Inhaltsverzeichnis

1. GELTUNGSBEREICH

Diese Prüfungsordnung gilt für die Prüfungen zum/zur:

— **EDV-Sachverständiger (Systeme und Anwendungen oder Systeme und Technik)**
— **IT-Forensic-Analyst Windows Betriebssysteme**
— **IT-Forensic-Analyst Mobile Device**
— **Sachverständiger IT-Forensic (lokale und mobile Systeme)**
— **IT-Security-Analyst Netzwerk und Internet**
— **Sachverständiger IT-Security (Netzwerk und Internet)**

gemäß DEKRA Standard die von der DEKRA Certification GmbH durchgeführt werden.

Diese Prüfungsordnung sowie die sonstigen vertraglichen Regelungen legen die objektiven Kriterien für die Zulassung von Teilnehmern zur Prüfung bzw. zum Zertifizierungsverfahren, fest. Alle Teilnehmer werden gleichermaßen an diesen objektiven Kriterien gemessen. Die Prüfung steht allen potentiellen Teilnehmern offen, die die Kriterien für die Zulassung erfüllen und einen entsprechenden Vertrag mit DEKRA Certification GmbH schließen.

Aus Gründen der besseren Lesbarkeit wird in der Prüfungsordnung davon abgesehen, die Funktionsbezeichnungen wie Prüfer oder Teilnehmer jeweils in der weiblichen und in der männlichen Form aufzuführen; es versteht sich von selbst, dass alle Funktionsbezeichnungen sowohl in der weiblichen als auch in der männlichen Form verwendet werden können.

2. ANMELDUNG UND ZULASSUNG DER PRÜFUNG

Die Anmeldung eines Teilnehmers zu einer Prüfung erfolgt über den Zertifizierungsantrag Prüfung/Zertifizierung im EDV/IT Bereich. Für die Teilnahme an einem Zertifizierungsverfahren müssen nachweislich nachstehende Zulassungsvoraussetzungen erfüllt werden:

2.1 EDV-Sachverständiger

2.1.1 Zulassungsvoraussetzung zur Prüfung EDV-Sachverständiger (Systeme und Anwendungen oder Systeme und Technik)

- einschlägiges, abgeschlossenes Studium (z. B. (Wirtschafts-)Informatik, Ingenieurstudiengang) und mindestens 3 Jahre einschlägige Berufserfahrung im Zertifizierungsbereich innerhalb der letzten 5 Jahre

oder

- abgeschlossene Berufsausbildung im Bereich EDV/IT (z. B. Informatiker, Informations- und Systemelektroniker) und mindestens 5 Jahre einschlägige Berufserfahrung im Zertifizierungsbereich innerhalb der letzten 8 Jahre

2.2 Fachbereich IT-Forensic

2.2.1 Zulassungsvoraussetzung zur Prüfung IT-Forensic-Analyst Windows Betriebssysteme

- einschlägiges, abgeschlossenes Studium (z. B. (Wirtschafts-)Informatik, Ingenieurstudiengang) und mindestens 3 Jahre einschlägige Berufserfahrung im Zertifizierungsbereich innerhalb der letzten 5 Jahre

oder

- abgeschlossene Berufsausbildung im Bereich EDV/IT (z. B. Informatiker, Informations- und Systemelektroniker) und mindestens 5 Jahre einschlägige Berufserfahrung im Zertifizierungsbereich innerhalb der letzten 8 Jahre

2.2.2 Zulassungsvoraussetzung zur Prüfung IT-Forensic-Analyst Mobile Device

Identische Zulassungsvoraussetzungen wie bei 2.2.

2.2.3 Zulassungsvoraussetzung zur Prüfung Sachverständiger IT-Forensic (lokale und mobile Systeme)

- einschlägiges, abgeschlossenes Studium (z. B. (Wirtschafts-)Informatik, Ingenieurstudiengang) und mindestens 5 Jahre einschlägige Berufserfahrung im Zertifizierungsbereich innerhalb der letzten 8 Jahre

oder

- abgeschlossene Berufsausbildung im Bereich EDV/IT (z. B. Informatiker, Informations- und Systemelektroniker) und mindestens 8 Jahre einschlägige Berufserfahrung im Zertifizierungsbereich innerhalb der letzten 10 Jahre

sowie

- Abschluss zum IT-Forensic Analyst Windows Betriebssysteme (Prüfungsteil 1) und IT-Forensic Analyst Mobile Device (Prüfungsteil 1) oder gleichwertige Nachweise.

