



DATEV-Marktplatz Premium Partnerlösungen im Kontext Privacy & Security

Gerd Kunkat, Andrea Gocke | Sabine Wächter

Digitale Ökosysteme | Strategy & Certifications

02.03.2026

Version 4

Regelung zur Umsetzungsfrist

- Siehe Folie Seite 3.

Änderung/Erweiterung der validen Liste der Zertifikate

- Siehe Folie Seite 11.
- Aufnahme „TÜV TRUST IT Trusted Application“.
- Entfernung ULD (wird nicht mehr angeboten).
- Entfernung VdS 10005 (erfüllt in neuer Version die Anforderung nicht mehr).



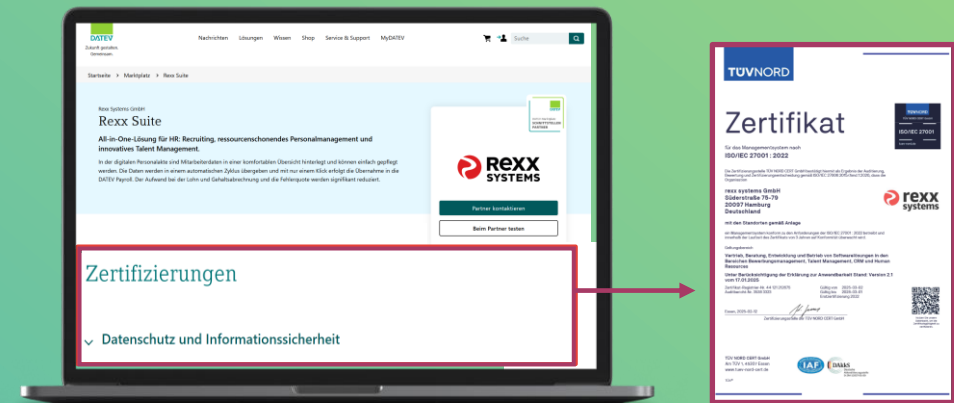
- Premium-Partner müssen bis spätestens **1. Juli 2026** über ein relevantes **Informationssicherheits- oder Datenschutz-Zertifikat** verfügen.
- **Ausnahmefall:** bei *gestarteten Zertifizierungsprozess*, kann eine Nachreichung bis 31.12.26 erfolgen. So lange wird der Marktplatzauftritt deaktiviert
- Bei Nichterfüllung der Zertifizierungspflicht erfolgt die **Kündigung** der Premium-Partnerschaft.
- Geltungsbereich: Der Zertifizierungs-Scope muss mindestens die Entwicklung und den Betrieb der Marktplatz-Lösung abdecken.

Umsetzungspflicht bis 01.07.2026

Nichtumsetzung führt zur Kündigung der Premium Partnerschaft



- Freiwillige Umsetzung eines anerkannten Informationssicherheitszertifikats stärkt das Vertrauen in Ihre Lösung
- Platzieren Sie das Zertifikat sichtbar auf dem DATEV-Marktplatz.



Agenda



01

**Motivation zu mehr
Security**

02

**Matching der
Partnerkategorien**

03

**Set skalierbare
Zertifizierung**

04

**Prozess einer
Zertifizierung**

01. Motivation zu mehr Security: EU-Regulatorik bei der Datenverarbeitung ist enorm

Nachweis von Sicherheit.

- **DATEV als Auftragsverarbeiter** bietet Nachweise über die Sicherheit der verarbeiteten Daten.
- Neue Regulatorik (DS-GVO, DORA, NIS 2.0).
- Zertifikate & Testate CoBC Art 2.
- Auditmöglichkeiten.



Security ist wichtig.

- **DATEV wirbt mit Zertifikaten** wie viele anderen Unternehmen. Dies erspart Rückfragen und schafft Vertrauen.
- Kundengewinnung.
- Vermarktung als „sicherer Partner“.



Ein Zertifikat sagt mehr als 1.000 Worte.

#effizient #vertrauenswürdig

01. Motivation zu mehr Security: Was Kanzleien beim Thema Sicherheit erwarten



02. Matching der Partnerkategorien: Privacy & Security im Kontext Premium Partner

DATEV

Durch Rahmenbedingungen wird das Partnermanagement operativ steuerbar.

Privacy & Security Anforderungen an Premium Partner, auch wenn beim jeweiligen Anbieter die Verantwortung des Geschäftsbetriebs liegt.



Kanzlei / Mandant

DATEV Mitglieder erwarten von einer "empfohlenen Partnerschaft", dass DATEV Privacy & Security sorgfältig betrachtet.

