Zertifizierung zum IT-Sachverständigen

Darstellung der Anforderungen an Gutachten für die Zertifizierungsstufen:

- **EDV(IT)-Sachverständiger**
  Stufe 1 Basis DEKRA Standard (Schwerpunkt Schadens-/Wertermittlung für Systeme und Anwendungen, bzw. Systeme und Technik)

- **Sachverständiger IT-Forensic**
  Stufe 1.1 Basis DEKRA Standard
  (lokale und mobile Systeme)

- **Sachverständiger IT-Security**
  Stufe 1.2 Basis DEKRA Standard (Schwerpunkt: Netzwerk und Internet)

Stand: 08/2019

Inhalt:

Aus Gründen der besseren Lesbarkeit wird in diesem Dokument davon abgesehen, die weibliche und männliche Form auszuführen. Es versteht sich von selbst, dass alle Bezeichnungen sowohl in der weiblichen als auch in der männlichen Form verwendet werden.

1. GRUNDSÄTZLICHE ANFORDERUNGEN AN IT-GUTACHTEN

1.1 Allgemeine Anforderungen an Gutachten

Ein Gutachten muss verständlich und nachvollziehbar sein. Maßstab hierfür ist ein fachlich unvorbereiteter Dritter. dieser muss in der Lage sein dem roten Faden, der sich durch das Gutachten zieht, folgen zu können. Ein Gutachten was unverständlich ist, wird als mangelhaft und unbrauchbar verworfen.

1.2 Lesbarkeit und Verständlichkeit eines Gutachtens

Gutachten sollen so erstellt werden, dass ein Dritte die Möglichkeit hat Notizen im Gutachten zu vermerken. Daneben sollten eine Schriftgröße und Art gewählt werden, die eine leichte Lesbarkeit des Textes ermöglicht.

Der Sachverständige hat die äußerliche Gestaltung entsprechend der vom DIN für Veröffentlichungen aus Wissenschaft, Technik, Wirtschaft und Verwaltung des Normenausschusses, Bibliotheks- und Dokumentenwesen herausgegeben Normen vorzunehmen.

- Schriftart: Arial bzw. Times New Roman
- Schriftgröße: 11/12 pt
- linker Seitenrand 4 cm, rechter Seitenrand 3 cm.
- Zeilenabstand: 1,15 bis max. 1,5
- Eigenhändige Unterschrift im Gutachten
- Besiegelung des Gutachtens
- Bindung des Gutachtens, dass unerwünschte Änderungen, bzw. der Austausch oder das Entfernen einzelner Seiten oder Abschnitte nicht möglich ist

1.3 Neutrale Sprache und Ausdrucksweise

Der Sachverständige hat sich der neutralen Ausdrucksweise zu bedienen. Insbesondere gegenüber Dritten darf er sich nicht zu sarkastischen oder herabsetzenden Äußerungen hinreißen lassen.

Dies gilt auch, wenn zum Beispiel mit Feststellungen von anderen Sachverständigen auseinandersetzen muss, die meist als Parteigutachter Grenzen der Neutralität überschritten haben.

1.4 Angaben der Grundlagen

Der Sachverständige hat sich mit den Grundlagen seiner Tätigkeit auseinander zu setzen. Dieses beinhaltet in vielen Fällen die Darstellung der rechtlichen und wirtschaftlichen Grundlagen, als auch die Auseinandersetzung mit dem Stand der Wissenschaft und Technik.

Sofern die verwendeten Grundlagen auf eine Quelle zurückzuführen sind, so ist diese anzugeben.

Die im Gutachten aufgeführten Quellen und Literaturhinweise sind im Anhang als Verweis aufzuführen. Literaturhinweise die nicht verwendet wurden, sind im Gutachten nicht aufzuführen.

1.5 Angabe der angewandten Verfahren

Daneben sind die angewandten Verfahren zu beschreiben und der Bezug zu dem Auftrag des Gutachtens herzustellen.

