Technische und organisatorische Maßnahmen (TOM)

Stand: 17. Juni 2026

Dies ist die aktuell gültige Fassung. Frühere Fassungen findest du im Archiv unten.

Technische und organisatorische Maßnahmen gem. Art. 32 DS-GVO

cubic solutions gewährleistet für die Auftragsverarbeitung ein angemessenes Schutzniveau. Grundlage ist unser nach ISO/IEC 27001:2022 zertifiziertes Informationssicherheits-Managementsystem, das Richtlinien, Risiken und Maßnahmen laufend steuert und jährlich extern geprüft wird. cubic solutions unterhält keine eigenen Geschäfts- oder Serverräume und keine eigene Rechenzentrumsinfrastruktur; gearbeitet wird mobil in zertifizierten Cloud- und SaaS-Diensten. Die folgenden Maßnahmen fassen den Schutz nach Art. 32 DS-GVO je Kategorie zusammen.

Zutrittskontrolle

Da cubic solutions keine eigenen Geschäfts- oder Serverräume unterhält, wird die physische Sicherheit, also Gebäude- und Raumsicherung, Zutrittsschutz und Brandschutz, durch die eingesetzten, nach anerkannten Standards zertifizierten Cloud- und Rechenzentrumsbetreiber gewährleistet.

Zugangskontrolle

Der Zugang zu Systemen ist über individuelle Benutzerkonten je Mitarbeitenden und eine zentrale Identitäts- und Zugriffsverwaltung geschützt. Es gelten eine Passwortrichtlinie mit Mindestanforderungen und die verschlüsselte Speicherung von Zugangsdaten. Endgeräte sind verschlüsselt und sperren automatisch bei Inaktivität. Eine zentral verwaltete Endpoint-Security (Virenschutz, Firewall, Angriffserkennung) und ein automatisiertes Patch-Management schützen vor Schadsoftware und bekannten Schwachstellen. Daten werden verschlüsselt gespeichert, administrative Zugriffe werden protokolliert.

Zugriffskontrolle

Zugriffe auf personenbezogene Daten erfolgen rollenbasiert nach dem Need-to-know-Prinzip. Alle Mitarbeitenden sind vertraglich auf das Datengeheimnis verpflichtet. Ergänzend gelten eine Clean-Desk-Richtlinie und das zentral durchgesetzte Verbot nicht autorisierter Software-Installationen.

Weitergabekontrolle

Bei der Übertragung werden personenbezogene Daten geschützt: E-Mails können verschlüsselt versendet werden, Endgeräte und Datenträger sind verschlüsselt, und die Übertragung läuft über die gesicherten, verschlüsselten Verbindungen (TLS) der eingesetzten Cloud-Dienste.

Eingabekontrolle

Über individuelle Benutzerkonten und rollenabhängige Zugriffsbeschränkungen ist nachvollziehbar, wer auf Daten zugreift. Administrative Änderungen werden protokolliert.

Auftragskontrolle

Externe Dienstleister werden sorgfältig nach Datenschutzgesichtspunkten ausgewählt und vertraglich verpflichtet. Mitarbeitende werden regelmäßig im Datenschutz geschult. Der Datenschutzbeauftragte wird bei neuen oder geänderten

Verarbeitungsverfahren eingebunden.

Verfügbarkeitskontrolle

Daten werden regelmäßig und automatisiert auf getrennten Systemen gesichert; für die Wiederherstellung bestehen entsprechende Verfahren. Redundanz, geografisch getrennte Rechenzentren, unterbrechungsfreie Stromversorgung, Klimatisierung und Brandschutz werden über die eingesetzten zertifizierten Cloud-Anbieter sichergestellt.

Trennungskontrolle

Kunden- und Projektdaten werden logisch getrennt verarbeitet: je Kunde bzw. Kontext bestehen eigene Arbeitsbereiche, auf die nur die jeweils berechtigten Personen Zugriff haben.