Intermundia – ToM und DSGVO

Stand 06.10.2025

Intermundia GmbH
Heiligenbreite 52
88662 Überlingen
Telefon: 49 7551 971 95 04
E-Mail: support@intermundia.de

INHALT

EINLEITUNG

Dieses Dokument beschreibt die technischen und organisatorischen Maßnahmen (ToMs), sowie Anforderungen an die Datenschutz-Grundverordnung (DSGVO) und deren Umsetzung. Es umfasst sowohl die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 DSGVO als auch umfassende Maßnahmen zur digitalen Datenverarbeitung nach anerkannten Best Practices (ISO 27001, BSI Grundschutz, Bitkom).

TECHNISCH-ORGANISATORISCHE MAßNAHMEN (TOM)

1. EINHALTUNG GENEHMIGTER VERHALTENSREGELN GEMÄß ART. 40 DSGVO

Kategorie	Zweck / Ziel	Beschreibung der Maßnahme	Umsetzungsstand / Nachweis
Rechtliche & organisatorische Maßnahmen	Sicherstellung, dass die Verarbeitung personenbezogener Daten im Einklang mit anerkannten Datenschutzstandards erfolgt	Intermundia verpflichtet sich zur Einhaltung der von den zuständigen Behörden der Europäischen Union gemäß Artikel 40 DSGVO genehmigten Verhaltensregeln (Codes of Conduct). Diese dienen der Förderung einer ordnungsgemäßen Anwendung der DSGVO.	Interne Prozesse werden regelmäßig auf Konformität mit den genehmigten Verhaltensregeln geprüft.
Verfahrensüberprüfung & Compliance	Laufende Sicherstellung der datenschutzkonformen Umsetzung der Verhaltensregeln	Intermundia überprüft regelmäßig seine Datenschutzprozesse und -richtlinien im Hinblick auf die Anforderungen der einschlägigen Verhaltensregeln. Änderungen oder Aktualisierungen werden fortlaufend berücksichtigt.	Implementiert; Verantwortliche Abteilung führt jährliche Überprüfungen und Aktualisierungen durch.
Schulung & Sensibilisierung	Förderung des Bewusstseins und der Einhaltung der Verhaltensregeln bei Mitarbeitenden	Mitarbeitende, die personenbezogene Daten verarbeiten, werden inhaltlich zu den geltenden Verhaltensregeln und deren Bedeutung für den Datenschutz geschult.	Schulungsnachweise liegen vor; jährliche Schulungen dokumentiert.

2. TOMS ZUR DIGITALEN DATENVERARBEITUNG

Die folgenden Maßnahmen orientieren sich an anerkannten Datenschutz- und Sicherheitsstandards (ISO 27001, BSI Grundschutz, Bitkom) und gewährleisten den Schutz personenbezogener Daten bei der digitalen Verarbeitung, Speicherung und Übertragung.

Kategorie	Zweck / Ziel	Beschreibung der Maßnahme	Umsetzungsstand / Nachweis
Zutrittskontrolle (physisch)	Verhinderung unbefugten physischen Zutritts zu Datenverarbeitungseinrichtungen	Zugang nur für autorisierte Personen über elektronische Zutrittskontrollsysteme; Besucherregistrierung und Begleitung; Videoüberwachung und Alarmanlagen.	Zutrittsprotokolle, Sicherheitskonzept
Zugangskontrolle (logisch)	Schutz vor unbefugter Nutzung von IT-Systemen	Personalisierte Benutzerkonten, 2-Faktor-Authentifizierung, zentrale Benutzerverwaltung, Passwort-Policies nach ISO 27001.	Benutzerverwaltung, IT-Sicherheitsrichtlinie, Auditberichte
Zugriffskontrolle	Verhinderung unbefugter Datenzugriffe innerhalb des Systems	Rollen- und Rechtekonzept, regelmäßige Überprüfung, technische Zugriffsbeschränkungen, Audit-Trails.	Berechtigungskonzept, Prüfprotokolle
Verfügbarkeitskontrolle (Backups)	Schutz vor Datenverlust	Automatisierte tägliche Backups, georedundante Speicherung, Verschlüsselung (AES-256), Wiederherstellungstests, Notfallübungen.	Backup-Protokolle, Wiederherstellungsberichte
Datenverschlüsselung	Sicherung der Vertraulichkeit personenbezogener Daten	Datenverschlüsselung im Ruhezustand (AES-256) und bei Übertragung (TLS 1.3); sicheres Key-Management.	Verschlüsselungskonzept
Netzwerksicherheit	Schutz vor externen und internen Angriffen	Mehrstufiges Firewall-System (Perimeter/Host), IDS/IPS, DMZ-Struktur,	Netzwerksicherheitskonzept

		regelmäßige Penetrationstests.	
Patch- & Update-Management	Schließen von Sicherheitslücken	Automatische Updates über zentrale Systeme; priorisierte Installation sicherheitsrelevanter Patches.	Patchberichte, Wartungsprotokolle
Endgerätesicherheit	Schutz mobiler und stationärer Endgeräte	Geräteverschlüsselung, aktuelle Virenschutzsoftware, Mobile-Device-Management (MDM), eingeschränkte Administratorrechte.	MDM-Berichte, IT-Richtlinien
Passwortsicherheit	Vermeidung unbefugter Kontoübernahmen	Passwort-Policy: mind. 12 Zeichen, Groß-/Kleinbuchstaben, Zahlen, Sonderzeichen, keine Wiederverwendung; Passwortmanager zwingend notwendig.	Passwort-Richtlinie, Auditberichte
Notfallmanagement	Aufrechterhaltung der Prozesse im Krisenfall	Notfall- und Wiederanlaufplan (BCP/DRP) mit klaren Rollen; Backup-Systeme außerhalb des Netzwerks.	Notfall Best Practices
Mitarbeitersensibilisierung	Förderung der Datenschutzkultur	Verpflichtende jährliche Schulungen, Awareness-Kampagnen, Phishing-Simulationen.	Schulungsnachweise, Awareness-Reports

3. ABSCHLUSS

Intermundia verpflichtet sich, alle beschriebenen Maßnahmen regelmäßig zu überprüfen, zu aktualisieren und an den Stand der Technik anzupassen. Dies gewährleistet ein hohes Niveau an Datenschutz, Informationssicherheit und Compliance.