

1. Anwendungsbereich

Der Verein Allianz Digitale Sicherheit Schweiz ADSS ("ADSS") bezweckt die Konzeption und Umsetzung von Initiativen zur Erhöhung der Sicherheit von KMU im Digitalen Raum. ADSS fusst auf einer öffentlich-privaten Trägerschaft, bestehend aus Partnern von Bund und Akteuren aus der Privatwirtschaft.

ADSS ist Inhaberin der Gütesiegels «CyberSeal». Mit diesem Gütesiegel zeichnet ADSS IT-Dienstleister aus, die ihren Kunden aus dem (nicht regulierten) KMU-Bereich beim Planen, Bauen und Betreiben ihrer IT-Infrastruktur einen angemessenen und aktuellen Minimalstandard an IT- und Informationssicherheit gewährleisten.

2. Zweck des Gütesiegels

Das Gütesiegel soll KMU, welche typischerweise nicht über eine eigene Informatikabteilung verfügen und IT-Dienste von einem oder wenigen IT-Dienstleistern beziehen, als Orientierungshilfe bei der Suche nach einem geeigneten Partner dienen.

3. Prüfung und Erteilung des Gütesiegels

3.1 Zur Erlangung des Gütesiegels wird der IT-Dienstleister einer Prüfung durch unabhängige von der ADSS mandatierte Auditoren unterzogen. Diese Prüfung umfasst typischerweise ein eintägiges Assessment mit den folgenden Schwerpunkten:

- Organisatorisch: Geschäftsmodell des IT-Anbieters, Aufgabenteilung Kunde/IT-Partner, Verwaltung des Zugriffs auf Kundeninfrastruktur, Systemdokumentation, Ausbildung der Mitarbeitenden, Business Continuity Management
- Technisch: Daten, Credentials und Berechtigungen, Netzwerkdesign, Penetrationstests, Firewalls, WLAN, AD Design, Verschlüsselung, Hardening Komponenten, eMail-System, Patch-Management, Mobile Devices, Home Office, Malware-Protection, Backup
- Prozessual: Change Management / Incident Management, Protokollierung, Monitoring, Entsorgung von Datenträgern, Services von Drittanbietern mit Abgängigkeiten zur Infrastruktur des KMU / zu anderen Anbietern, Schwachstellen beim Kunden

Die detaillierten Audit-Kontrollpunkte und -Prozesse richten sich nach dem jeweils gültigen Handbuch der ADSS.

3.2 Bei grösseren IT-Dienstleistern kann auch nur ein Teilbereich der Firma zertifiziert werden. Der Anwendungsbereich muss durch den IT-Dienstleister definiert werden, worauf die Überprüfung auf den angegebenen Anwendungsbereich beschränkt wird. Der so gewählte und zertifizierte Anwendungsbereich wird auf dem Gütesiegel vermerkt.

3.3 Der IT-Dienstleister ist verpflichtet, dem Auditor die für die Durchführung der Prüfung erforderlichen Unterlagen und Auskünfte vollständig und wahrheitsgemäss zugänglich zu machen.

3.4 Die erteilten und gültigen Garantiemarkenerteilungen werden auf der Webseite von ADSS digitalsecurityswitzerland.ch geführt.

4. Nutzung des Gütesiegels

Während der Dauer der Berechtigung gemäss Ziffer 10 kann der IT-Dienstleister das Gütesiegel CyberSeal werbemässig als Hinweis auf die erfolgte ADSS-Zertifizierung im Geschäftsverkehr verwenden, namentlich auf Geschäftspapier, Prospekten, Inseraten, Webauftritt. Das Gütesiegel darf

nicht abgeändert werden und darf nur im Zusammenhang mit dem zertifizierten Anwendungsbereich verwendet werden. Das Entgelt für den Gebrauch des Gütesiegels ist in der Nutzungsgebühr gemäss Ziffer 5 enthalten. Nach Ablauf der in Ziffer 10 genannten Dauer erlischt das Recht zum Gebrauch des Gütesiegels. Im Falle der vertragswidrigen oder missbräuchlichen Verwendung des Gütesiegels kann dem IT-Dienstleister nach erfolgloser schriftlicher Abmahnung durch ADSS das Recht auf den Gebrauch des Gütesiegels entzogen werden.

5. Gebühren

- 5.1 Die Gebühr für die Prüfung zur Erlangung des Gütesiegels und dessen Nutzung für die Dauer von drei Jahren gemäss Ziffer 10 beträgt CHF 3'700.-. Die jährliche Gebühr zur Aufrechterhaltung gemäss Ziffer 9.1 beträgt CHF 600.-.
- 5.2 Die vorgenannten Preise verstehen sich inklusive Administration, jedoch exklusive Mehrwertsteuer.