2.3 Fachbereich IT-Security

2.3.1 Zulassungsvoraussetzung zur Prüfung IT-Security-Analyst

- einschlägiges, abgeschlossenes Studium (z. B. (Wirtschafts-)Informatik, Ingenieurstudiengang) und mindestens 3 Jahre einschlägige Berufserfahrung im Zertifizierungsbereich innerhalb der letzten 5 Jahre

oder

- abgeschlossene Berufsausbildung im Bereich EDV/IT (z. B. Informatiker, Informations- und Systemelektroniker) und mindestens 5 Jahre einschlägige Berufserfahrung im Zertifizierungsbereich innerhalb der letzten 8 Jahre

2.3.2 Zulassungsvoraussetzung zur Prüfung Sachverständiger IT-Security

- einschlägiges, abgeschlossenes Studium (z. B. (Wirtschafts-)Informatik, Ingenieurstudiengang) und mindestens 5 Jahre einschlägige Berufserfahrung im Zertifizierungsbereich innerhalb der letzten 8 Jahre

oder

- abgeschlossene Berufsausbildung im Bereich EDV/IT (z. B. Informatiker, Informations- und Systemelektroniker) und mindestens 8 Jahre einschlägige Berufserfahrung im Zertifizierungsbereich innerhalb der letzten 10 Jahre

sowie

- Abschluss zum IT-Security Analyst (Prüfungsteil 1) oder gleichwertige Nachweise

Teilnehmer müssen die entsprechende Ausbildungsreihe mit den Kompetenzen in **Anhang 1** (Kompentenzmatrix IT) beschriebenen Inhalten erfolgreich durchlaufen. Erfolgreich durchlaufen bedeutet, dass alle Prüfungen durch des Seminaranbieters bestanden werden. Die entsprechenden Nachweise oder gleichwertige Nachweise sind der Zertifizierungsstelle vorzulegen.

Die Zertifizierungsstelle prüft die Vollständigkeit der Anmeldeunterlagen sowie die Erfüllung der Zulassungsvoraussetzungen und entscheidet über eine Teilnahme bzw. Nicht-Teilnahme an der Prüfung bzw. Zertifizierungsverfahren.

3. DURCHFÜHRUNG DER PRÜFUNG

Die Prüfung umfasst generell zwei Prüfungsteile: einen schriftlichen **Teil 1** und einen praktischen **Teil 2** in Heimarbeit. Die Prüfungsfragen werden von der Zertifizierungsstelle zusammengestellt und umfassen die Themenkomplexe des entsprechenden Zertifizierungsabschlusses (Kompetenzmatrix IT und Mindestanforderungen IT- **Anhang 1-4**).

3.1 Prüfung EDV-Sachverständiger

Prüfungsteil 1:

- Schriftliche Prüfung (Hilfsmittel: Taschenrechner),
- Multiple Choice („MC“) Aufgaben und ggf. offene Aufgaben
- Dauer: 60 Min.

Teil 2: Erstellung eines Gutachtens (in Heimarbeit).
Der Teilnehmer erhält aus dem Pool von verschiedenen Fallstellungen eine Fallaufgabe. Das Gutachten zu dieser Fallaufgabe muss nach Abschluss der schriftlichen Prüfung (Teil 1) innerhalb von 8 Wochen bei DEKRA Certification zur Bewertung vorliegen (Datum des Poststempels). Später eingereichte Gutachten werden als nicht bestanden bewertet. Eine Fristverlängerung ist nur mit Vorlage eines ärztlichen Attests möglich. Bei der Erstellung des Gutachtens sind die Anforderungen des **Anhangs 2** (Mindestanforderungen IT an Gutachten) dieser Prüfungsordnung zu beachten.

3.2 Prüfung IT-Forensic-Analyst Windows Betriebssystem

Prüfungsteil 1:

- Schriftliche Prüfung (keine Hilfsmittel erlaubt),
- Multiple Choice („MC“) Aufgaben und ggf. offene Aufgaben
- Dauer: 45 Min.

Bei den MC-Aufgaben ist immer mindestens eine Antwort richtig. Bitte kreuzen Sie alle richtigen Antworten an. Jede richtige Antwort wird mit einem Punkt bewertet. Achtung! Bei einer Aufgabe wird für jedes falsch gesetzte Kreuz (Antwort) ein Punkt abgezogen. Bei den offenen Aufgaben werden jeweils maximal 5 Punkte je nach Erfüllungsgrad der Beantwortung vergeben.

Prüfungsteil 2:

Auswertung eines Datenträger-Images und Berichterstellung (in Heimarbeit).
Der Teilnehmer erhält eine Aufgabenerstellung und Datenträgerabbild (Image im e01-Format). Der Teilnehmer muss selbstständig eine Auswertung durchführen und innerhalb von 14 Tagen per (Post oder per E-Mail) einen forensischen Auswertebericht an die DEKRA Certification zur Bewertung einreichen. Bei der Erstellung des Auswerteberichts sind die Mindestanforderungen (Mindestanforderungen IT an Berichte) **Anhang 3** dieser Prüfungsordnung zu beachten.

