Docusign Envelope ID: F1EE9337-0CED-43B2-8493-EBD8CF63A66C

Anlage 5: Technische und organisatorische Maßnahmen nach Art. 32 DSGVO für msg.CodIQ

msg systems ag

Version: 1.0

Stand: Januar 2026

Klassifizierung: öffentlich

www.msg.group

Docusign Envelope ID: F1EE9337-0CED-43B2-8493-EBD8CF63A66C

Inhaltsverzeichnis

© msg systems ag 2026 - öffentlich

Docusign Envelope ID: F1EE9337-0CED-43B2-8493-EBD8CF63A66C

© msg systems ag 2026 - öffentlich

Docusign Envelope ID: F1EE9337-0CED-43B2-8493-EBD8CF63A66C

1 Allgemein

1.1 Ziel und Zweck

Nach Art. 28 Abs. 3 c) i. V. m. Art. 32 Abs. 1 DSGVO ist der Auftragnehmer im Rahmen der Auftragsdatenverarbeitung unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technisch-organisatorischen Maßnahmen sorgfältig auszuwählen. Die in diesem Dokument beschriebenen technisch-organisatorischen Maßnahmen gemäß Art. 32 DSGVO sind als msg-Standard zu verstehen und beziehen sich sowohl auf alle Standorte der msg systems ag, als auch auf das Mobile Arbeiten. Sie finden Anwendung zwischen den Parteien, sofern eine Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DSGVO geschlossen wurde. Individuelle Ergänzungen und Detaillierungen im Rahmen der Auftragsverarbeitung sind in der jeweiligen Auftragsverarbeitungsvereinbarung festzulegen.

1.2 Bearbeitungsvermerke des Datenschutzbeauftragten

Die Wiedervorlage zur Prüfung bzw. Aktualisierung erfolgt bei meldepflichtigen Änderungen in Angaben dieses Dokumentes. Eine Prüfung erfolgt jedoch spätestens im Jahresturnus.

1.3 Vollständigkeitserklärung, Freigabe

Der Vorstand der msg systems ag sowie der Datenschutzbeauftragte bestätigen die Vollständigkeit und Richtigkeit der nachfolgenden Angaben und erteilen hiermit die Freigabe für dieses Dokument.

Ismaning, den 09.02.2026

Signiert von:
30E315B28E714C6...
(Dr. Jürgen Zehetmaier – Vorstandsvorsitzender)

Signiert von:
4CD787D59A0A4D1...
(Peter Zach – CRO)

Signiert von:
35D958763952438...
(Claus Bauer – Beauftragter für den Datenschutz in der msg Gruppe)

Docusign Envelope ID: F1EE9337-0CED-43B2-8493-EBD8CF63A66C

1.4 Begriffsbestimmungen

In diesem Kapitel werden Begriffe definiert, die in den folgenden Kapiteln verwendet werden. Darüber hinaus gelten die bestehenden Policies.

Mobiles Arbeiten

Unter „Mobilem Arbeiten“ versteht sich die Erbringung der Arbeitsleistung an beliebig wechselnden Orten außerhalb eines Standortes der msg Gruppe. Diese kann sowohl online als auch offline und sowohl ganztägig oder auch tagesanteilig erfolgen.

Folgende Bereiche fallen unter den Begriff „Mobiles Arbeiten“:

- Homeoffice: die private Räumlichkeit, die regelmäßig und überwiegende zum Mobilen Arbeiten genutzt wird
- Andere Räumlichkeiten (z.B. Hotel, andere private Umgebungen)
- Unterwegs (z.B. auf Reisen im Flugzeug, der Bahn oder im Auto)

Nicht unter den Begriff „Mobiles Arbeiten“ fallen:

- msg Standorte
- Telearbeit gemäß § 2 Abs. 7 ArbStättV

msg Standort

Unter „msg Standort“ versteht man einen Arbeitsplatz an einem beliebigen Standort der msg Gruppe mit CIT-Integration (Zugang CIT-Netz).

Docusign Envelope ID: F1EE9337-0CED-43B2-8493-EBD8CF63A66C

2 Infrastrukturelle Angaben zur msg systems ag

Die msg systems ag verfügt über eine heterogene Systemlandschaft, die sich durch unterschiedliche Serverplattformen und entsprechend unterstützende System-Software kennzeichnet. Die Rechnerlandschaft umfasst Server mit Betriebssystemen wie Microsoft Windows Server, Z/OS, Unix- und Linux-Distributionen. Das Unternehmen setzt die marktüblichen Applikationen, Datenbanken und Web-Tools zur Entwicklung, Erstellung, Vertrieb und Unterstützung ihrer Produkte ein.

