

Technische und organisatorische Maßnahmen gemäß Art. 32 DSGVO

Version: 2.1

Stand: 08.08.2026

Die MINTANO GmbH trifft geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau für die im Auftrag verarbeiteten personenbezogenen Daten zu gewährleisten.

Die Maßnahmen dienen insbesondere dem Schutz vor unbefugtem Zutritt, unbefugtem Zugang, unbefugtem Zugriff, unbeabsichtigter oder unrechtmäßiger Veränderung, Verlust, Vernichtung sowie Nichtverfügbarkeit personenbezogener Daten. Die Maßnahmen gelten für die von MINTANO eingesetzten Systeme, Anwendungen, Dienste, Endgeräte, Prozesse und Standorte, soweit diese für die Erbringung der vereinbarten Leistungen relevant sind. Soweit Hosting-, Cloud-, SaaS- oder sonstige Unterauftragnehmer eingesetzt werden, werden deren technische und organisatorische Maßnahmen ergänzend einbezogen.

MINTANO überprüft die Maßnahmen regelmäßig sowie anlassbezogen und passt sie bei Bedarf an, sofern das vereinbarte Schutzniveau nicht wesentlich unterschritten wird.

1. Vertraulichkeit

1.1 Zutrittskontrolle

MINTANO nutzt eigene Büro- und Lagerflächen in einem professionell gemanagten Coworking Space. Der physische Zutritt ist durch Maßnahmen des Standortbetreibers und von MINTANO geregelt.

Hierzu gehören insbesondere ein besetzter Empfang während der regulären Öffnungszeiten, Zutrittsberechtigungen über Transponder- beziehungsweise Chip-Systeme, Videoüberwachung in hierfür vorgesehenen Bereichen, definierte Reinigungszeiten sowie abschließbare Büro- und Lagerräume.

Unterlagen, Geräte und Datenträger mit personenbezogenen Daten werden nicht frei zugänglich aufbewahrt. Bei Abwesenheit werden die durch MINTANO genutzten Räume verschlossen.

Produktive Server- und Datenbankinfrastruktur wird nicht in eigenen Serverräumen von MINTANO betrieben. Die physische Sicherheit der eingesetzten Rechenzentrums-, Hosting- und Cloud-Infrastruktur wird durch die jeweiligen Anbieter gewährleistet.

1.2 Zugangskontrolle

Der Zugang zu Systemen und Anwendungen erfolgt über Benutzerkonten, Passwörter, Gerätecodes oder vergleichbare Authentifizierungsverfahren.

Für administrative Zugänge und geschäftskritische Systeme wird, soweit technisch verfügbar und nach Schutzbedarf angemessen, Mehr-Faktor-Authentifizierung eingesetzt.

MINTANO setzt für die Verarbeitung personenbezogener Daten grundsätzlich firmeneigene Apple-Endgeräte ein. Diese werden zentral über ein Mobile-Device-Management verwaltet.

Die Nutzung privater Endgeräte für die Verarbeitung von Auftragsdaten ist grundsätzlich nicht vorgesehen, sofern sie nicht im Einzelfall ausdrücklich freigegeben und mit angemessenen

Schutzmaßnahmen versehen ist.

Firmeneigene Endgeräte werden durch technische Schutzmaßnahmen wie Benutzerkonten, Gerätecodes, automatische Bildschirmsperren und systemseitig verfügbare Sicherheitsfunktionen geschützt. Lokale Speicherungen personenbezogener Daten werden auf das erforderliche Maß begrenzt.

1.3 Zugriffskontrolle

MINTANO beschränkt den Zugriff auf personenbezogene Daten nach dem Erforderlichkeitsprinzip. Zugriffsrechte werden rollen- oder funktionsbezogen vergeben und auf diejenigen Personen beschränkt, die sie zur Erfüllung ihrer Aufgaben benötigen.

Administrative Berechtigungen werden auf einen begrenzten Personenkreis beschränkt.

Berechtigungen werden bei Eintritt, Austritt und Rollenwechsel angepasst sowie regelmäßig oder anlassbezogen überprüft.