Später eingehende Prüfungsleistungen werden als nicht bestanden gewertet. Eine Fristverlängerung ist nur mit Vorlage eines ärztlichen Attests möglich.

3.3 Prüfung IT-Forensic-Analyst Mobile Device

Prüfungsteil 1:

- Schriftliche Prüfung (keine Hilfsmittel erlaubt),
- Multiple Choice („MC“) Aufgaben und ggf. offene Aufgaben
- Dauer: 45 Min.

Bei den MC-Aufgaben ist immer mindestens eine Antwort richtig. Bitte kreuzen Sie alle richtigen Antworten an. Jede richtige Antwort wird mit einem Punkt bewertet. Achtung! Bei einer Aufgabe wird für jedes falsch gesetzte Kreuz (Antwort) ein Punkt abgezogen. Bei den offenen Aufgaben werden jeweils maximal 5 Punkte je nach Erfüllungsgrad der Beantwortung vergeben.

Prüfungsteil 2:

Auswertung eines Datenträger-Images und Berichterstellung (in Heimarbeit).
Der Teilnehmer erhält eine Aufgabenerstellung und Datenträgerabbild. Der Teilnehmer muss selbstständig eine Auswertung durchführen und innerhalb von 14 Tagen per (Post oder per E-Mail) einen forensischen Auswertebericht an die DEKRA Certification zur Bewertung einreichen. Bei der Erstellung des Auswerteberichts sind die Mindestanforderungen IT für Berichte (**Anhang 3)** dieser Prüfungsordnung zu beachten.

Später eingehende Prüfungsleistungen werden als nicht bestanden gewertet. Eine Fristverlängerung ist nur mit Vorlage eines ärztlichen Attests möglich.

3.4 Prüfung Sachverständiger IT-Forensic (lokale und mobile Systeme)

Die Prüfung besteht aus zwei Teilen.

Prüfungsteil 1:

- Schriftliche Prüfung (Taschenrechner als Hilfsmittel erlaubt),
- Multiple Choice („MC“) Aufgaben- und offene Aufgaben,
- Dauer: 75 Min.

Bei den MC-Aufgaben ist immer mindestens eine Antwort richtig. Bitte kreuzen Sie alle richtigen Antworten an. Jede richtige Antwort wird mit einem Punkt bewertet. Achtung! Bei einer Aufgabe wird für jedes falsch gesetzte Kreuz (Antwort) ein Punkt abgezogen. Bei den offenen Fragen werden je nach Erfüllungsgrad der Beantwortung die Punkte vergeben (maximal 5 Punkte/Frage).

Prüfungsteil 2:
Erstellung eines Gutachtens (in Heimarbeit). Der Teilnehmer erhält aus dem Pool von verschiedenen Fallstellungen eine Fallaufgabe. Das Gutachten zu dieser Fallaufgabe muss nach Abschluss der schriftlichen Prüfung (Teil 1) innerhalb von 8 Wochen bei DEKRA Certification zur Bewertung vorliegen (Datum des Poststempels). Bei der Erstellung des Gutachtens sind die Mindestanforderungen IT **Anhang 2** dieser Prüfungsordnung zu beachten.

Später eingereichte Gutachten werden als nicht bestanden bewertet. Eine Fristverlängerung ist nur mit Vorlage eines ärztlichen Attests möglich.

3.5 Prüfung IT-Security-Analyst

Prüfungsteil 1:

- Schriftliche Prüfung (keine Hilfsmittel erlaubt),
- Multiple Choice („MC“) Aufgaben und ggf. offene Aufgaben
- Dauer: 45 Min.

Bei den MC-Aufgaben ist immer mindestens eine Antwort richtig. Bitte kreuzen Sie alle richtigen Antworten an. Jede richtige Antwort wird mit einem Punkt bewertet. Achtung! Bei einer Aufgabe wird für jedes falsch gesetzte Kreuz (Antwort) ein Punkt abgezogen. Bei den offenen Aufgaben werden jeweils maximal 5 Punkte je nach Erfüllungsgrad der Beantwortung vergeben.

