audatis Cert Auditstandard GAV-S: GEPRÜFTER AUFTRAGSVERARBEITER

Auditstandard GAV-S

Dieser Auditstandard bezieht sich auf die Überprüfung eines Auftragsverarbeiters und hat folgenden Geltungsbereich:

„Verarbeitung personenbezogener Daten im Rahmen von Betrieb, Entwicklung und Wartung von Software durch einen Auftragsverarbeiter“.

Im Rahmen des Audits werden die angemessene Umsetzung der vom Auftragsverarbeiter getroffenen und zur Überprüfung eingereichten technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung gem. Art. 32 DS-GVO sowie allgemeine Anforderungen zum Datenschutz als Auftragsverarbeiter gem. Art. 28 DS-GVO überprüft. In diesem Zusammenhang muss auch die Umsetzung der Mindeststandanforderungen an ein Informationssicherheitsmanagementsystem nachgewiesen werden.

Ziel des Standards ist es, den Auftraggebern des „geprüften Auftragsverarbeiters“ eine verlässliche Einschätzung über die Umsetzung des Datenschutzes und der angemessenen technischen und organisatorischen Maßnahmen zu ermöglichen.

Gültigkeit und Testat

Bei der Anwendung des Standards werden die Abweichungen von MUSS-Kriterien (siehe Teil A-C) in Form von Hauptabweichungen (Umsetzung nicht angemessen bzw. nicht nachweisbar), Nebenabweichungen (Umsetzung nur in Teilen nicht angemessen bzw. nicht vollständig dokumentiert) oder Verbesserungspotentialen klassifiziert.

Werden im Rahmen der Überprüfung keine Hauptabweichungen festgestellt wird das Testat: „geprüfter Auftragsverarbeiter“ erteilt, welches eine Gültigkeit von max. 2 Jahren hat. Werden wesentliche technische oder organisatorische Maßnahmen, auf welche sich das Testat bezieht, signifikant verändert, erlischt das Testat vorzeitig bzw. kann durch ein Überwachungsaudit verlängert werden.

Werden mehrere Nebenabweichungen festgestellt, welche in Summe zu einem erheblichen Risiko für die Verarbeitung personenbezogener Daten führen können, muss ein Maßnahmenplan vorgelegt werden, welcher die Abstellung der Nebenabweichungen innerhalb der nächsten 3 Monate beinhaltet. In diesem Fall kann ein „vorläufiges Testat“ erteilt werden. Nach spätestens 6 Monaten erfolgt in diesem Fall ein Überwachungsaudit, welches mindestens alle Bereiche mit Nebenabweichungen umfasst. Werden hierbei neue Hauptabweichungen festgestellt oder die Nebenabweichungen mit erheblichem Risiko nicht gem. des vorgelegten Maßnahmenplans abgestellt, endet die Gültigkeit des Testats. Andernfalls erfolgt die Erteilung des Testat „geprüfter Auftragsverarbeiter“ für den verbleibenden Zeitraum.

Die Ergebnisse der Überprüfung werden dem „geprüften Auftragsverarbeiter“ als Prüfbericht zur Verfügung gestellt.

Das Testat mit entsprechendem Gültigkeitsvermerk kann auf Wunsch des Auftragsverarbeiters in der audatis Cert Datenbank unter www.audatis-cert.de veröffentlicht werden. Dies kann von potentiellen Autraggebern des Auftragsverarbeiters als Instrument zur Risikominimierung bei der Auswahl von Dienstleistern dienen. Das mit dem Testat ebefalls verliehene Gütesiegel darf vom geprüften Auftragsverarbeiter für werbliche Zwecke verwendet werden.

Unabhängige Auditoren

Die Überprüfungen werden durch unabhängige Auditoren durchgeführt, welche von der audatis Cert GmbH basierend auf der notwendigen und nachweislichen Fachkunde berufen werden.

Umfang der Überprüfung

Der Auditstandard basiert auf 3 Teilen, welche im folgenden mit den MUSS-Kriterien beschrieben werden: Teil A mit allgemeinen Anforderungen an Auftragsverarbeiter, Teil B mit allgemeinen Anforderungen an die Informationssicherheit und Teil C mit den spezifischen Anforderungen an Auftragsvereareiter bei Betrieb, Entwicklung und Wartung von Software.

