



audatis MANAGER Kundenin- formation zur Dienstleisterprü- fung

Standardisierte Informationen zu Datenschutz, Informationssicherheit,
IKT-Drittparteienrisiken und Business Continuity

Inhalt

1	Schnellübersicht	4
2	Zweck, Geltungsbereich und Verwendung	4
3	Anbieterprofil	5
4	Beschreibung der IKT-Dienstleistung	5
5	Regulatorische Einordnung und DORA	6
6	Leistungsqualität, Verfügbarkeit und Support	6
7	Hosting, Leistungserbringung und Datenstandorte	6
8	Informationssicherheitsmanagement	7
9	Zugriffsschutz, Berechtigungen und Verschlüsselung	7
10	Schwachstellenmanagement und Penetrationstests	7
11	Backup, Wiederherstellung und Business Continuity	8
12	Datenexport, Vertragsende und Löschung	8
13	Incident Management und Kundenkommunikation	8
14	Datenschutz und Auftragsverarbeitung	8
15	Governance, Compliance und Integrität	9
16	Umfang standardisierter Nachweise und Vertraulichkeit	9
17	Referenzdokumente und Bereitstellung	9
18	Dokumentenpflege	10

Klassifizierung	<i>öffentliche Information für Kunden</i>
Dokumentenzweck	<i>Diese Kundeninformation bündelt wiederkehrende Angaben für die Lieferanten- und Dienstleisterprüfung der audatis Services GmbH, Luisenstr. 1, 32052 Herford und des audatis MANAGER. Sie dient als standardisierte Informationsquelle und verweist für veränderliche Leistungsparameter und Nachweise auf die jeweils maßgeblichen Primärdokumente.</i>
Stand	11.09.2026

1 Schnellübersicht

Prüffeld	Primärquelle / Nachweis	Bereitstellung
Leistungsumfang, Verfügbarkeit, Support, Wartung, Backup, Export	Leistungsbeschreibung / SLA audatis MANAGER	Download in den Vertragsdaten im audatis MANAGER möglich
Datenschutz und Auftragsverarbeitung	AVV einschließlich TOM und Unterauftragnehmer	Online im audatis MANAGER abschließbar und einsehbar
Informationssicherheitsmanagement	ISO/IEC 27001:2022 Zertifikat und Zertifikatsanlage	Trust Center
Hostingstandort	BITMi „Software Hosted in Germany“	Trust Center
Penetrationstest	Geeignetes Testat / Zertifikat zum audatis MANAGER	Trust Center / jeweils verfügbarer Nachweis
Compliance und Integrität	Code of Conduct der audatis Group	Trust Center
DORA-Vertragsanforderungen	Separate DORA-Zusatzvereinbarung, soweit einschlägig	Vertraglich / auf Anfrage
Kundenspezifische Zusatzfragen	Nur soweit durch Standardunterlagen nicht bereits beantwortet	Einzelfallprüfung

2 Zweck, Geltungsbereich und Verwendung

Die audatis Services GmbH stellt diese Kundeninformation zur einheitlichen, aktuellen und qualitätsgesicherten Beantwortung typischer Fragen im Rahmen von Lieferanten-, IKT-Dienstleister- und Third-Party-Due-Diligence-Prüfungen bereit. Die Angaben beziehen sich auf die standardmäßige Bereitstellung des audatis MANAGER als Software-as-a-Service-Lösung und auf die hierfür bestehenden organisatorischen und technischen Rahmenbedingungen.

Diese Kundeninformation ersetzt weder den Hauptvertrag noch die jeweils aktuelle Leistungsbeschreibung / SLA, den AVV oder sonstige individuell vereinbarte

Vertragsbestandteile. Für konkrete Leistungsparameter, datenschutzrechtliche Verpflichtungen und Nachweise sind die jeweils bezeichneten Primärdokumente maßgeblich.

Hinweis für kundeneigene Fragebögen: Soweit eine Frage bereits durch diese Kundeninformation oder die darin bezeichneten Primärdokumente und Nachweise beantwortet wird, verweist audatis grundsätzlich auf die jeweilige Standardinformation. Ergänzende kundenspezifische Angaben werden geprüft, wenn sie für die konkrete Dienstleisterbewertung erforderlich und nicht bereits durch vorhandene Unterlagen abgedeckt sind.