6. Gewährleistung und Haftung

- 6.1 ADSS führt die Prüfungen durch qualifizierte Auditoren mit der gebotenen Sorgfalt und nach bestem Wissen und Gewissen durch. Sie leistet keine Gewähr für die Korrektheit oder Werthaltigkeit von Prüfberichten und übernimmt keinerlei Ergebnisverantwortung.
- 6.2 ADSS haftet im Rahmen der von ihr übernommenen Tätigkeit nur für Vorsatz und grobe Fahrlässigkeit. Soweit gesetzlich zulässig, wird jede weitere Haftung wegbedungen. Sie haftet insbesondere nicht, i) dafür, dass das Gütesiegel von Dritten anerkannt wird; ii) für allfällige Schadenersatzansprüche Dritter, namentlich von Kunden der IT-Dienstleister; iii) für eine Nichterfüllung der Qualitätserwartungen Dritter sowie iv) für Sicherheitsvorfälle jeglicher Art.
- 6.3 Der IT-Dienstleister hält ADSS von jeglichen Ansprüchen Dritter frei, welche diese gegen ADSS im Zusammenhang mit der Verwendung des Gütesiegels durch den IT-Dienstleister erheben.

7. Vertraulichkeit und Datenschutz

- 7.1. Die Parteien verpflichten sich gegenseitig, alle vertraulichen Informationen, welche sie im Zusammenhang mit der Prüfung und Erteilung des Gütesiegels von der jeweils anderen Partei erhalten, geheim zu halten. Als vertrauliche Informationen gelten alle Informationen, die entweder als vertraulich bezeichnet werden oder aufgrund ihrer Natur als schützenswert erscheinen. Nicht als vertrauliche Informationen gelten Informationen, welche i) nachweislich im Zeitpunkt ihrer Mitteilung der anderen Partei bereits bekannt war; ii) ohne Zutun der empfangenden Partei offenkundig werden, oder iii) die empfangende Partei von gutgläubigen Dritten erhält, welche diese weder direkt noch indirekt von der offenlegenden Partei erhalten haben. ADSS verpflichtet sich insbesondere, die Geheimhaltungspflicht bezüglich vertraulicher Informationen, welche der IT-Dienstleister anlässlich der Prüfung offengelegt hat, dem eingesetzten Auditor schriftlich zu überbinden.
- 7.2. Die Parteien verpflichten sich zur Einhaltung der anwendbaren Datenschutzgesetze.

8. Geistige Eigentumsrechte

- 8.1 Durch die vorliegende Vereinbarung werden vorbestehende geistige Eigentumsrechte der Parteien nicht berührt. Von der ADSS erarbeitete Prüfberichte können vom IT-Dienstleister im Rahmen der vorliegenden Vertragsbestimmungen während der vereinbarten Dauer bestimmungsgemäss genutzt werden. Die Urheberrechte verbleiben bei ADSS.
- 8.2 Die markenrechtliche Nutzung der Garantiemarke durch den IT-Dienstleister wird nur für den in diesen Bestimmungen vereinbarten Gebrauch gewährt.

9. Aufrechterhaltung und Re-Zertifizierung

- 9.1 In den beiden Folgejahren der Zertifizierung bzw. Re-Zertifizierung wird je eine Aufrechterhaltung vorausgesetzt. Diese wird vom IT-Dienstleister nach Vorgaben der ADSS selbstständig durchgeführt (Selbstdeklaration). Die daraus resultierende Beschreibung wird von einem Auditor der ADSS geprüft.
- 9.2 Nach Ablauf von drei Jahren seit der Zertifizierung muss eine Re-Zertifizierung erfolgen, um das Gütesiegel für weitere drei Jahre verwenden zu dürfen. Die Re-Zertifizierung richtet sich grundsätzlich nach den Bestimmungen für die Zertifizierung.

10. Dauer

Vorbehältlich einer Re-Zertifizierung oder eines vorzeitigen Entzugs der Zertifizierung, z.B. aufgrund von missbräuchlicher Verwendung des Gütesiegels oder Nichtbehebung von Feststellungen aus der Aufrechterhaltungsprüfung, dauern die eingeräumten Nutzungsrechte am Gütesiegel drei Jahre.

11. Schlussbestimmungen

Die vorliegenden Prüfungs- und Nutzungsbestimmungen finden auf jede Prüfung, Erteilung und Nutzung des Gütesiegels Anwendung, auch wenn der IT-Dienstleister in Bestellungen auf eigene AGBs verweist. Änderungen bedürfen der Schriftform. Die Vertragsbestimmungen unterstehen Schweizer Recht unter Ausschluss von Staatsverträgen. Ausschliesslicher Gerichtsstand ist Bern.