Der Teil B kann durch adäquate Nachweise mit gleichem Mindestinhalt und -umfang auf Basis anerkannter internationaler oder nationaler Standards komplett oder teilweise ersetzt werden. Zugelassen sind derzeit gültige Zertifikate nach folgenden Standards:

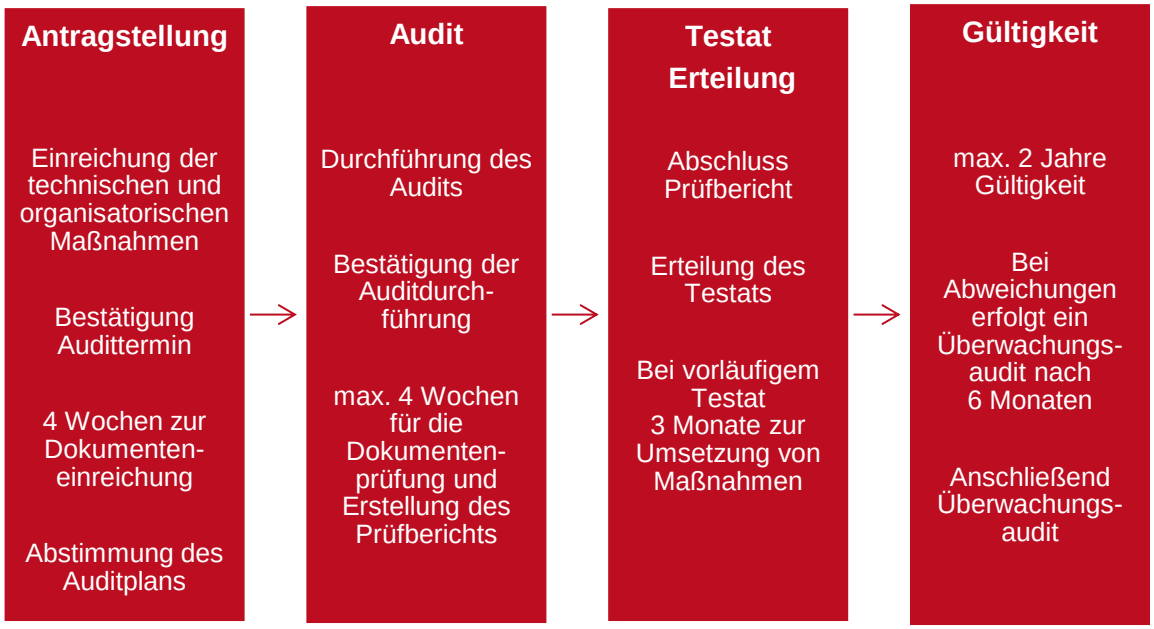
- ISO/IEC 27001:2013 oder höher
- BSI IT-Grundschutz
- VdS 10000

#	Teil A – Allgemeine Anforderungen an den Auftragsverarbeiter
1.0	Regelungen zum Datenschutz und dem Umgang mit personenbezogenen Daten im Unternehmen wurden nachweislich getroffen und sind den Mitarbeitenden bekannt.
1.1	Es sind Regelungen zum Umgang mit Datenschutzvorfällen gem. Art. 33 DS-GVO und anderen Sicherheitsvorfällen getroffen und den Mitarbeitenden bekannt.
1.2	Es sind Regelungen zum Umgang mit den Rechten betroffener Personen gem. Art. 12-21 DS-GVO getroffen und den Mitarbeitenden bekannt.
1.3	Es sind Regelungen zum Umgang mit Mitarbeitenden in Bezug auf den Unternehmenseintritt und -austritt sowie Verpflichtungen zum Datenschutz getroffen und umgesetzt.
1.4	Es sind angemessene Regelungen in Bezug auf den Einsatz von privaten Endgeräten sowie den privaten Gebrauch dienstlicher Endgeräte getroffen und umgesetzt.
2	Sofern notwendig wurde ein fachkundiger Datenschutzbeauftragter gem. Art. 37 ff. DS-GVO benannt.
3	Alle an der Datenverarbeitung beteiligten Mitarbeitenden werden direkt nach dem Eintritt ins Unternehmen und sodann min. jährlich zum Datenschutz und den unternehmensbezogenen Risiken der Informationssicherheit geschult.
4	Eine Dokumentation der von der Auftragsverarbeitung betroffenen Verarbeitungstätigkeiten ist gem. Art. 30 Abs. 1 DS-GVO vorhanden und enthält die relevanten Rechtsgrundlagen.
5.1	Eine Übersicht aller Auftraggeber und Auftragnehmer gem. Art. 30 Abs. 2 DS-GVO liegt vor.
5.2	Bei der Einbindung von weiteren (Sub-) Auftragsverarbeitern liegen entsprechende Vereinbarungen gem. Art. 28 DS-GVO vor. Werden (Sub-) Auftragsverarbeiter außerhalb des EWR eingesetzt, werden entsprechende Garantien gem. Art. 46 DS-GVO gewährleistet.
5.3	Es wurde ein Prozess etabliert, welcher zumindest die Überprüfung der (Sub-) Auftragsverarbeiter in Bezug auf technische und organisatorische Maßnahmen zu Beginn und sodann regelmäßig gewährleistet.
5.4	Es ist ein Prozess etabliert, welcher das Löschen von Daten des Auftraggebers nach Beendigung des Vertrags (inkl. digitaler Archive) oder auf Weisung hin ermöglicht.