Prüfungsteil 2:
Planung und Durchführung einer Sicherheitsüberprüfung (in Heimarbeit). Der Teilnehmer erhält eine Aufgabenerstellung. Der Teilnehmer muss selbstständig eine Sicherheitsanalyse durchführen und den Bericht innerhalb von 14 Tagen per (Post oder per E-Mail) an die DEKRA Certification zur Bewertung einreichen. Bei der Erstellung des Berichtes zur Sicherheitsanalyse sind die Mindestanforderungen IT an Berichte (**Anhang 4)** dieser Prüfungsordnung zu beachten.

Später eingehende Prüfungsleistungen werden als nicht bestanden gewertet. Eine Fristverlängerung ist nur mit Vorlage eines ärztlichen Attests möglich.

3.5 Prüfung Sachverständiger IT-Security

Die Prüfung besteht aus zwei Teilen.

Prüfungsteil 1:

- Schriftliche Prüfung (Recht für Sachverständige und Sachverständigentätigkeit Security, Taschenrechner als Hilfsmittel erlaubt),
- Multiple Choice („MC“) - und offene Fragen,
- Dauer: 75 Min.

Bei den MC-Aufgaben ist immer mindestens eine Antwort richtig. Bitte kreuzen Sie alle richtigen Antworten an. Jede richtige Antwort wird mit einem Punkt bewertet. Achtung! Bei einer Aufgabe wird für jedes falsch gesetzte Kreuz (Antwort) ein Punkt abgezogen. Bei den offenen Fragen werden je nach Erfüllungsgrad der Beantwortung die Punkte vergeben (maximal 5 Punkte/Frage).

Prüfungsteil 2:
Erstellung eines Gutachtens (in Heimarbeit). Der Teilnehmer erhält aus dem Pool von verschiedenen Fallstellungen eine Fallaufgabe. Das Gutachten zu dieser Fallaufgabe muss nach Abschluss der schriftlichen Prüfung (Teil 1) innerhalb von 8 Wochen bei DEKRA Certification zur Bewertung vorliegen (Datum des Poststempels). Bei der Erstellung des Gutachtens sind die Mindestanforderungen IT (**Anhang 2)** dieser Prüfungsordnung zu beachten.

Später eingereichte Gutachten werden als nicht bestanden bewertet. Eine Fristverlängerung ist nur mit Vorlage eines ärztlichen Attests möglich.

4. BEWERTUNG

Die Auswertung und Bewertung der Prüfung erfolgt durch den/die beauftragten Prüfer und wird auf den Prüfungsunterlagen dokumentiert. Das Prüfungsergebnis und die Prüfungsunterlagen werden der Zertifizierungsstelle übermittelt und gegen geprüft.

Die Prüfung gilt als bestanden, wenn mindestens 66% der maximalen Punktzahl pro Prüfungsteil erreicht werden. Bei einem Prozentanteil kleiner 66% eines Prüfungsteils gilt die komplette Prüfung als nicht bestanden und der nicht bestanden Prüfungsteile muss komplett wiederholt werden.

5. WIEDERHOLUNGEN VON PRÜFUNGEN

Eine nichtbestandene Prüfung bzw. Prüfungsteil können nur einmal wiederholt werden. Sonderregelung auf schriftlichen Antrag.

Eine Wiederholungsprüfung muss innerhalb 60 Tage nach Zustellung des Zertifizierungsentscheids schriftlich beantragt werden. Die dabei einzuhaltenden Fristen zur Prüfungsdurchführung werden im Zertifizierungsentscheid mitgeteilt.

6. ERTEILUNG UND ENTZUG DES ZERTIFIKATS

Das Zertifizierungsgremium entscheidet in der Regel innerhalb von 3 bis 4 Wochen nach dem Prüfungstermin bzw. nach Abgabe der Heimarbeit über die Erteilung des Zertifikats. Weicht das Zertifizierungsgremium vom Votum des Prüfers ab, ist dies schriftlich zu begründen. Das Ergebnis wird den Prüfungsteilnehmern schriftlich mitgeteilt (Zertifizierungsentscheid).

Das Zertifikat hat eine Gültigkeitsdauer von 3 Jahren und wird in deutscher Sprache ausgestellt. Mit Erteilung des Zertifikats verpflichtet sich der zertifizierte Sachverständige, die Rechte und Pflichten (Kodex IT-Sachverständige und Analysten – Anhang 5) einzuhalten. Die Zertifikatsinhaber werden registriert und können auf schriftliche Anfrage veröffentlicht werden. Die Zertifizierungsstelle bleibt die alleinige Eigentümerin des Zertifikates und des ggf. vergebenen Siegels.

Weitere Regelungen zum Zertifizierungsentscheid sowie zur Nutzung und Entzug des Zertifikats sind in der AZB unter Punkt 4, 5, 6 ,7 und 8 festgelegt.