3 Anbieterprofil

Merkmal	Angabe
Anbieter	audatis Services GmbH
Sitz	Luisenstr. 1, 32052 Herford, Deutschland
Leistung	Bereitstellung und Betrieb des audatis MANAGER als SaaS-Lösung
Datenschutzkontakt	datenschutz@audatis.de
Supportkontakt	support@audatis-manager.de
Unternehmensgruppe	audatis Group

4 Beschreibung der IKT-Dienstleistung

Der audatis MANAGER ist eine webbasierte SaaS-Lösung zur Unterstützung und Dokumentation von Datenschutz-, Compliance- und Informationssicherheitsprozessen. Der konkrete Funktionsumfang richtet sich nach der gebuchten Version und der jeweils aktuellen Leistungsbeschreibung / SLA.

- Datenschutzmanagement mit Dokumentations-, Aufgaben-, Maßnahmen- und Nachweisfunktionen
- Verwaltung und Dokumentation von Auftragsverarbeitungen, Verzeichnissen von Verarbeitungstätigkeiten und technischen und organisatorischen Maßnahmen
- Optionale Nutzung des audatis PORTAL für E-Learnings und Mitarbeiternachweise
- Optionales Hinweisgebersystem zur vertraulichen Entgegennahme und Bearbeitung von Hinweisen

- Optionale Erweiterung „Compliance + ISMS“ zur Dokumentation von Compliance-Anforderungen, ISMS, Risikomanagement und KI-Compliance
- Weitere optionale Funktionen entsprechend der jeweils aktuellen Leistungsbeschreibung / SLA

Welche Module und Zusatzfunktionen tatsächlich Vertragsgegenstand sind, ergibt sich aus dem jeweiligen Hauptvertrag und der jeweils aktuellen Leistungsbeschreibung / SLA.

5 Regulatorische Einordnung und DORA

Soweit ein Kunde dem Anwendungsbereich der Verordnung (EU) 2022/2554 (Digital Operational Resilience Act – DORA) unterliegt und den audatis MANAGER als IKT-Dienstleistung bezieht, unterstützt audatis die kundenseitige Dienstleisterprüfung durch standardisierte Informationen und – soweit einschlägig – durch eine gesonderte DORA-Zusatzvereinbarung.

Die Bewertung, ob die konkrete Nutzung des audatis MANAGER eine kritische oder wichtige Funktion oder wesentliche Teile davon unterstützt, ist durch das jeweilige Finanzunternehmen anhand des tatsächlichen Nutzungskontexts und seiner eigenen Risiko- und Kritikalitätsbewertung vorzunehmen. audatis nimmt diese kundenspezifische Einordnung nicht pauschal vor.

6 Leistungsqualität, Verfügbarkeit und Support

Die jeweils aktuelle Leistungsbeschreibung – Service Level Agreements (SLA) ist die Primärquelle für den Funktionsumfang sowie für Verfügbarkeits-, Wartungs-, Support-, Backup- und Exportregelungen des audatis MANAGER. Ein Download der jeweils aktuellen Fassung ist in den jeweiligen Kundenvertragsdaten im audatis MANAGER möglich.

Abweichende oder weitergehende Service-Level gelten nur, soweit sie ausdrücklich vertraglich vereinbart wurden. Diese Kundeninformation wiederholt bewusst keine veränderlichen Leistungsparameter aus der SLA.

7 Hosting, Leistungserbringung und Datenstandorte

Für den audatis MANAGER liegt das BITMi-Gütesiegel „Software Hosted in Germany“ vor. Das Gütesiegel dient als Nachweis für das Hosting des zertifizierten Produkts in Deutschland. Ergänzende datenschutzrechtliche Vorgaben zur Verarbeitung personenbezogener Daten ergeben sich aus dem jeweils abgeschlossenen AVV.

Die jeweils aktuellen Unterauftragnehmer und die hierfür maßgeblichen datenschutzrechtlichen Regelungen ergeben sich aus dem im audatis MANAGER abgeschlossenen AVV. Soweit regulierte Kunden zusätzliche Standortangaben für ihre IKT-Drittparteien-Dokumentation benötigen, werden diese innerhalb der separaten DORA-Zusatzvereinbarung, soweit einschlägig, bereitgestellt.

8 Informationssicherheitsmanagement

Die audatis Group betreibt ein nach ISO/IEC 27001:2022 zertifiziertes Informationssicherheitsmanagementsystem. Der Zertifizierungsumfang umfasst unter anderem Entwicklung, Betrieb und Support der eigenen Softwarelösung sowie Cybersecurity-Assessments und Penetrationstests. Die Zertifikatsanlage weist die audatis Services GmbH am Standort Herford als vom Geltungsbereich erfassten Standort aus.

