Kriterienkatalog zur Prüfung gemäß „IT-Grundschutz-Profil – Basis-Absicherung Kommunalverwaltung, Version 4.0“

datenschutz cert GmbH
Version 1.0

datenschutz cert

Inhaltsverzeichnis

1. Einleitung 4
   1.1. BSI-Kommunalprofil 5
   1.2. Vorteile einer Auditierung durch die datenschutz cert GmbH 5
   1.3. Warum ein Prüfnachweise durch die datenschutz cert GmbH? 6
2. Auditierung und Nachweisführung 7
   2.2. Laufzeiten 7
   2.3. Erst-Prüfung 7
   2.4. Wiederholungsprüfung (Re-Prüfung) 9
   2.5. Entzug, Aussetzen oder Einschränken eines Prüfnachweises 9
   2.6. Ablauf eines Prüfnachweises 9
   2.7. Kosten und Gebühren 10
   2.8. AGB und KBO 10
3. Anforderungen an einen Prüfbericht 11
4. Über die datenschutz cert GmbH 12
   4.1. Leitlinien 12
   4.2. Anerkennungen und Akkreditierungen 13

Historie

Version	Datum	geänderte Kapitel	Grund der Änderung	geändert durch
0.1	04.02.2025		Erstellung Entwurf	Mühlhause
0.2	28.05.2025		Fortschreibung Entwurf	Mühlhause
0.3	21.11.2025		Umstellung auf Kommunalprofil Version 4.0	Mühlhause
1.0	18.12.2025		Finalisierung	Dr. Maseberg

Dokumenten-Überwachungsverfahren

Status	Prozess-/Dokumentbesitzer	Version
Final	Matthias Mühlhause	1.0

1. Einleitung

Bei der Auditierung zur Informationssicherheit z.B. in öffentlichen Einrichtungen, Kommunalverwaltungen sowie kleinen und mittleren Unternehmen (KMU's) können ganzheitlich alle Aspekte zur Informationssicherheit betrachtet werden, die zum „Funktionieren" eines Unternehmens oder einer Behörde notwendig sind.

Die datenschutz cert GmbH prüft bzw. auditiert – und dies unabhängig –, in welchem Reifegrad die definierten Mindestsicherheitsmaßnahmen, die in einer Kommunalverwaltung umgesetzt wurden. Die Prüfung durch die datenschutz cert GmbH erfolgt auf Basis der folgenden Anforderungen des BSI:

[BSI-Kommunalprofil] Bundesamt für Sicherheit in der Informationssicherheit, „IT-Grundschutz-Profil ‚Basis-Absicherung Kommunalverwaltung'", Version 4.0, 13.11.2023.

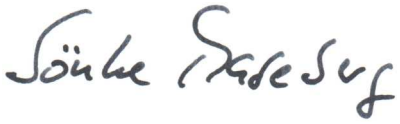
Im Falle der Erfüllung stellt die datenschutz cert hierzu einen Prüfnachweis aus. Dies kann unter anderem bei entsprechenden Behörden, für die Erlangung von Fördergeldern eingereicht werden.

Dieser Prüfnachweis, mit 2-jähriger Gültigkeit, bescheinigen einer Institution, dass sie definierte Mindestsicherheitsmaßnahmen aus [BSI-Kommunalprofil] hinreichend umgesetzt hat und dies sich durch eine unabhängige Prüfstelle, hat überprüfen lassen.

Die datenschutz cert GmbH setzt hierzu eigene kompetente und berufene Gutachter*Innen ein.

Das vorliegende Dokument beschreibt den Auditierungs- bzw. Prüfungsprozess- und das Vorgehen der Prüfstelle und stellt eine Präzisierung zu dem vollständigen Zertifizierungsschema der datenschutz cert GmbH dar.