#	Teil B – Anforderungen zur Gewährleistung der Sicherheit der Verarbeitung
6	Es werden angemessene und nachweisliche Maßnahmen zum Benutzermanagement umgesetzt, um die Vertraulichkeit und Integrität zu gewährleisten.
7	Es werden angemessene Maßnahmen zum Umgang mit Endgeräten und IT-Systemen ergriffen, welche Server, Laptops, Desktops, Tablets und Smartphones einschließen.
8	Es liegen angemessene Backupstrategien und Datensicherungspläne vor und werden umgesetzt, um die Verfügbarkeit zu gewährleisten.
9	Es werden angemessene Maßnahmen zur Netzwerksicherheit umgesetzt, welche die Vertraulichkeit, Verfügbarkeit und Integrität gewährleisten.
10	Es werden angemessene Maßnahmen zur physischen Sicherheit (Schutz von Gebäuden und Räumen) getroffen, um die Vertraulichkeit zu gewährleisten.
11	Es werden angemessene Maßnahmen zur Sicherheit beim Einsatz von Software und Diensten getroffen, um die Vertraulichkeit, Verfügbarkeit und Integrität zu gewährleisten.
12	Die vom Auftragsverarbeiter angegebenen und zum Audit eingereichten technischen und organisatorischen Maßnahmen nach Art. 32 DS-GVO zur Sicherheit der Verarbeitung wurden angemessen umgesetzt. Dabei können diese auch im Rahmen der anderen Prüfpunkte bereits berücksichtigt worden sein.

#	Teil C – Spezifische Anforderungen an Softwarebetrieb, -entwicklung, -wartung
13	Es werden Maßnahmen zur sicheren Softwareentwicklung ergriffen, die für den Umfang der Datenverarbeitung angemessen sind.
14	Es ist ein mehrstufiges Verfahren zur Sicherung der Softwarequalität bei der Entwicklung und Produktivsetzung von Software etabliert (3 Phasen: Development – Staging – Production).
15	Beim Testen erfolgt eine Anonymisierung personenbezogener Daten der Auftraggeber oder der Einsatz speziell für diesen Anwendungsfall erstellter Testdaten kann nachgewiesen werden.
16	Die Einhaltung von Privacy by Design und Privacy by Default wird bereits bei der Softwareentwicklung eingeplant und ermöglicht somit die Erfüllung der Anforderungen aus Art. 25 DS-GVO.

Verfahrensablauf



Bei der Antragsstellung müssen die zu prüfenden technischen und organisatorischen Maßnahmen eingereicht werden, welche Gegenstand der Überprüfung (Teil B.12) sind und explizit im Prüfbericht ausgewiesen werden.

Alle weiteren Unterlagen können im Rahmen einer max. 4 wöchigen Dokumentensammlungsphase vor dem Audit eingereicht werden. Der Auditplan wird mit dem Auftraggeber abgestimmt.

Auf Wunsch erhält der Auftraggeber eine Bescheinigung über die Anmeldung zum Audit sowie über das durchgeführte Audit, um den Zeitraum bis zur Erteilung eines Testat für Anfragen von Kunden überbrücken zu können.

Im Rahmen des Audits kann eine Prüfung der Überwachungsbereiche A.1 bis A.5 sowie C.13 bis C.16 remote erfolgen. Die Überprüfung der technischen und organisatorischen Maßnahmen auf Basis von Teil B erfolgt grundsätzlich vor Ort.

Bei dringlichen Änderungen vom Verfahrensablauf (insbesondere auf Grund des Infektionsschutzgesetzes oder von unverhältnismäßig hohen Reiseaufwänden bei Nebenstandorten) wird dies im Prüfbericht kenntlich gemacht und muss in einem Überwachungsaudit nach spätestens 12 Monaten vor Ort ergänzt werden.

Bei Unternehmen mit mehreren Standorten erfolgt die Überprüfung stichprobenartig. Die Anzahl der zu überprüfenden Standorte wird nach folgender Formel berechnet: $\sqrt{Anzahl\ Standorte}$.

Veröffentlichung

Dieser Auditstandard in der Version 1.1 wurde von der Geschäftsleitung der audatis Cert GmbH am 27.07.2023 angenommen und veröffentlicht. Er wird spätestens mit Ablauf des 26.07.2025 einer Eignungsprüfung unterzogen und bedarfsweise angepasst. Audits dürfen ab sofort nur nach dem neusten Auditstandard durchgeführt werden.

Herford, 27.07.2023

Dr. Daniela Knoop,
Leitung Konformitätsbewertung