- ISO/IEC 27001:2022 Zertifizierung durch TÜV Rheinland Cert GmbH
- Informationssicherheitsmanagement mit internen Kontroll- und Auditmechanismen
- Incident-Response-Prozesse zur Behandlung von Sicherheitsvorfällen
- Regelmäßige Schulungs- und Sensibilisierungsmaßnahmen
- Schwachstellenanalysen und Penetrationstests

Das ISO-Zertifikat und die zugehörige Zertifikatsanlage werden im Trust Center als Nachweise bereitgestellt. Einzelheiten zu technischen und organisatorischen Maßnahmen im Rahmen der Auftragsverarbeitung ergeben sich aus dem AVV einschließlich TOM.

9 Zugriffsschutz, Berechtigungen und Verschlüsselung

Für den audatis MANAGER bestehen technische und organisatorische Maßnahmen zum Schutz von Vertraulichkeit, Integrität und Verfügbarkeit. Dazu gehören insbesondere rollenbasierte Berechtigungsmechanismen, Schutz privilegierter Zugänge, verschlüsselte Übertragung und – abhängig von der jeweiligen Funktion – zusätzliche Schutzmechanismen für gespeicherte Inhalte.

Die jeweils aktuellen und maßgeblichen Detailangaben zu Authentifizierung, Berechtigungsmanagement, Verschlüsselung, Mandantentrennung und weiteren technischen und organisatorischen Maßnahmen ergeben sich aus dem AVV einschließlich TOM sowie, soweit leistungsbezogen, aus der jeweils aktuellen SLA. Diese Kundeninformation wiederholt diese veränderlichen Einzelmaßnahmen bewusst nicht vollständig.

10 Schwachstellenmanagement und Penetrationstests

Für den audatis MANAGER werden Schwachstellenanalysen und Penetrationstests im Rahmen des Informationssicherheitsmanagements durchgeführt. Geeignete Testate oder Zertifikate werden im Trust Center bereitgestellt, soweit ein aktueller Nachweis verfügbar ist.

Detaillierte technische Prüfberichte sind aus Gründen der Informationssicherheit nicht Bestandteil der standardmäßigen Kundenunterlagen. Bei regulatorisch begründeten Anforderungen an weitergehende Nachweise erfolgt eine Einzelfallprüfung unter Berücksichtigung von Vertraulichkeit und Sicherheitsinteressen.

11 Backup, Wiederherstellung und Business Continuity

Für den audatis MANAGER bestehen Maßnahmen zur Datensicherung, Wiederherstellung und Notfallvorsorge. Die jeweils geltenden Backup-, Wiederherstellungs- und Verfügbarkeitsregelungen ergeben sich aus der aktuellen Leistungsbeschreibung / SLA. Ergänzende technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten ergeben sich aus dem AVV einschließlich TOM.

Verbindliche RTO- oder RPO-Werte gelten nur, soweit diese ausdrücklich vertraglich vereinbart wurden. Konkrete Backup-Intervalle, Vorhaltezeiten und sonstige veränderliche Betriebsparameter werden in dieser Kundeninformation bewusst nicht wiederholt.

12 Datenexport, Vertragsende und Löschung

Die für den audatis MANAGER verfügbaren Export- und Sicherungsmöglichkeiten ergeben sich aus der jeweils aktuellen Leistungsbeschreibung / SLA. Nach Beendigung des Vertragsverhältnisses richten sich Rückgabe, Sicherung und Löschung von Kundendaten nach den jeweils anwendbaren vertraglichen Regelungen, insbesondere SLA und – soweit personenbezogene Daten betroffen sind – AVV.

Diese Kundeninformation begründet keine eigenständigen zusätzlichen Aufbewahrungs-, Export- oder Löschfristen.

13 Incident Management und Kundenkommunikation

audatis unterhält Prozesse zur Behandlung von Sicherheits- und Datenschutzvorfällen. Datenschutzrechtliche Informations- und Unterstützungspflichten ergeben sich aus dem AVV. Die für technische Störungen maßgeblichen Supportkanäle und Reaktionszeiten ergeben sich aus der jeweils aktuellen SLA.

Soweit für regulierte Kunden zusätzliche DORA-bezogene Melde- und Unterstützungsregelungen erforderlich sind, werden diese in der jeweiligen DORA-Zusatzvereinbarung geregelt.

