfältige Vertragsgestaltung | Ja |
| Abgrenzung der Kompetenzen und Pflichten zwischen Auftragnehmer und Auftraggeber | Ja |
| Schriftliche Weisungen an den Auftragnehmer | Ja |
| Regelungen zum Einsatz weiterer Subunternehmer | Ja |
| Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags | Ja |

| Maßnahme | Erfüllt? |
|---|---|
| Laufende Überprüfung des Auftragnehmers und seines Schutzniveaus bei längerer Zusammenarbeit | Ja |
| Protokollierung und Kontrolle der ordnungsgemäßen Vertragsausführung | Ja |

## 5.2 Datenschutz-Management

*Gewährleistet die Einhaltung der DSGVO durch die Etablierung entsprechender Prozesse*

| Maßnahme | Erfüllt? |
|---|---|
| Interner/externer Datenschutzbeauftragter (Kontaktdaten in AVV) | Ja |
| Mitarbeiter geschult und auf Vertraulichkeit/Datengeheimnis verpflichtet | Ja |
| Regelmäßige Sensibilisierung der Mitarbeiter (mindestens jährlich) | Ja |
| Interner Informationssicherheitsbeauftragter | Ja |
| Die Datenschutz-Folgenabschätzung (DSFA) wird bei Bedarf durchgeführt | Ja |
| Die Organisation kommt den Informationspflichten nach Art. 13, 14 DSGVO nach | Ja |
| Formaler Prozess zur Bearbeitung von Auskunftsanfragen seitens Betroffener | Ja |
| Software-Lösungen für Datenschutz-Management im Einsatz | Nein |
| Zentrale Dokumentation aller Verfahrensweisen und Regelungen zum Datenschutz | Ja |
| Sicherheitszertifizierung nach ISO 27001, BSI IT Grundschutz oder ISIS12 | Nein |
| Alternatives Informationssicherheitskonzept | Ja |
| Überprüfung der Wirksamkeit der technischen Schutzmaßnahmen (mindestens jährlich) | Ja |
| Berücksichtigung der ISO 27001, 27017, 27018 Zertifizierungen des Cloud-Anbieters | Ja |
| Abschluss eines AVV mit dem Cloud-Anbieter OVH | Ja |
| Jährliche Überprüfung der Compliance des Cloud-Anbieters | Ja |

## 5.3 Incident-Response-Management

*Unterstützung bei der Reaktion auf Sicherheitsverletzungen*

| Maßnahme | Erfüllt? |
|---|---|
| Dokumentierter Prozess zur Erkennung und Meldung von Sicherheitsvorfällen/ Datenpannen | Ja |

| Maßnahme | Erfüllt? |
|---|---|
| Dokumentierte Vorgehensweise zum Umgang mit Sicherheitsvorfällen | Ja |
| Einbindung von DSB in Sicherheitsvorfälle und Datenpannen | Ja |
| Einbindung von ISB in Sicherheitsvorfälle und Datenpannen | Ja |
| Dokumentation von Sicherheitsvorfällen und Datenpannen, z.B. via Ticketsystem | Ja |
| Formaler Prozess zur Nachbearbeitung von Sicherheitsvorfällen und Datenpannen | Ja |
| Einsatz von Firewall und regelmäßige Aktualisierung | Ja |
| Einsatz von Spamfilter und regelmäßige Aktualisierung | Ja |
| Einsatz von Virenscanner und regelmäßige Aktualisierung | Ja |
| Intrusion Detection System (IDS) | Ja |
| Intrusion Prevention System (IPS) | Ja |

## 5.4 Datenschutzfreundliche Voreinstellungen

*Gemäß Art. 25 Abs. 2 DSGVO*

| Maßnahme | Erfüllt? |
|---|---|
| Einfache Ausübung des Widerrufsrechts des Betroffenen durch technische Maßnahmen | Nein |
| Es werden nicht mehr personenbezogene Daten erhoben, als für den jeweiligen Zweck erforderlich sind | Ja |

---

Die Richtigkeit der Angaben wird bestätigt:

Benjamin von Ardenne

Geschäftsführer der lector.ai GmbH

Bremen, 14.07.2026



© 2026 lector.ai GmbH - Alle Rechte vorbehalten