Mitarbeitende, die personenbezogene Daten verarbeiten, werden auf Vertraulichkeit verpflichtet und erhalten angemessene Datenschutz- und Sicherheitsunterweisungen. Ein Datenschutzbeauftragter ist benannt.

1.4 Trennung von Daten, Systemen und Zwecken

Personenbezogene Daten unterschiedlicher Auftraggeber, Projekte oder Zwecke werden organisatorisch und, soweit durch die eingesetzten Systeme vorgesehen, logisch voneinander getrennt.

Die Trennung erfolgt insbesondere durch getrennte Projekte, Mandanten, Kundenkonten, Speicherorte, Rollen, Berechtigungen oder sonstige systemseitige Trennmechanismen. Eine physische Trennung sämtlicher Daten auf gesonderten Datenträgern oder Systemen wird nicht pauschal zugesagt.

Produktivsysteme werden von Test-, Entwicklungs- und Staging-Umgebungen organisatorisch und, soweit technisch vorgesehen, logisch getrennt.

Für Test-, Entwicklungs- und Staging-Zwecke werden nach Möglichkeit keine produktiven personenbezogenen Daten verwendet. Soweit eine Verarbeitung produktiver Auftragsdaten in solchen Umgebungen im Einzelfall erforderlich ist, erfolgt sie nur im erforderlichen Umfang und unter Berücksichtigung angemessener Schutzmaßnahmen.

1.5 Pseudonymisierung und Datenminimierung

MINTANO verarbeitet personenbezogene Daten nur in dem Umfang, wie dies zur Erbringung der vereinbarten Leistungen, zur Umsetzung dokumentierter Weisungen des Auftraggebers oder zur Erfüllung gesetzlicher Pflichten erforderlich ist.

Soweit möglich und dem jeweiligen Verarbeitungszweck sowie Schutzbedarf angemessen, werden personenbezogene Daten minimiert, logisch getrennt, pseudonymisiert oder anonymisiert.

Pseudonymisierungs- oder Anonymisierungsmaßnahmen werden insbesondere dann eingesetzt, wenn sie nach Art der Leistung technisch möglich und für den jeweiligen Zweck geeignet sind.

1.6 Verschlüsselung

MINTANO setzt Verschlüsselungsverfahren nach dem Stand der Technik ein, soweit dies nach Art, Umfang und Schutzbedarf der jeweiligen Verarbeitung angemessen und technisch möglich ist.

Die Übertragung personenbezogener Daten über öffentliche Netze erfolgt grundsätzlich verschlüsselt, insbesondere mittels TLS/SSL oder vergleichbarer Verfahren.

Soweit personenbezogene Daten in Hosting-, Cloud- oder SaaS-Systemen verarbeitet werden, werden Anbieter eingesetzt, die angemessene Maßnahmen zur Verschlüsselung, Zugriffsbeschränkung, Datentrennung und Verfügbarkeit bereitstellen.

2. Integrität

2.1 Eingabekontrolle und Nachvollziehbarkeit

MINTANO trifft geeignete Maßnahmen, um personenbezogene Daten vor unbeabsichtigter oder unbefugter Veränderung zu schützen.

Hierzu gehören insbesondere rollenbasierte Berechtigungen, beschränkte administrative Zugriffe, technische Zugriffsschutzmaßnahmen sowie die Nutzung systemseitiger Änderungs- und Protokollfunktionen.

Zugriffe, Änderungen und sicherheitsrelevante Systemereignisse werden nachvollziehbar gemacht, soweit dies durch die eingesetzten Systeme, Dienste und Anwendungen unterstützt wird.

Umfang, Dauer und Auswertung der Protokollierung richten sich nach Schutzbedarf, technischer Verfügbarkeit und Zweck der jeweiligen Verarbeitung.

Eine lückenlose Protokollierung sämtlicher Zugriffe über alle eingesetzten Systeme hinweg wird nicht pauschal zugesagt.

2.2 Weitergabekontrolle

Personenbezogene Daten werden nur weitergegeben, soweit dies zur Erbringung der vereinbarten Leistungen erforderlich ist, auf dokumentierter Weisung des Auftraggebers erfolgt oder durch den Auftragsverarbeitungsvertrag zugelassen ist.