Auf Grundlage der Leitlinie zur Informationssicherheit, die von den msg-Vorständen in neuester Version 2025 verabschiedet wurde, erfolgt ein stufenweiser Aufbau eines Informationssicherheitsmanagement-Systems (ISMS) in der msg systems ag.

Die Erstzertifizierung des ISMS erfolgte im Bereich Automotive im April 2017. Die letzte ISO Rezertifizierung erfolgte im Jahr 2024 nach DIN EN ISO / IEC 27001:2022.

Die Branche Automotive wurde zudem an den Standorten Ismaning, Leinfelden-Echterdingen und Ingolstadt nach dem VDA Label TISAX AL3, besonderer Datenschutz- und Prototypenteilebau speziell in Ismaning, geprüft.

Eine Zertifizierung des für msg.CodIQ verantwortlichen Bereichs Public Sector nach DIN EN ISO / IEC 27001:2022 ist für das Jahr 2026 geplant.

Die zentralen Komponenten der IT-Infrastruktur der msg systems ag werden durch den Zentralbereich IT & Organisation betrieben.

Darüber hinaus werden Cloud basierte Dienste genutzt und im Zuge des Multi-Provider Managements einige IT-Services durch externe Partner erbracht. Beispiele hierfür sind Microsoft sowie weitere Cloud Dienstleister. Hier bestehen Vereinbarungen zur Auftragsverarbeitung mit den Dienstleistern, sofern personenbezogene Daten betroffen sind.

Durch eine unternehmensübergreifende Sicherheitsorganisation und regelmäßige Termine des GRO Information Security-Teams mit dem Datenschutzbeauftragen kann eine angemessene Berücksichtigung der Anforderungen des Art. 32 DSGVO sichergestellt werden.

Das Hauptgebäude der msg systems ag befindet sich in der Robert-Bürkle-Straße 1 in 85737 Ismaning (R1). Alle Gebäude der msg sind in verschiedene Sicherheitszonen unterteilt. Diese Zonen können, je nach Berechtigungsstufe, über ein elektronisches, oder manuelles Zutrittssystem mit einer Zutrittskarte/Schlüssel betreten werden. In dem Hauptgebäude befindet sich das Rechenzentrum RZ R1. Das Backup-Rechenzentrum RZ K30 befindet sich bei Noris Networks, Klausnerstraße 30, 85609 Aschheim (K30).

Die Rechenzentren werden als Full Managed Datacenter durch den Zentralbereich IT & Organisation betrieben. Durch ein automatisiertes Monitoring wird ein 7 x 24 Stunden Betrieb an 365 Tagen gewährleistet. Die Rechenzentren RZ R1 ist ISO 27001 zertifiziert, das RZ K30 ist ISO 27001 & EN 50600 zertifiziert.

Docusign Envelope ID: F1EE9337-0CED-43B2-8493-EBD8CF63A66C

3 Technisch-organisatorische Maßnahmen

Die Einhaltung und Umsetzung der nachfolgenden Maßnahmen sind bei der msg systems ag über die Leitlinie zur Informationssicherheit geregelt. Die msg systems ag betreibt ein nach ISO 27001 zertifiziertes Informationssicherheitsmanagement-System (ISMS), in welches 2026 auch der Bereich Public Sector aufgenommen wird. Daneben betreibt die msg systems ag ein nach ISO 9001 zertifiziertes Qualitätsmanagement-System (QMS). Ein Data Protection Management System (DPMS) berücksichtigt die Anforderungen der DSGVO und ist nach dem Muster der ISO 27701 aufgebaut.

Sofern durch den Zentralbereich IT und Organisation weitere Dienstleister in die Leistungserbringung einbezogen werden, sind auch diese über Verträge zur Auftragsverarbeitung gebunden. Bei der Dienstleisterauswahl wird auf eine Zertifizierung nach ISO 27001 oder vergleichbare Zertifizierungen geachtet.

Bei der Verarbeitung wird im weiteren Unterauftragsverhältnis der Dienstleister AWS eingesetzt (siehe CodIQ Testlizenzvereinbarung SaaS-Vertrag Anlage 4 AV). Es gelten damit auch die technisch organisatorischen Maßnahmen von AWS auf die hiermit verwiesen wird. Allgemeine Informationen zu diesem Thema finden sie unter Navigating GDPR Compliance on AWS. Eine Übersicht der genutzten Services erhalten sie auf Anfrage.

Zur Wahrung der Beratung- und Kontrollfunktionen im Rahmen der DSGVO und des BDSG wird ein Datenschutzbeauftragter (DSB) eingesetzt. Er wird bei seiner Arbeit durch einen Datenschutzkoordinator (DSK) unterstützt.