Sofern mehrere Verfahren in Betracht kommen, ist die Auswahl für ein Verfahren zu erläutern und zu begründen, warum dieses und nicht ein anderes angewendet wird.

2. INHALT EINES IT-GUTACHTENS

2.1 Deckblatt eines Gutachtens

Dem schriftlichen Gutachten ist ein Deckblatt vorgelagert.

- Name, Anschrift, Kontaktdaten des Sachverständigen
- Fachgebiet des Sachverständigen
- Bezeichnung „Gutachten“ mit zusätzlicher Spezifizierung der Gutachtenerstellung
- eindeutige Gutachtennummer
- Erstellungsdatum des Gutachtens
- Nennung des Auftraggebers
- Gesamtumfang des Gutachtens inkl. Anlagen
- Ggf. Aktenzeichen des Auftraggebers/Gerichts
- Anzahl der Ausfertigungen / Nr. der Fertigung

2.1.1 Zusätzlich für EDV-Sachverständige/IT-Sachverständige

- Bewertungsstichtag / Qualitätsstichtag

2.1.2 Zusätzlich für Sachverständige IT-Forensic/IT-Security

- Untersuchungszeitraum

2.2 Allgemeiner Inhalt eines Gutachtens

- Inhaltsverzeichnis mit Seitenzahlen
- Anlagenverzeichnis
- Kopf-/Fußzeile ab Seite 2
    - Name des Sachverständigen
    - Name des Auftraggebers
    - Gutachten-Nr.
    - Seitenzahl

2.3 Grundlagen des Gutachtens

Zu einem Gutachten gehören Unterlagen, bei Gerichtsaufträgen in der Regel Gerichtsakten, die dem Sachverständigen ausgehändigt werden. Die Gerichtsakte wird in der Regel im Original ausgehändigt, die sonstigen Unterlagen in Kopie.

Sonstige Grundlagen des Gutachtens sind zu benennen und ggf. Auflagen zu verweisen:

- Beschreibung der Ausgangssituation
- Vollständige Nennung inkl. Anschrift des Auftraggebers
- Fragestellung / Beweisfragen des Auftraggebers
- Beschreibung des Gutachtenzwecks
- Bezeichnung aller vom Auftraggeber zur Verfügung gestellten Unterlagen
- eigene Recherchen des Sachverständigen mit geeigneter Quellangabe
- verwendete Literatur, Normen mit Quellangaben
  (Titel, Autor, Verlag, Ausgabe/Auflage)

2.3.1 Zusätzlich bei Sachverständigen IT-Forensic

- Beschreibung der verwendete Auswerteumgebung
- Beschreibung der eingesetzten Hard- und Software für die forensische Auswertung
    - Produktname der Hard- und Software
    - bei Software Versionsnummer (Release)
    - Kurzbeschreibung wofür das Gerät verwendet wird, bzw. wofür die Software verwendet wird.

2.3.2 Zusätzlich bei Sachverständigen IT-Security

- verwendete Normen, Richtlinien
- verwendete Software
    - Produktname Software
    - bei Software Versionsnummer (Release)
    - Kurzbeschreibung wofür das Gerät verwendet wird, bzw. wofür die Software verwendet wird.

2.4 Ortsbesichtigung / Persönliche Inaugenscheinnahme

Ohne eine persönliche Inaugenscheinnahme (Ortstermin), kann in der Regel kein Auftrag ausgeführt werden. Eine Ausnahme ist dann gegeben, wenn z. B. die zu begutachtende Sache nicht mehr vorhanden ist (z. B. Diebstahl, Veräußerung, usw.).

Der Sachverständige ermittelt auftragsgemäß den Zustand der zu begutachtenden Sache. Der Sachverständige beschreibt, was er vor selbst gesehen und vorgefunden hat, ohne die Einflussnahme durch Dritte.