Partnerlösungen mittels datenzentrierter Workflows sicher integrieren in DATEV Produkte.



DATEV-Marktplatz Partner

Transparenz: klare Regeln am DATEV-Marktplatz für eine Kooperation

Nachweisfähigkeit über Standards: Zertifikate

02. Matching der Partnerkategorien: Differenzierung der Partnerkategorien

Kriterium	Premium Partner	Schnittstellen Partner
Der Partner wird von DATEV proaktiv empfohlen.	+	-
Der Partner wird in DATEV Entwicklungen stärker mit einbezogen – bspw. Pilotierung DATEV APIs.	+	-
Kund:innen fordern von Partnerlösungen einen Security Level, den sie von DATEV Lösungen kennen.	+	+



Privacy & Security Anforderungen differenzieren je nach Partnerkategorie

- An Premium Partner haben die Kunden deutlich höhere Privacy & Security Anforderungen, da „von DATEV empfohlen“.

02. DATEV-Marktplatz Premium Partner: Mehr Sicherheit



Sicherheitsanspruch DATEV

DATEV als Auftragsverarbeiter bietet Nachweise über Sicherheit der verarbeiteten Daten.

Umfrage Kundenerwartung
Partnerlösungen haben gleichen Security Level wie DATEV-Lösungen.

Rolle DATEV
Datenschutz und Datensicherheit sicherstellen - im Auftrag unserer Mitglieder und Kunden.

Nachweisfähigkeit

DATEV-Marktplatz zeigt Transparenz und Informationen zur Sicherheit der Partnerlösungen.

Zertifikat als Nachweis zur Sicherheit der Partnerlösung im DATEV-Marktplatz.

Scope der Zertifizierung
min. Entwicklung & Betrieb der SW.

Set akzeptierter Zertifikate
kleine Einstiegshürden, beherrschbare Kosten, Marktverbreitung, Standards.

Vorgehen in Kooperationen

DATEV-Marktplatz Premium Partner erwerben eigenverantwortlich ein für sie passendes Zertifikat bei einem passendem Zertifizierungsanbieter.

Skalierung
je nach Zertifizierungsbedarf [Internationalität, Branche, Aufwand,, Größe].

Reifegradprüfung
kostenpflichtige Quick Audits zur GAP-Analyse mit externen Zertifizierungsanbietern bei fehlender Zertifizierung als Vorbereitung.



Zertifizierungspflicht für Bestehende DATEV-Marktplatz Premium Partner

müssen eigenverantwortlich ein Datenschutz- und Informationssicherheits-Zertifikat erwerben - **Umsetzungstermin bis zum 01.07.2026.**

Neue DATEV-Marktplatz Premium Partner müssen ein Zertifikat vorweisen - seit 06/2024.

Link: <https://go.datev.de/marktplatz-security>

03. Set akzeptierter Zertifizierungen: Skalierung der Zertifikate

Basis Level Zertifikate

Standardabsicherung

- BSI-Grundschatz Basis Absicherung. 1-3 Monate Vorbereitung.
- Zertifizierungskosten ab ca. 5 TEUR. Implementierungskosten ca. 3-5 TEUR.

Medium Level Zertifikate

Kleinere und mittlere Unternehmen

- VdS, CISIS12, 6-12 Monate Vorbereitung.
- Zertifizierungskosten ab ca. 5 TEUR. Implementierungskosten abhängig von Größe und Reifegrad ca. 8 - 25 TEUR.



High Level Zertifikate

Erhöhte Security Anforderungen

- ISO, TISAX, C5, BSI-Grundschatz. 6-18 Monate Vorbereitung.
- Zertifizierungskosten ab ca. 10-15 TEUR und höher, je nach Scope. Implementierungskosten abhängig von Größe und Reifegrad ca. 10 - 25 TEUR.



Skalierung entsprechend des Zertifizierungsbedarfs

- **Set von akzeptierten Zertifikaten**, mit geringen Einstiegshürden und erfahrungsgemäß überschaubaren Kosten.
- **Kriterien** für das passende Zertifikat: Aufwand, Nutzen, Scope, Kundenanforderungen, Branchen, internationale Ausrichtung, Unternehmensgröße, Strategien.

Alle genannten Kosten und Zeitaufwände sind Schätzwerte - basierend auf Gesprächen mit Beratern und Partnern.