Kontaktdaten des Datenschutzbeauftragten (DSB): Herr Claus Bauer, datenschutz@msg.group

Die Mitarbeitenden erhalten, neben den Regelungen im Arbeitsvertrag (Verpflichtung auf Vertraulichkeit), zu Beginn ihrer Tätigkeit eine Datenschutzunterweisung. Später erfolgt eine regelmäßige Sensibilisierung durch Newsletter, Schulungen und persönliche Ansprachen sowie interne Audits.

Zu den Maßnahmen, die gewährleisten, dass die innerbetriebliche Organisation so gestaltet ist, dass sie den Anforderungen des Datenschutzes gerecht wird, gehören unter anderem:

- Ein ISMS/DPMS nach ISO 27001
- Eine implementierte ISMS-DB (Information Security Management System Database)
- Ein Corporate Security Management Portal
- Ein für alle Mitarbeitenden zugängliches ISMS-Handbuch
- Eine implementierte CMDB (Configuration Management Database; Beschreibung der IT-Komponenten) (Integration von msg.CodIQ erfolgt bis Q3/2026)
- Ein Krisenmanagement / Business Continuity Management inkl. zugehöriger Disaster Recovery Verfahren (Integration von msg.CodIQ erfolgt bis Q3/2026)
- Ein qualifiziertes Wertemanagement (Asset-Management)

Die Schutzziele, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit nach Art. 32 DSGVO werden im Rahmen des ISMS/DPMS sichergestellt.

Nachfolgend sind die Maßnahmen gemäß Art. 32 DSGVO beschrieben.

Docusign Envelope ID: F1EE9337-0CED-43B2-8493-EBD8CF63A66C

3.1 Vertraulichkeit

3.1.1 Zutrittskontrolle

Maßnahmen, die Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehren:

- Personalisierte, elektronische Zutrittskontrollsysteme für Büroräume und Rechenzentren (Multi-Faktor): Zutrittsberechtigung haben nur autorisierte Mitarbeitende. Die entsprechenden Zutrittsberechtigungen werden regelmäßig überprüft.
- Einsatz eines Transponder-/Karten-/Schlüssel-Schließanlagesystems für ausgewählte Büroräume
- Dienstanweisungen zur Handhabung von Zutrittskontrollen
- Richtlinien zur Begleitung und Kennzeichnung von Gästen im Gebäude
- Abhängig vom Standort: Einsatz von Wachdienst mit regelmäßigen Rundgängen, Alarmanlagen und datenschutzkonformer Videoüberwachung in sicherheitskritischen Bereichen (z.B. Rechenzentren)
- Zutrittslisten in den Rechenzentren
- Durch unabhängiges Zutrittssystem gesicherte Rechenzentren

3.1.2 Zugangskontrolle

Maßnahmen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Organisatorische und technische Regelung zum sicheren und ordnungsgemäßen Einsatz von Passwörtern
- Serversysteme in den Rechenzentren, bzw. In der Cloud sind nur mit personalisierten Administrationsaccounts zu administrieren. Diese sind zusätzlich über eine 2-Faktor Authentifikation geschützt.
- Eindeutige Zuordnung von Benutzerkonten zu Benutzern, keine unpersönlichen Sammelkonten
- Festplatten- und Datenträgerverschlüsselung, durch Security Policy vorgeschriebener Diebstahlschutz
- Einsatz von mehrstufigen Schutzmechanismen (Multi-VendorEndpoint Detection Systeme, Multi-Vendor Firewalls)
- Einsatz eines zentral gesteuerten Patchmanagements und einer Vulnerability Management Lösung
- Richtlinie zum physischen Schutz benutzter Systeme (Clean Desk Policy, Bildschirmsperre, Blickschutzfilter)
- Netzwerksegmentierung, Netzzonen, Firewalls
- Logische Zugangsregelung zum Netzwerk, Netzwerkzugang erhalten nur freigegebene Unternehmensgeräte (zertifikatsbasierte Network Access Control-Lösung)

Zusätzlich zu den hier genannten allgemeinen Maßnahmen für Systeme der msg systems ag wurden speziell für msg.CodIQ folgende Maßnahmen umgesetzt:

- Der Zugriff auf IT-Ressourcen erfolgt rollenbasiert nach dem Least-Privilege-Prinzip. Hochprivilegierte Konten werden besonders geschützt und nicht für den Regelbetrieb genutzt.
- Die IT-Infrastruktur ist logisch segmentiert. Öffentliche Zugriffe erfolgen ausschließlich über vorgelagerte Sicherheits- und Zugriffskomponenten; interne Systeme sind nicht direkt öffentlich erreichbar.

Diese Maßnahmen werden laufend erweitert.