Bremen, den 18.12.2025



Dr. Sönke Maseberg
Geschäftsführer
datenschutz cert GmbH

1.1. BSI-Kommunalprofil

Das BSI-Kommunalprofil [BSI-Kommunalprofil] definiert die Zielsetzung wie folgt: „Dieses Profil basiert auf dem BSI-Standard 200-2 „IT-Grundschutz-Methodik“ [BSI-200-2] und definiert die Mindestsicherheitsmaßnahmen, die in einer Kommunalverwaltung umzusetzen sind, um sich nach hiesiger Einschätzung nicht der groben Fahrlässigkeit schuldig zu machen. Das Profil erleichtert den Einstieg in die Informationssicherheit und hilft, die gröbsten Schwachstellen aufzudecken, die es zu beseitigen gilt, um möglichst schnell das Sicherheitsniveau in der Breite anzuheben. Um ein dem Stand der Technik angemessenes Sicherheitsniveau zu erreichen, müssen darauf aufbauend in einem weiteren Schritt jedoch zusätzliche Anforderungen erfüllt werden.“

Um den Umsetzungsstand für die Basis-Absicherung erforderlichen Anforderungen unabhängig, unparteilich und vertrauenswürdig sowie mit der entsprechenden Branchenkenntnis zu überprüfen, sollte die Institution eine unabhängige Prüfstelle wie die datenschutz cert GmbH zu einer Erst-Prüfung beauftragen. Diese prüft die Dokumente und auditiert in einer Vor-Ort-Prüfung, mit von ihr bestellten Gutachter*innen den Umsetzungsgrad der definierten Mindestsicherheitsmaßnahmen. Auf der Grundlage der im Prüfbericht zusammengefassten Ergebnisse gibt der/die Gutachter*in eine Empfehlung an die Prüfstelle der datenschutz cert GmbH ab.

Kommt der/die Gutachter*in zu dem Ergebnis, dass die Institution im Rahmen der Stichprobenprüfung anhand einer vorgegeben Prüfcheckliste der Prüfstelle, die definierten Mindestsicherheitsmaßnahmen umgesetzt hat, kann ein Prüfnachweis durch die Prüfstelle nach dem BSI-Kommunalprofil [BSI-Kommunalprofil] ausgestellt werden.

Gemäß diesem Kriterienkatalog kann nach zwei Jahren eine erneute Re-Prüfung neu beauftragt werden.

1.2. Vorteile einer Auditierung durch die datenschutz cert GmbH

Kommunalverwaltungen sind verpflichtet, ihre IT-Systeme und Verwaltungsvorgänge durch technische und organisatorische Maßnahmen ausreichend abzusichern. Diese Verpflichtungen ergeben sich z. B. aus datenschutzrechtlichen Anforderungen (u. a. EU-Datenschutz-Grundverordnung) oder dem Grundsatz des rechtmäßigen Verwaltungshandelns (Rechtsstaatsprinzip Art. 20 Abs. 3 Grundgesetz). Das Onlinezugangsgesetz (OZG) fordert in § 5 in Verbindung mit § 3 der IT-Sicherheitsverordnung Portalverbund (ITSiV-PV) für mittelbar angebundene IT-Komponenten der Kommunen mindestens die Umsetzung der Basis-Absicherung nach BSI Standard 200-2 oder einen vergleichbaren vom Land anerkannten Standard. In der Begründung zur ITSiV-PV wird zur Umsetzung in Kommunen auf das IT-Grundschutz-Profil Basis-Absicherung Kommunalverwaltung verwiesen, vgl. Abs. 5.3 [BSI-Kommunalprofil].

Erfahrungsgemäß bekommen Organisationseinheiten durch eine unabhängige Auditierung weiteren Input zu ihrem kontinuierlichen Verbesserungsprozess und die Organisationseinheit bekommt mit einem Prüfnachweis einen objektiven Nachweis gegenüber Dritten.

Organisationen, die den Schutz von sensiblen Daten ernst nehmen, die Aufrechterhaltung ihrer eigenen Dienstleistung sichern möchten und selbst auferlegte Sicherheitsstandards umsetzen wollen oder aber auch, um den rechtlichen Anforderungen des Gesetzgebers zu genügen, wird mit dem BSI-Kommunalprofil [BSI-Kommunalprofil] der Einstieg in Informationssicherheits-Managementsystem (ISMS) geboten, der sodann auch mit einem Prüfnachweis nachgewiesen werden kann.