03. Set akzeptierte Zertifizierungen: Liste und Kriterien

Zertifikat-Testat	Skalierung	Scope	Zielgruppen	Regelwerke/Auditkriterien	Art & Akkreditierung
ISO 27001	High Level	IS (Managementsystem)	Branchenübergreifend	ISO 27001	Zertifikat, DakKS
ISO 27701	High Level	DS (Managementsystem)	Branchenübergreifend	ISO 27001 <u>und</u> aufbauend ISO 27701	Zertifikat
ISO 27017	High Level	IS – Fokus Cloud-Dienstleistungen	Branchenübergreifend	ISO 27001 <u>und</u> aufbauend ISO 27017	Zertifikat, DakKS
ISO 27018	High Level	DS- Fokus Cloud-Dienstleistungen	Branchenübergreifend	ISO 27001 <u>und</u> aufbauend ISO 27018	Zertifikat, DakKS
C5	High Level	IS/DS Cloud-Anbieter	Branchenübergreifend	<u>Cloud Computing Compliance Criteria Catalogue</u>	Zertifikat, BSI
BSI Grundschatz	High Level	IS (Managementsystem)	Branchenübergreifend	<u>BSI - IT-Grundschatz-Bausteine (Edition 2023) (bund.de)</u>	Zertifikat, BSI
TISAX	High Level	IS (Managementsystem)	Branche Automobilektor	VDA Information Security Assessment https://portal.enx.com/de-DE/TISAX/downloads/	Zertifikat, DakKS
Art 42 - Europrise	High Level	DS (IT-Produkte & Dienstleistungen)	Branchenübergreifend (KMU)	<u>EuroPriSe Criteria</u>	Zertifikat, DakKS
Art 42 - Auditor	High Level	DS Cloud-Anbieter	Branchenübergreifend (KMU)	<u>Kriterienkatalog</u>	Zertifikat, DakKS
VdS 10000	Medium Level	IS (Managementsystem)	Branchenübergreifend (KMU)	<u>VdS 10000-Richtlinien Informationssicherheitsmanagement</u>	Zertifikat, akkreditiert
VdS 10010	Medium Level	DS (Managementsystem)	Branchenübergreifend (KMU)	Valide nur wenn aufbauend auf VdS 10000 <u>VdS-Richtlinien 10010 Datenschutzmanagement</u>	Zertifikat, akkreditiert
CISIS12	Medium Level	IS/DS (Managementsystem)	Branchenübergreifend (KMU)	<u>Compliance & Informationssicherheit, 12 Schritte, Baustein, Maßnahmenkatalog</u>	Zertifikat, akkreditiert
TÜV TRUST IT Trusted Application	Medium Level	IS (Managementsystem spez. auf Anwendungsebene)	Branchenübergreifend	<u>Kriterienkatalog: Trusted Application</u> <u>Angebot Datev-Trusted-Application.pdf</u>	Zertifikat, ausgerichtet an Akkreditierung
BSI Grundschatz Basis-Absicherung	Basis Level	IS (Informationsverbund)	Branchenübergreifend	<u>Leitfaden zur Basis-Absicherung</u> <u>Checklisten Basis-Absicherung</u> <u>BSI führt IT-Grundschatz-Testat nach Basis-Absicherung ein</u>	Testat, BSI, akkreditiert



- **Neu: Aufnahme von „TÜV TRUST IT Trusted Application“ in der Liste valider Zertifikate:**
- **Als Mindest-Scope der Zertifizierung fordert DATEV:** *„Entwicklung und Betrieb der DATEV-Marktplatz Premium Partner Lösung“.*
- **Fokus der anerkannten Zertifikate:**
Orientierung an ISO27001, Akkreditierung bzw. Ausrichtung an einer Akkreditierung, ISMS-Aufbau gefordert.
- **Skalierung:**
Exemplarisch geschätzt auf Basis des Umfangs des uns vorliegenden Kriterienkatalogs - nicht auf Basis der Zertifizierungsgesamtkosten.

04. Prozess einer Zertifizierung: Vorgehen Zertifizierung für Partner

Beispielhafte Auswahl möglicher Zertifizierungsanbieter im Bereich Informationssicherheit und Datenschutz - ohne Anspruch auf Vollständigkeit.



Vorgehen

DATEV-Marktplatz Premium Partner

müssen eigenverantwortlich ein Zertifikat bei einem für Sie passenden Anbieter erwerben - **bis zum 01.07.2026.**

Bei Nichtumsetzung erfolgt eine Kündigung der DATEV-Marktplatz Premium Partnerschaft zum 01.07.2026