7. ÜBERWACHUNG

Die zertifizierte Person hat eigenverantwortlich ihren Kompetenzerhalt sicherzustellen. Die DEKRA Certification GmbH überwacht die Einhaltung der Nutzungsbedingungen für das Zertifikat und das Siegel. Dazu gehören – sofern im Gültigkeitszeitraum des Zertifikats eintretend – die Auswertung von Informationen von Aufsichtsbehörden, die Bewertung von Beschwerden und Informationen von interessierten Kreisen sowie von eingeleiteten rechtlichen Schritten in Bezug auf die zertifizierte Person.

8. RE-ZERTIFIZIERUNG / ZERTIFIKATSVERLÄNGERUNG

Das Zertifikat verliert nach Ablauf (Gültigkeit der Zertifizierung) seine Gültigkeit. Eine Re-Zertifizierung / Zertifikatsverlängerung kann zum Ende der Zertifikatsgültigkeit mittels Re-Zertifizierungsantrag **F-03S-17** (Download unter www.dekra-personenzertifizierung.de) bei DEKRA Certification GmbH beantragt werden. Voraussetzung für eine Re-Zertifizierung ist die positive Bewertung der eingereichten Nachweise (siehe **8.1** bis **8.6**) durch DERKA Certification GmbH. Bei der Antragsstellung sind folgende Fristen zu beachten:

1-ste Frist: Antrag auf Re-Zertifizierung:
Idealerweise wird die Re-Zertifizierung 2 Monate vor Zertifikatsablauf beantragt, spätestens jedoch 3 Monate nach Zertifikatsablauf muss der Antrag bei der DEKRA Certification GmbH eingehen (Datum des Poststempels). Später eingehende Anträge können nicht mehr berücksichtigt werden.

2-te Frist: Nachweise (Weiterbildung und 2 Gutachten / Berichte):
Idealerweise werden die Nachweise zusammen mit dem Antrag bei der DEKRA Certification GmbH eingereicht. Die Nachweise müssen jedoch vollständig bis spätestens 6 Monaten nach Zertifikatsablauf vorliegen (Datum des Poststempels). Später eingehende Nachweise können nicht mehr berücksichtigt werden.

Entsprechend der Zertifizierungsstufe sind folgende Nachweise einzureichen:

8.1 EDV-Sachverständiger

- 2 verschiedene Gutachten (entsprechend der Zertifizierungsstufe), die im Laufe der Zertifikatsgültigkeit durch den Antragsteller selbst ausgearbeitet und erstellt wurden

sowie

- Besuch geeigneter Fortbildungsveranstaltungen im Laufe der Zertifikatsgültigkeit und den Nachweis von mindestens 24 Weiterbildungspunkten (siehe Kodex – Anhang 5)

und

- die Entrichtung der Kosten für die Zertifikatsverlängerung

8.2 IT-Forensic-Analyst Windows Betriebssysteme

- 2 unterschiedliche IT-Forensic Berichte entsprechend der Zertifizierungsstufe die im Laufe der Zertifikatsgültigkeit durch den Antragsteller selbst ausgearbeitet und erstellt wurden

sowie

- Besuch geeigneter Fortbildungsveranstaltungen im Laufe der Zertifikatsgültigkeit und den Nachweis von mindestens 16 Weiterbildungspunkten (siehe Kodex – Anhang 5)

und

- die Entrichtung der Kosten für die Zertifikatsverlängerung

8.3 IT-Forensic-Analyst Mobile Device

- 2 unterschiedliche IT-Forensic Berichte entsprechend der Zertifizierungsstufe die im Laufe der Zertifikatsgültigkeit durch den Antragsteller selbst ausgearbeitet und erstellt wurden

sowie

- Besuch geeigneter Fortbildungsveranstaltungen im Laufe der Zertifikatsgültigkeit und den Nachweis von mindestens 16 Weiterbildungspunkten (siehe Kodex – Anhang 5)

und

- die Entrichtung der Kosten für die Zertifikatsverlängerung

8.4 Sachverständige IT-Forensic (lokale und mobile Systeme)

- 2 verschiedene Gutachten (entsprechend der Zertifizierungsstufe), die im Laufe der Zertifikatsgültigkeit durch den Antragsteller selbst ausgearbeitet und erstellt wurden

sowie

- Besuch geeigneter Fortbildungsveranstaltungen im Laufe der Zertifikatsgültigkeit und den Nachweis von mindestens 24 Weiterbildungspunkten (siehe Kodex – Anhang 5)

und

- die Entrichtung der Kosten für die Zertifikatsverlängerung

8.5. IT-Security-Analyst

- 2 unterschiedliche Berichte über IT-Sicherheitsanalysen die im Laufe der Zertifikatsgültigkeit durch den Antragsteller selbst ausgearbeitet und erstellt wurden