Docusign Envelope ID: F1EE9337-0CED-43B2-8493-EBD8CF63A66C

3.1.3 Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können:

- Clean Desk Policy
- Benutzeridentifizierung und Berechtigungsvergabeverfahren (Identity and Access Management)
- Trennung von Berechtigungsbewilligung (organisatorisch) durch den Verantwortlichen sowie Berechtigungsvergabe (technisch) durch die IT
- Einsatz einer Identity and Access Management – Plattform
- Netzlaufwerke mit Zugriff nur für berechtigte Benutzer(-gruppen)
- Richtlinie zum Patchlevel eingesetzter Systeme (Security-Policy für CIT-Devices)

Zusätzlich zu den hier genannten allgemeinen Maßnahmen für Systeme der msg systems ag wurden speziell für msg.CodIQ folgende Maßnahmen umgesetzt:

- Nutzeridentitäten werden über ein zentrales Authentifizierungssystem verwaltet. Sicherheitsmechanismen wie Passwort-Richtlinien und Sitzungsbegrenzungen werden eingesetzt. Mehrfaktor-Authentifizierung wird für privilegierte Zugänge eingesetzt und kann auch für andere Benutzer eingesetzt werden.
- Zugangsdaten und sonstige vertrauliche Informationen werden sicher gespeichert und nicht im Klartext in Anwendungen oder Konfigurationsdateien abgelegt.

3.1.4 Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

- Logische Mandantentrennung
- Trennung von Test- und Produktionsumgebungen
- Aufgabentrennung der Mitarbeitenden (segregation of duties)

3.1.5 Pseudonymisierung

Bei der Pseudonymisierung handelt es sich um eine zentrale technische und organisatorische Sicherungsmaßnahme, welche die DSGVO nicht nur in Art. 32 Abs. 1a), sondern wiederholt in unterschiedlichen Zusammenhängen erwähnt. Sie kann Einfluss auf die Zulässigkeit einer Verarbeitung personenbezogener Daten haben und erhöht den Schutz der Rechte und Freiheiten der Betroffenen. Der Erwägungsgrund 26 DSGVO stellt hierbei eindeutig heraus, dass auch pseudonymisierte Daten weiterhin personenbezogene Daten bleiben. Grundsätzlich stehen drei Pseudonymisierungsmethoden zur Verfügung:

• Der Betroffene vergibt selbst ein Pseudonym und separiert dieses von den Daten, die ihn identifizieren.
• Ein unabhängiger Dritter, der über die entsprechende Zuordnungsregel verfügt, vergibt ein Pseudonym für den Betroffenen.
• Die verantwortliche Stelle erstellt ein Pseudonym und separiert dieses von den identifizierenden Merkmalen des Betroffenen. Da die datenverarbeitende Stelle selbst über die Zuordnungsregel verfügt, bietet eine derartige Pseudonymisierung nur Schutz gegenüber Dritten. Das Vorgehen ist in Erwägungsgrund 29 DSGVO als technische und organisatorische Sicherungsmaßnahme vorgesehen. Die Entscheidung über die Pseudonymisierungsmethode hängt vom jeweiligen Anwendungsfall ab. Im

Docusign Envelope ID: F1EE9337-0CED-43B2-8493-EBD8CF63A66C

Rahmen einer Auftragsverarbeitung erfolgt die Pseudonymisierung durch die verantwortliche Stelle, sodass dem Auftragsverarbeiter die Identifizierung der betroffenen Person ohne die Hilfe der verantwortlichen Stelle nicht möglich ist.

Im Rahmen der Auftragsverarbeitung für msg.CodIQ ist die verantwortliche Stelle für die Pseudonymisierung zuständig, sodass der msg systems ag als Auftragsverarbeiter die Identifizierung der betroffenen Person ohne die Hilfe der verantwortlichen Stelle nicht möglich ist.
Die verantwortliche Stelle erstellt ein Pseudonym und separiert dieses von den identifizierenden Merkmalen des Betroffenen. Das Vorgehen ist in Erwägungsgrund 29 DSGVO als technische und organisatorische Sicherungsmaßnahme vorgesehen.

Zusätzlich enthält CodIQ ein LLM basiertes Pseudonymisierungstool, welches identifizierende Merkmale wie Name, Vorname, Telefonnummer, Organisation, Adresse, Geburtsdatum, Email-Adresse, Reisepassnummer, Personalausweisnummer, Datum, Kreditkartennummer überwiegend pseudonymisieren soll. Dieses Tool stellt ein Zusatzangebot dar, um die Verarbeitung personenbezogener Daten zu reduzieren.