14 Datenschutz und Auftragsverarbeitung

Für Verarbeitungstätigkeiten im Auftrag wird ein AVV gemäß Art. 28 DS-GVO bereitgestellt. Der AVV kann im audatis MANAGER elektronisch abgeschlossen und dort eingesehen werden. Er enthält insbesondere Regelungen zu Gegenstand und Dauer der Verarbeitung, Datenarten und Kategorien betroffener Personen, technischen und organisatorischen Maßnahmen, Kontrollrechten, Unterauftragnehmern sowie Unterstützungspflichten.

- Betrieblicher Datenschutzbeauftragter; Kontakt: datenschutz@audatis.de
- Technische und organisatorische Maßnahmen als Bestandteil des AVV

- Verzeichnis der Auftragsverarbeitung und Beschreibung der verarbeiteten Daten im AVV
- Regelungen zu Unterauftragnehmern einschließlich Änderungs- und Kontrollmechanismen
- Regelungen zur Unterstützung bei Datenschutzverletzungen und Betroffenenrechten

15 Governance, Compliance und Integrität

Der Code of Conduct der audatis Group dokumentiert die gruppenweiten Grundsätze für rechtmäßiges und integrires Verhalten. Er enthält insbesondere Regelungen zu Rechtskonformität, Arbeitsbedingungen und sozialer Verantwortung, Gleichbehandlung, Umwelt und Nachhaltigkeit, Datenschutz und Schutz von Geschäftsgeheimnissen, fairem Wettbewerb, Interessenkonflikten sowie Korruptions- und Bestechungsprävention.

Der Code of Conduct ist als öffentliche Information klassifiziert und wird im Trust Center bereitgestellt.

16 Umfang standardisierter Nachweise und Vertraulichkeit

Zur Gewährleistung konsistenter und qualitätsgesicherter Informationen stellt audatis vorrangig standardisierte Nachweise zur Verfügung. Nicht öffentliche interne Unterlagen werden grundsätzlich nicht standardmäßig an Kunden herausgegeben.. Hierzu zählen insbesondere detaillierte technische Sicherheitsberichte, interne Konfigurationen, vollständige Penetrationstestberichte, interne Unternehmensplanungen und sonstige vertrauliche Geschäftsunterlagen.

Besteht für einen Kunden aufgrund konkreter gesetzlicher, aufsichtsrechtlicher oder vertraglicher Anforderungen ein darüber hinausgehender Informationsbedarf, prüft audatis Art, Umfang und geeignete Form des Nachweises im Einzelfall. Dabei werden das berechnete Prüferinteresse des Kunden sowie Informationssicherheits-, Vertraulichkeits- und Geschäftsgeheimnisinteressen berücksichtigt.

17 Referenzdokumente und Bereitstellung

Dokument / Nachweis	Zweck	Bereitstellung
Leistungsbeschreibung – Service Level Agreements (SLA) audatis MANAGER	Funktionsumfang, Verfügbarkeit, Support, Wartung, Backup, Export	Download in den Vertragsdaten im audatis MANAGER möglich

Dokument / Nachweis	Zweck	Bereitstellung
AVV audatis MANAGER	Auftragsverarbeitung, TOM, Unterauftragnehmer, Datenschutzrechte	Online im audatis MANAGER abschließbar und einsehbar
ISO/IEC 27001:2022 Zertifikat	Nachweis Informationssicherheitsmanagement	Trust Center
Anlage zum ISO/IEC 27001 Zertifikat	Nachweis Geltungsbereich / Standorte einschließlich audatis Services GmbH	Trust Center
BITMi „Software Hosted in Germany“	Nachweis Hosting des audatis MANAGER in Deutschland	Trust Center
Penetrationstest-Testat audatis MANAGER	Nachweis durchgeführter Penetrationstest	Trust Center / jeweils verfügbarer Nachweis
Code of Conduct audatis Group	Governance-, Compliance- und Integritätsgrundsätze	Trust Center
DORA-Zusatzvereinbarung	Vertragliche DORA-Mindestanforderungen, soweit einschlägig	Separat / auf Anfrage

18 Dokumentenpflege

Diese Kundeninformation wird bei wesentlichen Änderungen ihrer eigenen Aussagen oder der zugrunde liegenden Dokumentenarchitektur überprüft und bei Bedarf aktualisiert. Veränderungen einzelner Leistungsparameter, technischer Maßnahmen oder Nachweise werden grundsätzlich in den hierfür vorgesehenen Primärdokumenten gepflegt und erfordern nicht automatisch eine Aktualisierung dieser Kundeninformation.