sowie

- Besuch geeigneter Fortbildungsveranstaltungen im Laufe der Zertifikatsgültigkeit und den Nachweis von mindestens 16 Weiterbildungspunkten (siehe Kodex – Anhang 5)

und

- die Entrichtung der Kosten für die Zertifikatsverlängerung

8.6 Sachverständige IT-Security (Netzwerk und Internet)

- 2 verschiedene Gutachten (entsprechend der Zertifizierungsstufe), die im Laufe der Zertifikatsgültigkeit durch den Antragsteller selbst ausgearbeitet und erstellt wurden

sowie

- Besuch geeigneter Fortbildungsveranstaltungen im Laufe der Zertifikatsgültigkeit und den Nachweis von mindestens 24 Weiterbildungspunkten (siehe Kodex – Anhang 5)

und

- die Entrichtung der Kosten für die Zertifikatsverlängerung.

9. PRÜFUNGSUNTERLAGEN

Alle Unterlagen zur Prüfung werden von der Zertifizierungsstelle elektronisch oder in Papierform archiviert aufbewahrt. Die Aufbewahrungsfrist beträgt 10 Jahre. DEKRA Certification GmbH und die an der Prüfung beteiligten Personen haben gegenüber Dritten über diese Unterlagen strikte Vertraulichkeit zu wahren.

10. PRÜFUNGSKOSTEN

10.1 Prüfungskosten EDV-Sachverständiger

	Preis zzgl. MwSt.	Preis inkl. MwSt.
Erst-Prüfung	575,00 EUR	684,25 EUR
Wiederholungsprüfungen		
Teil 1	195,00 EUR	232,05 EUR
Teil 2	255,00 EUR	303,45 EUR
Rezertifizierung	375,00 EUR	446,25 EUR

10.2 Prüfungskosten IT-Forensic-Analyst Windows Betriebssysteme

	Preis zzgl. MwSt.	Preis inkl. MwSt.
Erst-Prüfung	319,00 EUR	379,61 EUR
Wiederholungsprüfungen		
Teil 1	175,00 EUR	208,25 EUR
Teil 2	225,00 EUR	267,75 EUR
Rezertifizierung	219,00 EUR	260,61 EUR

10.3 Prüfungskosten IT-Forensic-Analyst Mobile Device

	Preis zzgl. MwSt.	Preis inkl. MwSt.
Erst-Prüfung	319,00 EUR	379,61 EUR
Wiederholungsprüfungen		
Teil 1	175,00 EUR	208,25 EUR
Teil 2	225,00 EUR	267,75 EUR
Rezertifizierung	219,00 EUR	260,61 EUR

10.4 Prüfungskosten Sachverständiger IT-Forensic (lokale und mobile Systeme)

	Preis zzgl. MwSt.	Preis inkl. MwSt.
Erst-Prüfung mit gültigen DEKRA-Zertifikat	695,00 EUR 619,00 EUR	827,05 EUR 736,61 EUR
Wiederholungsprüfungen		
Teil 1	175,00 EUR	208,25 EUR
Teil 2	255,00 EUR	303,45 EUR
Rezertifizierung	475,00 EUR	565,25 EUR

10.5 Prüfungskosten IT-Security-Analyst (Netzwerke und Internet)

	Preis zzgl. MwSt.	Preis inkl. MwSt.
Erst-Prüfung	319,00 EUR	379,61 EUR
Wiederholungsprüfungen		
Teil 1	175,00 EUR	208,25 EUR
Teil 2	225,00 EUR	267,75 EUR
Rezertifizierung	219,00 EUR	260,61 EUR

10.6 Prüfungskosten Sachverständiger IT-Security (Netzwerk und Internet)

	Preis zzgl. MwSt.	Preis inkl. MwSt.
Erst-Prüfung	695,00 EUR	827,05 EUR
mit gültigen DEKRA-Zertifikat	619,00 EUR	736,61 EUR
Wiederholungsprüfungen		
Teil 1	175,00 EUR	208,25 EUR
Teil 2	255,00 EUR	303,45 EUR
Rezertifizierung	475,00 EUR	565,25 EUR

11. ÄNDERUNGSDIENST

Der Teilnehmer bzw. die zertifizierte Person hat sich laufend eigenverantwortlich über Änderungen an den für den Zertifizierungsprozess relevanten Verfahren, Beschreibungen, Dokumenten und Formularen zu informieren. Die aktuellen Unterlagen sind auf der Website der DEKRA Certification GmbH erhältlich.