3.2 Integrität

3.2.1 Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist:

- Sicherung elektronischer Übertragung mittels verschlüsselter Verbindungen (VPN, TLS)
- Sicherung bei Übermittlung mittels sicherer Dateiaustauschplattform (Verfahrensbeschreibung, Protokollierung, Verschlüsselung)

Zusätzlich zu den hier genannten allgemeinen Maßnahmen für Systeme der msg systems ag wurden speziell für msg.CodIQ folgende Maßnahmen umgesetzt:

- Sicherung elektronischer Übertragung für alle externen und internen Schnittstellen mittels verschlüsselter Verbindungen (TLS)
- Daten in Datenbanken und Speichersystemen werden grundsätzlich verschlüsselt gespeichert. Die Erstellung unverschlüsselter Ressourcen wird technisch verhindert Eingesetzte Software wird vor Nutzung auf bekannte Sicherheitslücken überprüft. Kritische Schwachstellen führen zum Ausschluss vom Produktivbetrieb.

Diese Maßnahmen werden laufend erweitert.

3.2.2 Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind:

Docusign Envelope ID: F1EE9337-0CED-43B2-8493-EBD8CF63A66C

- Nur die im Zusammenhang mit Leistungen aus dem Vertrag tätigen Mitarbeitenden des Auftragnehmers sind zur Verarbeitung personenbezogener Daten des Auftraggebers berechtigt
- Benutzerauthentifizierung der zur Eingabe, Änderung oder Löschung autorisierter Personen
- Berechtigungssteuerung der Zugriffsart (lesender oder schreibender Zugriff)
- Protokollierung der Zugriffe

Zusätzlich zu den hier genannten allgemeinen Maßnahmen für Systeme der msg systems ag wurden speziell für msg.CodIQ folgende Maßnahmen umgesetzt:

- Zugriffe auf IT-Systeme und sicherheitsrelevante Aktionen werden protokolliert und regelmäßig durch Mitarbeiter ausgewertet. Die Protokolldaten werden zentral gespeichert, vor unbefugtem Zugriff geschützt und fristgerecht gelöscht.

3.3 Verfügbarkeit und Belastbarkeit

3.3.1 Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Backup- und Recovery-Konzept mit täglicher Sicherung und Aufbewahrung der gesicherten Daten in getrennten Brandabschnitten / Rechenzentren / Cloud Systemen. Eine Änderung von gesicherten Daten ist nur mit unabhängigen Accounts möglich (Ransomwareschutz).
- Verfahren zur Wiederherstellung von Daten aus Backup (z. B. Restore nur nach autorisiertem Auftrag)
- Einsatz einer zentralen Monitoring Lösung
- Einsatz einer zentralen SIEM-Lösung
- Einsatz von Schutzprogrammen (Virenscanner, Firewalls)
- Einsatz einer Vulnerability Management Plattform (Server)
- Einsatz von Festplattenspiegelung im Server- und Storagebereich (RAID)
- Einsatz unterbrechungsfreier Stromversorgung im Serverbereich (USV, NEA)
- Einsatz von Klimatisierung und Brandschutz (Brandfrüherkennung, Löschanlage)
- Zentraler DDOS-Schutz für Webzugriffe

Zusätzlich zu den hier genannten allgemeinen Maßnahmen für Systeme der msg systems ag wurden speziell für msg.CodIQ folgende Maßnahmen umgesetzt:

- Für personenbezogene Daten bestehen Backup- und Wiederherstellungsverfahren. Wiederherstellungstests werden regelmäßig durchgeführt Die Systeme sind skalierbar ausgelegt, um Lastspitzen abzufangen und die Verfügbarkeit sicherzustellen

Diese Maßnahmen werden laufend erweitert.

3.3.2 Belastbarkeit

Maßnahmen, die gewährleisten, dass personenbezogene Daten hinsichtlich Robustheit und Resilienz geschützt sind:

- Incident- / Business Continuity Management und Disaster Recovery Verfahren (BCM)
- Skalierbarkeit von Systemen in hybrider IT-Landschaft
- Kritische Systeme sind redundant aufgebaut

Docusign Envelope ID: F1EE9337-0CED-43B2-8493-EBD8CF63A66C

Zusätzlich zu den hier genannten allgemeinen Maßnahmen für Systeme der msg systems ag wurden speziell für msg.CodIQ folgende Maßnahmen umgesetzt:

- API-Aufrufe, Datei-Uploads und KI-Anfragen unterliegen technischen Nutzungs- und Mengenbegrenzungen.
- Maßnahmen zum Schutz vor Überlastungs- und DDoS-Angriffen sind implementiert.

Diese Maßnahmen werden laufend erweitert.