In seinem Gutachten wird der Sachverständige ausführen müssen, warum er die Sache oder das Objekt untersucht hat, damit Prozessvertreter, Parteien, Richter oder Dritte verstehen, wie er zu diesem Ergebnis kommt.

Der Sachverständige fast in der Beschreibung des Ortstermins seine Feststellungen zusammen. Dabei sollten folgende Angaben vorhanden sein.

- Ort und Datum des Ortstermins.
- Teilnehmende Personen, sowie ggf. vor Ort eingesetzten Hilfskräfte.
- Beginn und Ende des Ortstermins.
- Anwesenheitszeiten der teilnehmenden Personen.
- Beschreibung der vor Ort durchgeführten Maßnahmen und Feststellungen.
- Nennung und Beschreibung der eingesetzten Hilfsmittel (z. B. Messgeräte, usw.)
- Sollte eine Hilfskraft vor Ort eingesetzt werden, so ist deren Tätigkeit und Feststellungen zu nennen und ggf. zu beschreiben.
- Nennung von Hinweisen der Beteiligten, die für Gutachtenbewertung von Relevanz sind.

2.4.1 Zusätzlich bei Sachverständigen IT-Forensic

- Beschreibung forensischer Sicherungs- und Analyseverfahren.
- Nennung der eingesetzten Tools (z. B. Live-Sicherung, Live-Analyse)
- Nennung der durchgeführten Maßnahmen

2.5 Beschreibung der zu begutachtenden Objekte

Einer der wichtigsten Punkte im Rahmen der Gutachtenerstellung ist die Beschreibung des zu begutachtenden Objektes. Der Sachverständige muss sich in diesem Fall auf das Wesentliche beschränken und die für das Gutachten entscheidenden Tatsachen darstellen.

Bei den Gutachten im Bereich der Wertermittlung, IT-Forensic und IT-Security gelten u. a. folgende Mindestangaben.

2.5.1 Wertermittlung

Die charakteristischen Daten eines Systems sind anlagespezifisch. Sie geben Auskunft über Art und Typ des Gegenstands, seiner Leistungsfähigkeit, seiner Optionen und über seinen Hersteller bzw. Systemintegrator.

Der Sachverständige hat sicherzustellen, dass im Gutachten eine eindeutige Zuordnung möglich ist. Mindestens sollte jedoch enthalten sein:

- Typenschildangaben
    - Modell
    - Typenangabe
    - Charakteristische Leistungsmerkmale
- ggf. Betriebsanleitungen oder Handbücher
- ggf. Systemkonfigurationsunterlagen oder Dateien
- ggf. Anschaffungsbelegen
- ggf. Software
    - Betriebssystem
    - ggf. Anwendungssoftware (inkl. Versions-Nr., ggf. Service-Pack)

2.5.2 IT-Forensic

In der IT-Forensic gilt der Grundsatz des unveränderbaren Beweismittels und deren lückenlosen Dokumentation. Bei digitalen Daten ist neben dem Gerät auch Information des dahinterliegenden Systems, bzw. des verbauten Datenträgers zu nennen.

Mindestens jedoch sollte enthalten sein:

- Technische Kenndaten
- Seriennummer des Geräts und des verbauten Datenträgers
- Hashwert des Datenträgers (MD5 oder SHA1 oder vergleichbarer Hashwert)

2.5.3 IT-Security

Im Bereich der IT-Security werden u. a. Konzepte erstellt. Art und Umfang der Konzeptionserstellung richten sich individuell nach den Vorgaben des Auftraggebers. Dabei kann es sein, dass auch nur einzelne Bereiche untersucht werden. Weiteren Unterteilungen sind jederzeit durch den Sachverständigen möglich.