Elektronische Übermittlungen erfolgen grundsätzlich verschlüsselt oder über geschützte Systemzugänge.

Bei der Einbindung von Unterauftragnehmern werden nur solche Daten übermittelt, die für die jeweilige Leistung erforderlich sind.

Soweit eine Drittlandverarbeitung stattfindet oder ein Zugriff aus einem Drittland nicht ausgeschlossen werden kann, stellt MINTANO im Rahmen der eigenen vertraglichen und tatsächlichen Möglichkeiten sicher, dass die Voraussetzungen der Art. 44 ff. DSGVO eingehalten werden.

Dies erfolgt insbesondere auf Grundlage von Angemessenheitsbeschlüssen der Europäischen Kommission, verbindlichen internen Datenschutzvorschriften, Standardvertrags- beziehungsweise Standarddatenschutzklauseln der Europäischen Kommission – gegebenenfalls ergänzt um zusätzliche Schutzmaßnahmen – oder anderen gesetzlich zulässigen Transfermechanismen.

2.3 Auftragskontrolle und Unterauftragnehmer

Unterauftragnehmer werden unter Berücksichtigung von Art und Umfang der Verarbeitung, Schutzbedarf der Daten und bereitgestellten Sicherheitsmaßnahmen ausgewählt.

Soweit erforderlich, werden Vereinbarungen zur Auftragsverarbeitung oder sonstige geeignete Datenschutzvereinbarungen geschlossen.

Der Einsatz von Unterauftragnehmern richtet sich nach der jeweils geltenden Unterauftragnehmerliste beziehungsweise den Regelungen des Auftragsvertragsvertrages.

MINTANO achtet darauf, dass Unterauftragnehmer nur solche personenbezogenen Daten erhalten, die

für die jeweilige Leistung erforderlich sind.

2.4 Lösch- und Datenträgerkontrolle

Die Löschung oder Rückgabe von Auftragsdaten erfolgt nach Maßgabe des Auftragsvertrags, der vereinbarten Leistungsbeschreibung, dokumentierter Weisungen des Auftraggebers oder gesetzlicher Vorgaben.

Automatische Löschungen nach Vertragsende werden nicht pauschal zugesagt. Soweit Löschfristen, Löszeitpunkte oder Löslogiken durch den Auftraggeber festgelegt werden, setzt MINTANO diese im Rahmen der bereitgestellten technischen und organisatorischen Möglichkeiten um.

Löschungen werden in angemessenem Umfang dokumentiert, soweit dies technisch vorgesehen und für die jeweilige Verarbeitung erforderlich ist.

Datenträger und lokale Datenbestände werden sicher gelöscht oder vernichtet, soweit sie nicht mehr benötigt werden und keine gesetzlichen oder vertraglichen Aufbewahrungspflichten entgegenstehen.

3. Verfügbarkeit und Belastbarkeit

3.1 Verfügbarkeit der Systeme und Dienste

MINTANO trifft geeignete Maßnahmen, um die Verfügbarkeit der für die Auftragsverarbeitung eingesetzten Systeme und Dienste angemessen sicherzustellen.

Hierzu gehören insbesondere der Einsatz professioneller Hosting-, Cloud- und SaaS-Anbieter, eigene Datensicherungen relevanter Systeme und Datenbestände sowie interne Zuständigkeiten für Backup- und Wiederherstellungsprozesse.

Umfang, Frequenz und Aufbewahrungsdauer von Datensicherungen richten sich nach Kritikalität des jeweiligen Systems, Schutzbedarf der Daten und vertraglichen Anforderungen.

Maßnahmen zur physischen Rechenzentrumssicherheit, Stromversorgung, Brandschutz, Klimatisierung, Redundanz und infrastrukturseitigen Überwachung werden, soweit einschlägig, durch die eingesetzten Hosting-, Cloud- oder SaaS-Anbieter gewährleistet.