3.4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

3.4.1 Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden:

Der jeweilige Vertrag mit dem Auftraggeber enthält detaillierte Angaben über Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers und benennt die Weisungsbefugnisse

- Der Auftragnehmer hat einen betrieblichen Datenschutzbeauftragten bestellt und sorgt durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betrieblichen Prozesse
- Dokumentation der IT-Servicemanagement-Aktivitäten (Ticketsystem)

3.4.2 Datenschutz-Management

Ein Datenschutz-Management-System gewährleistet, dass die Rechenschaftspflicht zum Nachweis der Einhaltung der gesetzlichen Grundsätze und Regelungen, des Stands der Technik und der Aktualität und Wirksamkeit der Maßnahmen eingehalten wird. Die msg verfügt über ein Data Protection Management System (DPMS) nach Muster der ISO 27701 unter Berücksichtigung der ISMS-Controls. Folgende Maßnahmen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

- Datenschutzorganisation mit benanntem Beauftragten für den Datenschutz in der msg Gruppe, sowie benannte Datenschutzkoordinatoren in den Einheiten
- Richtlinien und Anweisungen zur Gewährleistung der Datenschutz Compliance
- Verpflichtung der Mitarbeitenden auf das Datengeheimnis
- Regelmäßige Schulungen der Mitarbeitenden zum Datenschutz
- Führen einer Übersicht über Verarbeitungstätigkeiten (Art. 30 DSGVO) als verantwortliche Stelle und Auftragsverarbeiter
- Zentral gesteuerter Prozess zur Wahrung der Betroffenenrechte
- Auditierung der Informationssicherheit nach ISO 27001
- Auditierung der Informationssicherheit des Public Sector / msg.CodIQ nach ISO 27001 geplant für 2026

3.4.3 Incident-Response-Management

Das Incident Response Management wird bei msg sowohl im Rahmen des ISMS wie auch im DPMS dokumentiert und gelebt. Technisch-organisatorische Maßnahmen und Prozesse gewährleisten, dass erkannte oder vermutete Sicherheitsvorfälle identifiziert und systematisch beseitigt werden. Im Rahmen des DPMS stellt ein Prozess sicher, dass im Fall von Datenschutzverstößen ein Meldeprozess ausgelöst wird.

Docusign Envelope ID: F1EE9337-0CED-43B2-8493-EBD8CF63A66C

- Zentral gesteuerter Prozess Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Aufsichtsbehörden (Art. 33 DSGVO)
- Zentral gesteuerter Prozess Meldeprozess für Datenschutzverletzungen nach Art. 4 Ziffer 12 DSGVO gegenüber den Betroffenen (Art. 34 DSGVO)
- Zentral gesteuerter Prozess Meldeprozess für Datenschutzverletzungen nach Art. 28 DSGVO gegenüber der verantwortlichen Stelle im Rahmen einer Auftragsverarbeitung

Sicherheitsereignisse aus Cloud-Diensten werden in das Incident-Response-Verfahren integriert.

3.4.4 Datenschutzfreundliche Voreinstellungen

Art und Umfang des Personenbezugs sowie Pseudonymisierung werden im Rahmen der Projektinitialisierung berücksichtigt.

Bei der Nutzung des Produktes CodIQ obliegt dem Kunden darauf zu achten, dass Ihre Mitarbeitenden über den ordnungsgemäßen Einsatz informiert werden und die Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erfolgt.

Die Nutzereingaben und Dateiuploads, die während der Nutzung von CodIQ erfolgen, werden unmittelbar nach der Websession gelöscht und nicht gespeichert. Nutzerkonten werden spätestens 365 Tage nach dem letzten aktiven Log-in gelöscht.

Es werden keine Daten zu Trainingszwecken der KI genutzt.

© msg systems ag 2026 - öffentlich

Docusign Envelope ID: F1EE9337-0CED-43B2-8493-EBD8CF63A66C

4 Technisch-organisatorische Maßnahmen Mobiles Arbeiten

Bei der Datenverarbeitung im Mobilen Arbeiten besteht ein erhöhtes Risiko, dass Dritte einen unbefugten Zugang zu personenbezogenen Daten erhalten. Der msg systems ag ist dieses erhöhte Risiko bewusst. Aus diesem Grund ist die Einhaltung und Umsetzung der nachfolgenden, risikominimierenden Maßnahmen - als Ergänzung zu den technisch-organisatorischen Maßnahmen der msg systems ag – verpflichtend.

Auch beim Mobilen Arbeiten gelten die Vorgaben aus den CIT Policies.

4.1 Vertraulichkeit

4.1.1 Zutrittskontrolle

Es sind geeignete Maßnahmen zu treffen, die Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehren:

- Der Arbeitsplatz ist in einem eigenen Raum oder in einem hinreichend separierten Bereich eingerichtet.
- Es ist sichergestellt, dass keine externe Einsichtnahme in den Bildschirm möglich ist.
- Es ist sichergestellt, dass die Geräte und Speichermedien auch in Abwesenheiten nicht für andere unberechtigte Personen zugänglich sind.