Nachfolgende Bausteine geben eine Orientierung:

- Geschäftsprozesse
- IT-Systeme
- Gebäude/Räume
- Netze und Kommunikation
- Infrastruktur
- Anwendungen

2.6 Beschreibung der angewandten Verfahren im Gutachten

Aufgrund der besonderen Erfahrung in seinem Sachgebiet erkennt der Sachverständige vorhandene Abweichungen und hat diese fachlich zu beschreiben. Insbesondere die durchgeführten Maßnahmen und Verfahren sind so zu beschreiben, dass sie für einen Laien verständlich sind. Die Maßnahmen wie auch die Verfahren sind nach dem jeweilig gültigen technischen Stand durchzuführen.

Sofern von den gängigen Verfahren abgewichen wird, ist dieses zu erläutern und das angewandte Verfahren so zu erklären, dass deutlich erkennbar ist, warum dieses und nicht das gängige Verfahren angewandt wird.

2.6.1 Wertermittlung

In der Wertermittlung sind alle angewandten Verfahren zu beschreiben, die angewandten Wertermittlungsansätze und Begrifflichkeiten sind zu erläutern, z. B.

- Grundlagen der Zeitwert-, Verkehrswert-, Restwertberechnungen, usw.
- Grundlagen der Zeitwert- und Gebrauchswertfaktors
- Grundlagen der Softwareberechnung
    - Standardsoftware
    - Individualsoftware

2.6.2 Zusätzlich bei IT-Forensic

- Beschreibung forensischer Vorbereitungsmaßnahmen
    - Welche Methode wurde angewendet.
    - Welche Hard- und Software wurde genutzt.
    - Beschreibung der Sicherungsumgebung
      (z. B. getrennt vom Netzwerk, autark, usw.)
- Beschreibung was dem Original-Beweismittel
    - Lagerung, Archivierung, Rückgabe, usw.
- Verifizierung der gesicherten Daten mittels Hashwertverfahren

2.6.3 Zusätzlich bei IT-Security

- Vorgehensmodell
- Schutzziele
- Definition des Gefährdungspotentials bzw. Risikoabstufungen

2.7 Analyse und Bewertung

Im Bereich der Bewertung und Analyse werden alle Feststellungen zu einem Ereignis formuliert. Es ist Aufgabe des Sachverständigen darauf hinzuweisen, ob nur dieses Ereignis eintreten kann oder ob noch Alternativen im Ergebnis möglich sind.

Im Einzelnen können Szenario Analysen zu einem wahrscheinlichen Ergebnis führen. Der Wahrscheinlichkeitsgrad soll hierfür angegeben werden.

Bei der Analyse und Bewertung soll so aufgebaut werden, dass der Laie den Gedankengang des Sachverständigen folgen kann. Die jeweiligen Bewertungskriterien sind zu nennen und zu begründen. Das Ergebnis ist zu erläutern und eine Plausibilisierung durchzuführen.

2.7.1 Zusätzlich in der Wertermittlung

- Zeitwertberechnung
    - Berechnung des Alters
    - Begründung der betriebsgewöhnlichen Nutzungsdauer
    - Berechnung und Erläuterung des Zeitwertfaktors
    - Auswahl und Begründung des Gebrauchswertfaktors
- Verkehrswertberechnung
    - Begründung für die Auswahl des Verfahrens
    - Angaben zum ermittelten Verkehrswert und Ableitung und Begründung der Vergleichswerte

2.7.2 Zusätzlich in der IT-Forensic

- Erläuterung der Beweisführung und Plausibilisierung der Ergebnisse
- Eindeutige Verifizierung der relevanten Beweismittel (Name, Speicherpfad, Hashwert)

2.7.3 Zusätzlich in der IT-Security

- Begründung und Erläuterung der Feststellungen
- Begründung und Definition der Schutzbedarfsfeststellung
- Empfehlungen zur Erhöhung des Schutzbedarfs (nach Best-Practice)

2.8 Zusammenfassung des Gutachtens

Der Sachverständige hat nach dem Auftrag oder dem Beweisbeschluss seine Zusammenfassung zu formulieren und die Fragestellung zu beantworten.