Nicht zu unterschätzen sind die positiven Effekte, die Reputation betreffend, um Vorgesetzten, Eigentümer, Geschäftspartnern einen verantwortungsvollen Umgang mit Informationen und auch personenbezogenen Daten widerzuspiegeln und nicht zuletzt die Möglichkeit, einen Prüfnachweis einer anerkannten Institution wie der datenschutz cert GmbH für das Marketing zu nutzen.

1.3. Warum ein Prüfnachweise durch die datenschutz cert GmbH?

Über 18 Jahre Erfahrung in der Auditierung/ Prüfung und Zertifizierung von Informationssicherheit und Datenschutz. Wir sind eine anerkannte und akkreditierte Zertifizierungsstelle mit qualifizierten und berufenen Gutachter*innen. Wir sind bei der DAkkS als Zertifizierungsstelle unter anderem für die Norm ISO/IEC 27001, ISO/IEC 27701, ips-DSGVO und weitere z.B. eIDAS akkreditiert. Wir sind als Prüfstelle für IT-Sicherheit vom BSI anerkannt. Des Weiteren verfügen wir über BSI-lizenzierte IT-Grundschutz-Auditoren und sind beim BSI anerkannter IT-Sicherheitsdienstleister für Penetrationstests.

2. Auditierung und Nachweisführung

Zunächst wird in diesem Abschnitt vorgestellt, wie die datenschutz cert GmbH definierte Mindestsicherheitsmaßnahmen gem. BSI-Kommunalprofil [BSI-Kommunalprofil] in der Umsetzung prüft und einen Prüfnachweis erstellt.

2.1.1. Auditanfrage (Anfrageformular)

Für die Erst-Prüfung ist von der Kommunalverwaltung das Anfrageformular (ZV41) zu füllen und der datenschutz cert GmbH unterschrieben zur Verfügung zu stellen. Diese Angaben sind wesentlich für die Angebotserstellung, Beauftragung und ergänzt die Prüfgrundlage.

2.2. Laufzeiten

Der Prüfnachweis ist zwei Jahre gültig. Jedes Prüfverfahren besteht aus den folgenden Phasen:

- Erst-Prüfung;
- erneute Re-Prüfung (max. 24 Monaten nach Erteilung des Prüfnachweises).

Es wird ein zweistufiges Prüfverfahren eingesetzt:

- Der bei der datenschutz cert GmbH berufene Gutachter prüft die Umsetzung der definierten Mindestsicherheitsmaßnahmen und erstellt einen Prüfreport.
- Zur Nachweisführung prüft die Prüfstelle den Report, insbesondere um eine Vergleichbarkeit zwischen den Prüfungen sicherstellen zu können.

2.3. Erst-Prüfung

Die Erst-Prüfung spaltet sich auf in

- Vorbereitung,
- Prüfung vor Ort und
- Nachbereitung,

woran sich dann die Nachweisführung anschließt, sofern das Auditteam einen Prüfnachweis empfiehlt.

2.3.1. Vorbereitung

Im Rahmen der Vorbereitung stellt die Organisation dem Gutachter die für die Prüfung benötigten Referenzdokumente zur Verfügung – typischerweise umfasst dies

- eine Darstellung des Geltungsbereiches sowie
- eine Darstellung der Vorgehensweise nach IT-Grundschutz.

In der Regel findet nur eine Prüfung eines Standortes (Zentrale/ Hauptverwaltung) der Kommunalverwaltung statt.

Die Prüfung von mehreren Standorten (Multi-Site Verfahren) wird durch eine repräsentative Stichprobe durchgeführt. Die Höhe der Stichprobe sowie die Anzahl

wird von der Prüfstelle, auf Basis anerkannter Regeln (ISO/IEC 27006, IAF MD 1) festgelegt.

2.3.2. Prüfung gemäß BSI-Kommunalprofil

Die Prüfung besteht aus Dokumentenprüfung sowie Site Visit.