4.1.2 Zugangskontrolle

Es sind geeignete Maßnahmen zu treffen, die verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Der sichere Umgang mit Passwörtern sowie die strikte Einhaltung der Passwortregelungen aus der Security-Policy für CIT-Devices ist sichergestellt.
- Eine sichere LAN/WLAN Verbindung sowie Passwörter analog den CIT-Anforderungen sind verpflichtend.
- Die Einhaltung der Clean Desk Policy, v.a. in Hinblick auf die Anforderungen zu Bildschirmsperre, Blickschutzfilter und Datenträgerverschlüsselung sind gewährleistet.
- Die Zwei-Faktor-Authentifizierung ist obligatorisch.

4.1.3 Zugriffskontrolle

Es sind geeignete Maßnahmen zu treffen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert verändert oder entfernt werden können:

- Bei Transport und Nutzung von Papierdokumenten und sonstigen personenbezogenen Daten ist ein unbefugter Zugriff ausgeschlossen (Zugriffschutz).
- Der sichere Verschluss und die sichere Entsorgung von Papierdokumenten und sonstigen personenbezogenen Daten ist entsprechend den msg Anforderungen (Clean Desk Policy) gewährleistet.

Docusign Envelope ID: F1EE9337-0CED-43B2-8493-EBD8CF63A66C

4.1.4 Trennungsgebot

Es sind geeignete Maßnahmen zu treffen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden:

- Alle Dokumente werden auf dienstlichen Systemen im Netz der msg oder auf dienstlich bereitgestellten Cloud Systemen gespeichert.
- Eine Speicherung personenbezogener dienstlicher/geschäftlicher Daten auf privaten Devices oder Geräten oder in privaten Cloud- Speichern ist untersagt.
- Alle Sprachassistenten, die nicht von der msg freigegeben sind, sind deaktiviert.

4.1.5 Pseudonymisierung

Bei der Pseudonymisierung handelt es sich um eine zentrale technische und organisatorische Sicherungsmaßnahme, welche die DSGVO nicht nur in Art. 32 Abs. 1a), sondern wiederholt in unterschiedlichen Zusammenhängen erwähnt. Sie kann Einfluss auf die Zulässigkeit einer Verarbeitung personenbezogener Daten haben und erhöht den Schutz der Rechte und Freiheiten der Betroffenen. Der Erwägungsgrund 26 DSGVO stellt hierbei eindeutig heraus, dass auch pseudonymisierte Daten weiterhin personenbezogene Daten bleiben. Grundsätzlich stehen drei Pseudonymisierungsmethoden zur Verfügung:

• Der Betroffene vergibt selbst ein Pseudonym und separiert dieses von den Daten, die ihn identifizieren.
• Ein unabhängiger Dritter, der über die entsprechende Zuordnungsregel verfügt, vergibt ein Pseudonym für den Betroffenen.
• Die verantwortliche Stelle erstellt ein Pseudonym und separiert dieses von den identifizierenden Merkmalen des Betroffenen. Da die datenverarbeitende Stelle selbst über die Zuordnungsregel verfügt, bietet eine derartige Pseudonymisierung nur Schutz gegenüber Dritten. Das Vorgehen ist in Erwägungsgrund 29 DSGVO als technische und organisatorische Sicherungsmaßnahme vorgesehen. Die Entscheidung über die Pseudonymisierungsmethode hängt vom jeweiligen Anwendungsfall ab. Im Rahmen einer Auftragsverarbeitung erfolgt die Pseudonymisierung durch die verantwortliche Stelle, sodass dem Auftragsverarbeiter die Identifizierung der betroffenen Person ohne die Hilfe der verantwortlichen Stelle nicht möglich ist.

4.2 Integrität

4.2.1 Weitergabekontrolle

Es sind geeignete Maßnahmen zu treffen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung, während ihres Transports oder ihrer Speicherung, nur von Berechtigten genutzt werden. Insbesondere können die Daten nicht unbefugt gelesen, kopiert, verändert oder entfernt werden. Es kann überprüft werden, an welchen Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen sind:

- Die Verarbeitung personenbezogener Daten mittels elektronischer Übertragung ist mittels verschlüsselter Verbindungen (VPN, TLS) gesichert.