Der Sachverständige muss davon ausgehen, dass immer zuerst die Zusammenfassung gelesen wird, da der Auftraggeber erst einmal an dem Ergebnis interessiert ist. Dies bedeutet, dass die Zusammenfassung kurz und knapp die wesentlichen und relevanten Ergebnisse des Gutachtens erläutert und zusammenfasst. Zur besseren Verständlichkeit wird die Fragestellung oder die Beweisfragen wiederholt und die dazu gehörenden Antworten daruntergeschrieben.

Inhalte einer Zusammenfassung:

- Kurze Beschreibung der Ausgangssituation und ggf. Informationen aus dem Ortstermin
- Wiederholung der Fragestellung / Beweisfragen
- Kurze, knappe und übersichtliche Antwort der Fragestellung / Beweisfragen

Erst wenn hier keine befriedigende Antwort gefunden wird, wird das Gutachten durch den Auftraggeber, bzw. Leser durchgearbeitet. Wobei es meist eine Partei gibt, die im Verfahren unterliegt und deren Prozessvertreter versucht das Gutachten auszuheben. Somit sollte jedes Wort genau im Ergebnis formuliert werden.

In der Zusammenfassung dürfen keine neuen Erkenntnisse oder Ergebnisse vorhanden sein, die nicht im eigentlichen Gutachten abgehandelt worden sind.

2.9 Schlussbemerkungen

In den Schlussbemerkungen (Schlussformel) sollte die Unbefangenheitserklärung, sowie die höchstpersönliche Gutachtenerstattung versichert werden.

Nach der Schlussformel hat der Sachverständige das Gutachten

- das Erstellungsdatum
- die eigenhändige Unterschrift und
- Stempel

zu setzen.

2.10 Anlagen zum Gutachten

Die Anlagen des Gutachtens sollen es dem Leser ermöglichen einen Zusammenhang zu anderen Punkten der Gutachtenerstattung zu erarbeiten.

Der Sachverständige hat als Anlage alle für die Bearbeitung des Sachverhalts notwendigen Unterlagen aufzuführen.

Ein Sachverständiger Dritter muss anhand der Unterlagen, das Gutachten mit den Feststellungen und dem Ergebnis nachvollziehen können.

3. KO-KRITERIEN FÜR EINZUREICHENDE ZULASSUNGSGUTACHTEN UND PRÜFUNGSGUTACHTEN

3.1 Fehlende Vollständigkeit (fehlen wesentlicher Teile)

- keine Auftragsbeschreibung
- fehlende Darstellung der Befund- und Anknüpfungstatsachen
- fehlende Unterschrift/Stempel

3.1.1 Zusätzlich bei der Wertermittlung

- keine Begründung des ausgewählten Verfahrens
- keine Begründung der betriebsgewöhnlichen Nutzungsdauer
- keine Begründung des Gebrauchswertfaktors

3.1.2 Zusätzlich in der IT-Forensic

- keine Beschreibung der forensischen Vorbereitungsmaßnahmen
- fehlende Angabe der sicheren Auswerteumgebung

3.1.3 Zusätzlich in der IT-Security

- keine Erläuterung des angewandten Verfahrens
- keine Erläuterung der Schutzziele

3.2 Grundlagenfehler

- unvollständige oder falsche Beantwortung der Fragstellung/Beweisfragen
- fehlende Begründung zur der Vorgehensmethode
- fehlende Offenlegung der Methodik (kein nachvollziehbarer und plausibler Lösungsweg)
- Rechenfehler oder falscher Rechenweg, falsche Analyseergebnisse
- wiederholte Rechenfehler, falsche Analysen
- fehlende Erläuterung der in den Verfahren herangezogenen Eingangsparameter

3.3 Mangelnde Sorgfaltspflichten

- mehrfach divergierende Angaben innerhalb des Gutachtens
- mangelhafte Rechtschreibung und Grammatik
- mangelhafter Stil oder Layout
  (z. B. keine Bindung, Pflichtangaben Gutachtendeckblatt)