Bei der Umsetzungsprüfung werden durch Kontrollfragen in einer Prüfcheckliste die Umsetzung geprüft und bewertet. Der Gutachter überzeugt sich nach einem Stichprobenverfahren von der wirksamen Umsetzung der Anforderungen und dokumentiert dies in seinem Prüfreport.

Die zu prüfende Bausteine werden vom Gutachter nach einem Stichprobenverfahren aus den Baustein- und Maßnahmenkatalog ausgewählt bzw. sind bereits gemäß einem Prüfschema vorgegeben.

Beim Audit vor Ort werden die definierten Mindestsicherheitsmaßnahmen in der Umsetzung prüft und bewertet:

- Für jeden anwendbaren Aspekt der Prüfgrundlage prüft der Gutachter, wie lt. Dokumentation dieser Aspekt der Prüfgrundlage umgesetzt werden soll. Dabei sichtet der Gutachter die Dokumentation und prüft sie auf Vollständigkeit, Plausibilität und Nachvollziehbarkeit zu den Anforderungen an die definierten Mindestsicherheitsmaßnahmen.
- Für jeden anwendbaren Aspekt der Prüfgrundlage prüft der Gutachter beim Audit den Umsetzungsgrad der in der Dokumentation angegebenen Maßnahmen.
- Der Gutachter erstellt final einen ausführlichen Prüfbericht, auf Basis einer durch die datenschutz cert GmbH vorgegeben Prüfcheckliste.
- Etwaige Abweichungen werden aufgenommen; dazu gibt es fünf Abstufungen:
    1. Abweichung von einer Standardanforderung, die grundsätzlich die Funktionsfähigkeit der definierten Mindestsicherheitsmaßnahmen in Frage stellt (Hauptabweichung/ Major Non-Conformities).
    2. Abweichung von einer Standardanforderung, die in ihrer Summe die Funktionsfähigkeit der definierten Mindestsicherheitsmaßnahmen in Frage stellt (Nebenabweichung/ Minor Non-Conformities);
    3. Abweichung von einer Standardanforderung, die in ihrer Geringfügigkeit die Funktionsfähigkeit der definierten Mindestsicherheitsmaßnahmen insgesamt nicht in Frage stellt (großes Verbesserungspotential);
    4. Abweichung von einer Standardanforderung, die in ihrer Geringfügigkeit die Funktionsfähigkeit der definierten Mindestsicherheitsmaßnahmen insgesamt nicht wesentlich in Frage stellt (kleines Verbesserungspotential);
    5. Anforderungen des Standards sind erfüllt;

Bei offen Abweichungen kann kein Prüfnachweis erteilt werden, alle geprüften Anforderungen müssen umgesetzt sein. In diesem Fall wird die Prüfstelle einen Prüfnachweis erstellen.

Die Auditierung wird strikt unabhängig von jeglicher Beratung durchgeführt.

2.3.3. Nachweisführung

Auf Grundlage des Prüfberichts sowie weiterer relevanter Informationen und Nachweise trifft die Prüfstelle final die Entscheidung, ob die definierten Mindestsicherheitsmaßnahmen Standard-konform umgesetzt wurden und erteilt, dann ein gültigen Prüfnachweis: Dieser Prüfnachweis bescheinigt dem Antragsteller, dass die die definierten Mindestsicherheitsmaßnahmen für den im Prüfnachweis ausgewiesenen Anwendungsbereich den Anforderungen der Prüfgrundlage angemessen genügt.

Prüfung und Nachweisführung werden strikt unabhängig voneinander durchgeführt.

2.4. Wiederholungsprüfung (Re-Prüfung)

Nach Ablauf des zwei Jahre gültigen Prüfnachweis kann eine Wiederholungsprüfung durchgeführt werden, dass sich im Wesentlichen an der Erst-Prüfung orientiert und zusätzlich die kontinuierliche Wirksamkeit der definierten Mindestsicherheitsmaßnahmen feststellen soll.