3.2 Backup und Wiederherstellung

MINTANO trifft geeignete Maßnahmen, um die Verfügbarkeit personenbezogener Daten im Fall technischer Störungen, Systemausfälle oder sonstiger betrieblicher Unterbrechungen im angemessenen Umfang wiederherstellen zu können.

Hierzu gehören insbesondere regelmäßige Datensicherungen relevanter Systeme und Datenbestände, interne Zuständigkeiten für Backup- und Wiederherstellungsprozesse sowie die Einbindung der jeweils eingesetzten Hosting-, Cloud- und SaaS-Anbieter.

Die Wiederherstellbarkeit wird risikobasiert, stichprobenartig oder anlassbezogen überprüft.

Konkrete Wiederherstellungszeiten werden nur geschuldet, soweit sie ausdrücklich vertraglich vereinbart sind.

3.3 Belastbarkeit und Schutz vor Störungen

MINTANO setzt Systeme, Dienste und Anbieter ein, die eine dem jeweiligen Verarbeitungszweck angemessene Belastbarkeit und Stabilität unterstützen.

Die technische Ausgestaltung richtet sich nach Art und Umfang der vereinbarten Leistungen, dem

Schutzbedarf der Daten sowie den durch die eingesetzten Hosting-, Cloud- und SaaS-Anbieter bereitgestellten Funktionen.

Soweit im Verantwortungsbereich von MINTANO liegend, werden Softwareupdates, Patches und sicherheitsrelevante Aktualisierungen regelmäßig eingespielt.

Die Nutzung und Auslastung wesentlicher Systeme wird im Rahmen der verfügbaren technischen Möglichkeiten überwacht oder durch die eingesetzten Anbieter abgesichert.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.1 Überprüfung der Maßnahmen

MINTANO überprüft die Angemessenheit und Wirksamkeit der technischen und organisatorischen Maßnahmen regelmäßig sowie anlassbezogen.

Anlassbezogene Prüfungen erfolgen insbesondere bei wesentlichen Änderungen eingesetzter Systeme, Dienstleister, Prozesse oder Risiken.

Zu den Überprüfungsmaßnahmen gehören insbesondere die Prüfung von Berechtigungen, Datenschutz- und Sicherheitsunterweisungen, Bewertung eingesetzter Dienstleister, regelmäßige Softwareupdates und Patches sowie die Anpassung interner Vorgaben.

4.2 Schulung und Sensibilisierung

Mitarbeitende, die personenbezogene Daten verarbeiten, werden auf Vertraulichkeit verpflichtet und erhalten angemessene Datenschutz- und Sicherheitsunterweisungen.

Die Unterweisungen erfolgen risikobasiert, anlassbezogen oder im Rahmen interner organisatorischer Prozesse.

MINTANO stellt interne Ansprechpartner für Datenschutz- und IT-Sicherheitsfragen bereit. Ein Datenschutzbeauftragter ist benannt.

4.3 Weiterentwicklung der Maßnahmen

Die technischen und organisatorischen Maßnahmen können weiterentwickelt oder durch gleichwertige Maßnahmen ersetzt werden, sofern das vereinbarte Schutzniveau nicht wesentlich unterschritten wird.

Änderungen erfolgen insbesondere zur Anpassung an technische Entwicklungen, geänderte Systemlandschaften, neue Dienstleister, organisatorische Änderungen oder geänderte Risiken.

Wesentliche Änderungen, die das Schutzniveau erheblich beeinträchtigen können, werden nach Maßgabe des Auftragsvertrages mitgeteilt oder abgestimmt, soweit dies gesetzlich oder vertraglich erforderlich ist.

5. Dokumentation

MINTANO dokumentiert wesentliche Datenschutz- und Sicherheitsmaßnahmen in angemessenem Umfang. Hierzu gehören insbesondere interne Vorgaben, Vertraulichkeitsverpflichtungen, Unterweisungen, Berechtigungsänderungen, Weisungen des Auftraggebers, Löschungen sowie relevante Prüfungen. Die Dokumentation dient dem Nachweis der Einhaltung der vereinbarten technischen und organisatorischen Maßnahmen sowie der Unterstützung des Auftraggebers im Rahmen seiner gesetzlichen und vertraglichen Pflichten.