Stand: 08/2019

ANHANG 1 – KOMPETENZMATRIX IT

- Siehe www.dekra-personenzertifizierung.de

ANHANG 2 – MINDESTANFORDERUNGEN AN IT-GUTACHTEN

- Siehe www.dekra-personenzertifizierung.de

ANHANG 3 – MINDESTANFORDERUNGEN AN IT-FORENSIK-BERICHTE

- **Formalia**
  Der Auswertebericht muss u. a. Angaben zum Auswerter/Analysten (Titelseite), Auftraggeber, Geschäftszeichen, Untersuchungszeitraum, Anzahl der Ausfertigungen, Auftrag, Untersuchungsgegenstand, eingesetzte Hard- und Software, IT-forensische Vorgehensmethode, Verifizierungsmaßnahmen, Anlagen und Originalunterschrift enthalten.

  Der Bericht muss gut lesbar sein, sowie einwandfreie Rechtschreibung und Grammatik aufweisen. Der Bericht ist in einem repräsentativen Layout zu halten.

- **Ziel, Aufgabe**
  Aus dem Bericht muss klar die Beantwortung der Fragen und die Grundsätze einer IT-forensischen Beweissicherung hervorgehen.

- **Vorgehensweise**
  Im Bericht sind kurze Ausführungen zur Arbeitsplatzumgebung (Laborsituation), sowie die Nennung von entsprechend eingesetzten Hard- und Software-Tools zu treffen.

- **Feststellungen**
  Der Bericht muss eindeutige Aussagen treffen zum vorliegenden Untersuchungsgegenstand (Beweismittel).

- **Aussagen**
  Im Bericht zu nennen sind Ergebnisse mit Angabe des
  - Dateinamen
  - Speicherpfad
  - Prüfsumme (Hashwert – mind. MD5)

- **Schlussbemerkungen**
  Der Bericht muss Schlussbemerkungen zu der Archivierung, Verbleib von Sicherungskopien, sowie die Originalunterschrift des Analysten enthalten.

ANHANG 4 – MINDESTANFORDERUNGEN AN IT-SECURITY-BERICHTE

- **Formalia**
  Der IT-Security Bericht muss u. a. Angaben zum Auswerter/Analysten (Titelseite), Auftraggeber, Geschäftszeichen, Untersuchungszeitraum, Anzahl der Ausfertigungen, Auftrag, Untersuchungsgegenstand, eingesetzte Hard- und Software, Anlagen und Originalunterschrift enthalten.

  Der Bericht muss gut lesbar sein, sowie einwandfreie Rechtschreibung und Grammatik aufweisen. Der Bericht ist in einem repräsentativen Layout zu halten.

- **Ziel, Aufgabe**
  Aus dem Bericht müssen klar die Beantwortung der Fragen und die genaue Dokumentation der aufgefundenen Schwachstellen hervorgehen.

- **Vorgehensweise**
  Im Bericht sind kurze Ausführungen zur Arbeitsplatzumgebung (Laborsituation), sowie die Nennung von entsprechend eingesetzten Hard- und Software-Tools zu treffen.

- **Feststellungen**
  Der Bericht muss eindeutige Aussagen treffen zum vorliegenden Untersuchungsgegenstand (Netzwerk oder Internet) und die Rohergebnisse geordnet und systematisch darstellen.

- **Aussagen**
  Im Bericht zu nennen sind Ergebnisse mit Angabe des
  - Schwachstelle
  - Schritt-für-Schritt-Beschreibung

- **Schlussbemerkungen**
  Der Bericht muss Schlussbemerkungen, wie Verschwiegenheitserklärung, Verbleib von Aufzeichnungen, sowie die Originalunterschrift des Analysten enthalten.

ANHANG 5 – KODEX IT-SACHVERSTÄNDIGE UND ANALYSTEN

1. Persönliche Eignung

Der Sachverständige muss persönlich zuverlässig sein. Dies erfordert insbesondere, dass

- er in geordneten wirtschaftlichen Verhältnissen lebt;
- er nicht vorbestraft ist;
- er die Gewähr für die Einhaltung der Pflichten gemäß den Zertifizierungsbedingungen bietet;
- er als angestellter Sachverständiger vom Arbeitgeber oder Dienstherren eine schriftliche Bestätigung vorlegt, dass er seine Tätigkeit eigenverantwortlich, weisungsfrei, und persönlich ausüben kann; ins- besondere muss ihm die Unterschriftsleistung im Rahmen der Nummer 6 zugestanden werden,
- er über die für die ordnungsgemäße Ausübung seiner Tätigkeit erforderlichen Einrichtungen verfügt.