2.5. Entzug, Aussetzen oder Einschränken eines Prüfnachweises

Der Prüfnachweis wird entzogen, wenn der Antragsteller nachhaltig gegen die Konformitätsbewertungsordnung (KBO) der datenschutz cert GmbH verstößt. Ein solcher Verstoß liegt insbesondere vor, wenn

- der geprüfte Untersuchungsgegenstand in der beschriebenen Weise verändert wurde und/oder der Anbieter keine Prüfung/ Auditierung ermöglicht,
- im Rahmen der Prüfung/ Auditierung nicht die für die Vergabe des Prüfnachweises erforderlichen Voraussetzungen erfüllt werden,
- der Antragsteller aufgrund drohender oder eingetretener Insolvenz einen zuverlässigen Geschäftsbetrieb nicht mehr aufrechterhalten kann oder
- die Prüf-/Auditkosten nicht spätestens innerhalb der in der Rechnung der datenschutz cert GmbH genannten Frist gegenüber der Prüfstelle beglichen werden.

Die Prüfstelle teilt dem Antragsteller die Gründe des Entzugs mit.

Ferner kann die datenschutz cert GmbH Prüfnachweise mit Laufzeiten aussetzen, wenn eine wesentliche Anforderung der Prüfgrundlage nicht erfüllt wird (max. Aussetzung: 6 Monate), oder einschränken, wenn für diesen ausgeschlossenen Teil wesentliche Anforderung der Prüfgrundlage nicht erfüllt werden (Einschränkung des Geltungsbereiches). Im Anschluss an eine Aussetzung erfolgt entweder die Behebung unter Berücksichtigung entsprechender Nachweise (mit Wiederherstellung) oder die Zurückziehung des Prüfnachweises.

2.6. Ablauf eines Prüfnachweises

Soweit der Prüfnachweis mit Laufzeiten nach Ablauf der Gültigkeit entfällt, hat der Anbieter dafür zu sorgen, dass sämtliche Hinweise auf einen gültigen Prüfnachweis aus den genutzten Medien unverzüglich entfernt werden.

2.7. Kosten und Gebühren

Kosten fallen für die Auditierung an: Dokumentenprüfung, Vor-Ort-Audit, Berichtserstellung.

Eine separate Gebühr durch die Prüfstelle wird nicht erhoben. Der Prüfbericht und der Prüfnachweis als pdf-Datei sind kostenfrei.

Papierdrucke, andere Sprachen (Prüfbericht/ Prüfnachweis) als deutsch und persönliche Übergaben werden nach Aufwand berechnet und müssen vor Auftragserteilung an die Prüfstelle bekannt gemacht werden.

Neben den Prüfkosten fallen Reisekosten an. Diese werden nach Aufwand berechnet.

Angebote zur Prüfung gem. BSI-Kommunalprofil [BSI-Kommunalprofil] werden grundsätzlich für eine Laufzeit über 2 Jahre erstellt.

Ein Kombinationsaudit oder Übernahme einer anderen Prüfgrundlage ist nicht möglich.

Sprechen Sie uns für ein konkretes Angebot bitte einfach über https://www.datenschutz-cert.de/kontaktformular an.

2.8. AGB und KBO

Im Falle eines Vertragsschlusses gelten ausschließlich unsere Allgemeinen Geschäftsbedingungen (AGB) sowie unsere Konformitätsbewertungsordnung (KBO), die Sie unter https://www.datenschutz-cert.de/ueber-uns/agb.html abrufen können.