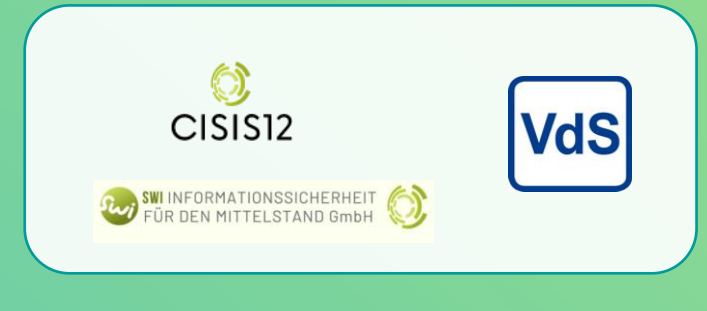
04. Prozess einer Zertifizierung: Beispielhafte Anbieter für Reifegradprüfungen zur GAP Analyse

Beispielhafte Auswahl möglicher Zertifizierungsanbieter im Bereich Informationssicherheit und Datenschutz - ohne Anspruch auf Vollständigkeit.

- **Aussagekräftiger Nachweis** anhand eines DS/IS Zertifikats [TPISA - Third Party Information Security Assessment].
- **Valide Zertifizierung** kann aufbauend zur Prüfung entstehen.
- **Vermittlung von Beratern** für Aufbau von ISMS / DSMS zur Vorbereitung auf Zertifizierung.
- **Skalierungsmöglichkeiten** im Prüfumfang.
- **Prüfungsstandard** richtet sich an kleine und mittlere Unternehmen (KMU).
- **Quick Checks** als Self-Audit und als Grundlage zur Reifegradprüfung.



Anbieter Reifegradprüfung



Die hier genannten Anbieter für Reifegradprüfungen sind DATEV eG bereits bekannt.

Kontaktdaten können vermittelt werden.

Den Partnern steht die Auswahl eines eigenen Anbieters frei.

04. Beispiel Prozess: Quick Audits als Vorbereitung zum ISMS Aufbau und Zertifizierung am Beispiel CISIS12 (SWI) und VdS



04. Zertifizierung mit ISMS Aufbau: - Prozesse und Architektur für mehr Sicherheit.

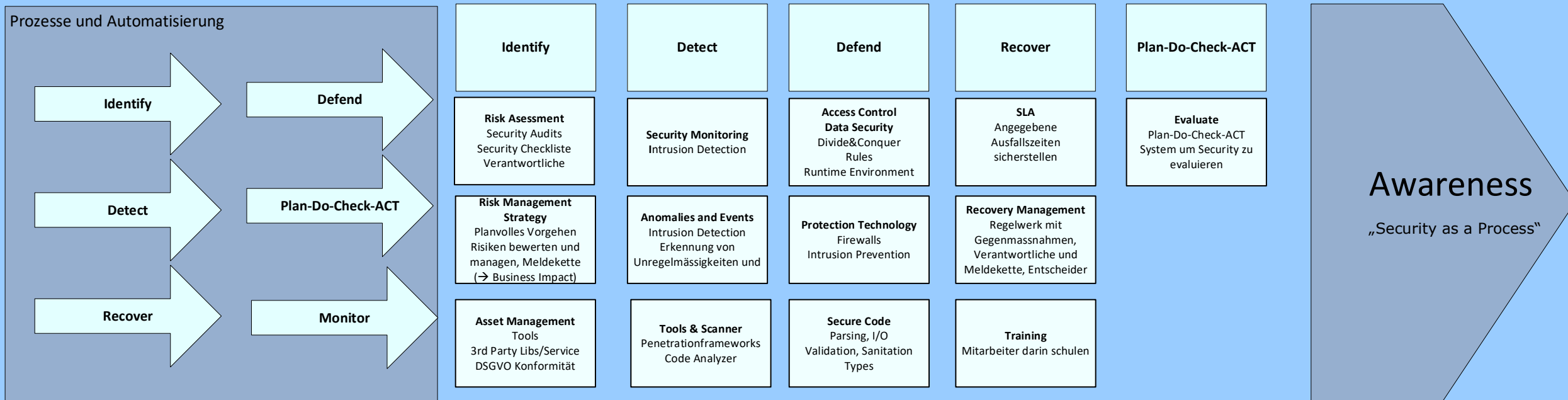
Situation ohne ISMS

- Security wird als einmaliger Snapshot oder technische Angelegenheit fehlverstanden.
- Verantwortlichkeiten, Prozesse und Strukturen sind ungeklärt.
- Was passiert dann, wenn ein Angriff erfolgt.
...Wer macht was? Zeitdruck...Downtimes...Nachweise...Datendiebstahl...Klagen.

Lösung

- **Prozesse** für Security implementieren und dokumentieren.
- **Strukturaufbau** mit Informationssicherheitsmanagementsystem (ISMS).
- **Orientierung an gesetzliche Vorgaben.**

Realisierung eines Security Frameworks





Zukunft gestalten. Gemeinsam.