© msg systems ag 2026 - öffentlich

Docusign Envelope ID: F1EE9337-0CED-43B2-8493-EBD8CF63A66C

- Alle Dokumente im Mobilen Arbeiten werden nach ihrer Schutzklasse DIN 66399 für vertrauliche und streng vertrauliche Daten vernichtet. Die Regelungen sind in der Policy zur Dokumenten- und Informationsklassifizierung festgelegt.
- Der Austausch von Unternehmensinformationen in nicht freigegebenen Messenger-Plattformen (z.B. WhatsApp) ist verboten.

4.2.2 Eingabekontrolle

Siehe Kapitel 3.2.2

4.2.3 Verfügbarkeitskontrolle

Es sind geeignete Maßnahmen zu treffen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind:

- Die Speicherung von Daten erfolgt nur auf Systemen, die vom Arbeitgeber bereitgestellt sind.

4.2.4 Belastbarkeit

Siehe Kapitel 3.3.2

4.3 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

4.3.1 Auftragskontrolle

Es sind geeignete Maßnahmen zu treffen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden:

- Die Datenverarbeitung im Mobilen Arbeiten wird in den Verträgen mit Kunden und Dienstleistern berücksichtigt.

4.3.2 Datenschutz-Management

Ein Datenschutz-Management-System gewährleistet, dass die Rechenschaftspflicht zum Nachweis der Einhaltung der gesetzlichen Grundsätze und Regelungen, des Stands der Technik und der Aktualität und Wirksamkeit der Maßnahmen eingehalten wird. Die msg verfügt über ein Data Protection Management System (DPMS) nach Muster der ISO 27701 unter Berücksichtigung der ISMS-Controls. Folgende Maßnahmen gewährleisten, dass eine den datenschutzrechtlichen Grundanforderungen genügende Organisation vorhanden ist:

- Der Besuch der regelmäßigen Datenschutzschulung der msg systems ag ist verpflichtend.

4.3.3 Incident-Response-Management

Das Incident Response Management wird bei msg sowohl im Rahmen des ISMS wie auch im DPMS dokumentiert und gelebt. Technisch-organisatorische Maßnahmen und Prozesse gewährleisten, dass erkannte oder vermutete Sicherheitsvorfälle erfasst und systematisch beseitigt werden. Im Rahmen des DPMS stellt ein Prozess sicher, dass im Fall von Datenschutzverstößen ein Meldeprozess ausgelöst wird:

- Für den Fall eines Datenverlusts (z. B. Verlust von Papierunterlagen oder Datenträgern) oder eines Datenschutzverstoßes (z. B. Zugang von Unbefugten an den Computer) oder eine sonstige Verletzung des Schutzes personenbezogener Daten besteht eine Meldepflicht gegenüber dem

Docusign Envelope ID: F1EE9337-0CED-43B2-8493-EBD8CF63A66C

Datenschutzbeauftragten. Im weiteren Prozess erfolgt eine Meldung gegenüber der Datenschutzaufsichtsbehörde durch den Datenschutzbeauftragten.

- Bei Verdachtsfällen besteht das Recht auf eine Auditierung durch den Datenschutzbeauftragten oder eine von ihm autorisierte unabhängige Stelle.

4.3.4 Datenschutzfreundliche Voreinstellungen

Durch geeignete technisch-organisatorische Maßnahmen wird sichergestellt, dass in Bezug auf die Menge, den Umfang, die Speicherfrist und den Zugriff durch Voreinstellungen die Verarbeitung nur für den jeweiligen bestimmten Verarbeitungszweck erfolgt.

Die Default-Einstellungen werden sowohl bei den standardisierten Voreinstellungen von Systemen und Applikationen als auch bei der Einrichtung der Datenverarbeitungsverfahren von Seiten msg berücksichtigt (Privacy by Default, Art. 25 Abs. 2 DSGVO).

Im Rahmen von Privacy by Design (Art. 25 Abs. 1 DSGVO) werden Funktionen und Rechte konzeptioniert sowie im Hinblick auf Datenminimierung die Zulässigkeit bestimmter Eingaben und Eingabemöglichkeiten (z. B. von Freitexten) festgelegt sowie über die Verfügbarkeit von datenschutzrelevanten Nutzungsfunktionen entschieden (z. B. Reporting).

Art und Umfang des Personenbezugs sowie angemessene Pseudonymisierung und Anonymisierung werden im Rahmen der Projektinitialisierung berücksichtigt.

Docusign Envelope ID: F1EE9337-0CED-43B2-8493-EBD8CF63A66C

5 Dokumentübersicht

5.1 Allgemeine Bestimmungen und Copyright

© msg systems ag, 2026

5.2 Versionshistorie

Version	Beschreibung	Autor	Datum
1.0	Erstellung msg.CodIQ spezifischer TOMs auf Basis der msg TOMs (Version 9.0)	Michael Gürster Lisa Buhlmann Dirk Goldhammer	Januar 2026