3. Anforderungen an einen Prüfbericht

Der Prüfbericht zur Vorlage bei der Prüfstelle muss auf Basis der Vorlagen der Prüfstelle und inhaltlich mindestens zu folgenden Aspekten Stellung beziehen:

- Organisatorische und formale Angaben zur Auditierung:
  - der mit der Auditierung angestrebte Prüfnachweis;
  - untersuchte Organisation, Name, Anschrift, Standort;
  - genaue Bezeichnung des Untersuchungsgegenstands, Abgrenzung zu den nicht geprüften Bereichen;
  - Namen des Prüf-/ Auditeam Teilnehmer*innen
  - Zeitraum der Prüf-/Auditierung;
- Angewandte Methodik: z.B. Prüfung von Dokumenten des Auftraggebers, Führung von Mitarbeitergesprächen, Durchführung von Stichproben vor Ort (Site Visit) oder Plausibilitätstests;
- Prüfgrundlage der Auditierung:
  - Prüfkriterien und Prüfgrundlage ist das BSI-Kommunalprofil [BSI-Kommunalprofil] mit Nennung des Versionsstandes der Grundlage;
  - eingesehene Dokumente;
  - befragte Abteilungen/Arbeitsbereiche/Unternehmensorgane;
  - Gegenstand der Stichproben;
  - Ortsbesichtigung, Standort, Adresse, Dauer, Teilnehmer;
- Erklärung der Auditor*in zur Unabhängigkeit und Unparteilichkeit;
- Kurzdarstellung des Untersuchungsgegenstands;
- Zusammenstellung des für den konkreten Prüfgegenstand anwendbaren Prüfkriterien/Anforderungen;
- Prüfergebnisse:
  - Auditierung und Bewertung von Prüfpunkten gemäß vorgegebener Prüfgrundlage (Prüfcheckliste);
- Empfehlung des Auditors mit:
  - Zusammenfassung der Prüfergebnisse / Management Summary;
  - Vorschlag an die Prüfstelle.

4. Über die datenschutz cert GmbH

Die datenschutz cert GmbH bietet Konformitätsbewertungen auf dem Gebiet des Datenschutzes und der Informationssicherheit an. Diese Konformitätsbewertungen schließen sowohl Prüfaktivitäten als auch Zertifizierungstätigkeiten ein – einerseits für IT-Systeme und -Produkte und andererseits für Verfahren und Managementprozesse.

Die datenschutz cert GmbH ist ein Unternehmen der DSN Group. Sitz der Gesellschaft ist Bremen. Geschäftsführer ist Dr. Sönke Maseberg. Die Unternehmen der DSN Group sind inhabergeführt.

4.1. Leitlinien

Die datenschutz cert GmbH bietet Konformitätsbewertungen unter folgenden grundsätzlichen Leitlinien an:

4.1.1. Unabhängigkeit und Unparteilichkeit

Wir sind unabhängig und unparteilich. Es gilt das übergeordnete Interesse und die vorrangige Pflicht, Auditierung, Evaluierungen, Zertifizierungen und Bestätigungen entsprechend den Vorgaben frei von internen und externen kommerziellen, finanziellen und sonstigen Zwängen durchzuführen. Maßstab ist das jeweilige Kriterien Werk. Zudem führen wir keinerlei Beratung durch.

Wir haben einen "Ausschuss zur Sicherstellung der Unparteilichkeit der datenschutz cert GmbH" (Ausschuss) etabliert, mit dem die grundsätzlichen Regelungen zur Unabhängigkeit und Unparteilichkeit der Zertifizierungstätigkeiten diskutiert und durchgeführte Zertifizierungsprozesse auf ihre Unabhängigkeit hin überprüft werden.

Zur Gewährleistung der Unabhängigkeit und Unparteilichkeit unserer erteilten Prüfnachweise setzen wir für den Auditierung- und Entscheidungsprozess darüber hinaus regelmäßig externe Fachbegutachter ein.

4.1.2. Vertraulichkeit

Wir sichern Ihnen Vertraulichkeit zu.

4.1.3. Offenheit und Transparenz

Wir sind offen und transparent hinsichtlich unserer Tätigkeiten, d.h.

- wir kommunizieren klar und unmissverständlich, was und nach welchen Regeln geprüft und zertifizieren wird;
- unsere Prüfnachweise und Prüfberichte sind klar und verständlich formuliert;
- wir veröffentlichen die zugrundeliegenden Regelwerke – sofern nicht durch Copyright geschützt;
- wir benennen klar, wofür wir akkreditiert sind;
- wir lassen uns selber regelmäßig prüfen;
- wir sind offen für alle Anfragen und Beschwerden: Wenn Sie Fragen zu einem von uns erteilten Zertifikat haben oder potentiell den Missbrauch eines Zertifikats

vermuten: Bitte sprechen Sie uns an. Wir sichern Ihnen Vertraulichkeit zu und gehen der Sache nach. Wir informieren Sie über den Stand der Untersuchung sowie den Abschluss.

4.1.4. Datenschutz

Wir kommen aus dem Datenschutz. Jede Art von Konformitätsprüfung wird – im Rahmen des jeweiligen Untersuchungsgegenstands – unter den besonderen Aspekten des Datenschutzes beleuchtet. Dadurch stellen wir sicher, dass die von uns geprüften und bewerteten IT-Produkte und -Systeme den Anforderungen des Datenschutzes genügen.

Unser Anspruch ist, dass sich "datenschutz zertifizierte" Produkte und Prozesse etablieren und für unsere Kunden einen Mehrwert zu einem besseren Datenschutz darstellen und dass unser Zertifikat eine entsprechende Anerkennung genießt.

4.2. Anerkennungen und Akkreditierungen

Die datenschutz cert GmbH ist bei der **Deutschen Akkreditierungsstelle GmbH (DAkkS)** zu folgenden Regelwerken akkreditiert:

- ISO/IEC 27001 für Informationssicherheits-Managementsysteme (ISMS)
- „IT-Sicherheitskatalog gemäß § 11 Abs. 1a EnWG“ für Strom- und Gasnetzbetreiber
- „IT-Sicherheitskatalog gemäß § 11 Abs. 1b EnWG“ für Energieanlagenbetreiber
- ISO/IEC 27701 für Datenschutz-Managementsysteme (DSMS)
- eIDAS für Vertrauensdiensteanbieter
- „ips-VSS-IT“ für Videosprechstunden
- Zertifizierungsstandard ‚DSGVO – information privacy standard‘ gem. Art. 42 DSGVO

„ips-VSS-IT“ für Videosprechstunden und „DSGVO – information privacy standard“ sind von der datenschutz cert GmbH erstellte, **behördlich genehmigte Zertifizierungsstandards**.

Auditoren der datenschutz cert GmbH sind beim **Bundesamt für Sicherheit in der Informationstechnik (BSI)** als Auditoren für die TR-03109-6 (Smart Meter Gateway Administratoren) sowie BSI TR-03145 (Secure CA Operation) zertifiziert.

Die datenschutz cert GmbH ist als Prüfstelle für IT-Sicherheit und IT-Sicherheitsdienstleister beim Bundesamt für Sicherheit in der Informationstechnik (BSI) anerkannt.

Die datenschutz cert GmbH beschäftigt beim BSI lizenzierte IT-Grundschutz-Auditoren. Die datenschutz cert GmbH stellt eines der beiden GS-Zertlabs, die für das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Prüfbegleitung in den IT-Grundschutz-Verfahren durchführt.

Die datenschutz cert GmbH ist bei der **Bundesnetzagentur** anerkannte Zertifizierungsstelle nach eIDAS gem. Vertrauensdienstegesetz (VDG).

Aufgrund der Akkreditierung bei der DAkkS und der Anerkennung beim BSI darf die datenschutz cert GmbH im Kontext von §8a BSIG/KRITIS-VO-Verfahren die Rolle der

„**prüfenden Stelle**“ einnehmen. Ferner sind die Auditoren der datenschutz cert GmbH beim BSI als Prüfer für § 8a BSIG anerkannt; dies umfasst auch die Prüfung von Systemen zur Angriffserkennung (SzA).

datenschutz cert

datenschutz cert GmbH

Hauptsitz Bremen
Konsul-Smidt-Straße 88a
28217 Bremen
Tel.: +49 421 69 66 32-550

Standort Offenbach
Mainstraße 143
63065 Offenbach am Main
Tel.: +49 69 870 07 83-580

office@datenschutz-cert.de
www.datenschutz-cert.de