2. Gewissenhaftigkeit

Jeder Auftrag ist mit der Sorgfalt eines ordentlichen Sachverständigen zu erledigen. Dabei muss der aktuelle Stand von Wissenschaft, Technik und Praxiserfahrung zugrunde gelegt werden. Die tatsächlichen Grundlagen für gutachterliche Aussagen sind sorgfältig zu ermitteln. Die Gutachten müssen systematisch aufgebaut, übersichtlich gegliedert, nachvollziehbar begründet und auf das Wesentliche konzentriert werden. Kommen für die Beantwortung der gestellten Fragen mehrere Lösungen ernsthaft in Betracht, so hat der Sachverständige diese darzulegen und gegeneinander abzuwägen. Sofern Mindestanforderungen für gutachterliche Leistungen im Zertifizierungsgebiet vorliegen, hat er diese anzuwenden.

3. Unabhängigkeit

Der Sachverständige darf bei der Erbringung seiner Leistungen keiner Einflussnahme ausgesetzt sein, die geeignet ist, seine tatsächlichen Feststellungen, Bewertungen und Schlussfolgerungen so zu beeinträchtigen, dass die gebotene Objektivität und Glaubwürdigkeit seiner Aussagen nicht mehr gewährleistet sind. Insbesondere hat der Sachverständige zu gewährleisten, dass er seine gutachtlichen Leistungen ohne Rücksicht auf das Auftragsvolumen oder die geschäftlichen Beziehungen zu einem einzelnen Auftraggeber (wirtschaftliche Unabhängigkeit) und ohne Rücksicht auf Ergebniswünsche des Auftraggebers (persönliche Unabhängigkeit) erbringt.

4. Unparteilichkeit

Der Sachverständige hat seine Leistungen stets so zu erbringen, dass er sich weder in Gerichtsverfahren noch bei Privataufträgen dem Vorwurf der Besorgnis der Befangenheit aussetzt. Er hat bei der Erstellung des Gutachtens strikte Neutralität zu wahren, muss die gestellten Fragen objektiv und unvoreingenommen beantworten und darf in Gerichtsverfahren

nicht mit den Prozessparteien und bei Privatauftrag nicht mit den Auftraggebern verwandt oder verschwägert sein. Auf Umstände, die geeignet sind, Misstrauen gegen seine Unparteilichkeit zu begründen, hat er seinen Auftraggeber vor Auftragsübernahme hinzuweisen.

Treten nach Auftragsübernahme derartige Umstände ein, so hat er seinen Auftraggeber unverzüglich davon in Kenntnis zu setzen.

5. Weisungsfreiheit

Dem Sachverständigen ist es untersagt, Weisungen entgegenzunehmen, die das Ergebnis seiner Sachverständigentätigkeit verfälschen können.

6. Persönliche Aufgabenerledigung

Der Sachverständige hat die von ihm angeforderten Leistungen unter Anwendung der ihm zuerkannten Sachkunde in eigener Person zu erbringen. Hilfskräfte darf er bei Gerichtsaufträgen nur zur Vorbereitung des Gutachtens und insgesamt nur insoweit beschäftigen, als er ihre Mitarbeit ordnungsgemäß überwachen kann; den Umfang ihrer Tätigkeit hat er im Gutachten kenntlich zu machen. Die vom Sachverständigen auf diese Weise erstellten Gutachten darf nur er alleine unterschreiben; mithin darf weder die Unterschrift der Hilfskraft noch diejenige des Arbeitgebers oder Dienstherrn unter dem Gutachten angebracht werden.

Wenn ein zertifizierter Sachverständiger ein Gemeinschaftsgutachten (ein Gutachten mit einem oder mehreren sachverständigen aus demselben oder einem fremden Sachbereich) fertigt und mitunterschreibt, so müssen im Gutachten die Teile eindeutig benannt sein, deren Erarbeitung durch ihn erfolgten.

7. Schweigepflicht

Dem Sachverständigen ist es untersagt, Kenntnisse, welche er bei der Ausübung seiner Tätigkeit als zertifizierter Sachverständiger erlangt hat, Dritten unbefugt mitzuteilen oder zum Schaden anderer oder zu seinem oder zum Nutzen anderer unbefugt zu verwerten. Der Sachverständige hat auch seine Mitarbeiter zur Beachtung der Schweigepflicht anzuhalten.
Die Schweigepflicht des Sachverständigen und seiner Mitarbeiter besteht über die Beendigung des Auftragsverhältnisses hinaus; sie gilt auch nach Erlöschen der Zertifizierung. Die Schweigepflicht des Sachverständigen erstreckt sich nicht auf die Anzeige- und Auskunftspflichten nach den Ziffern 12 und 13.

8. Pflicht zur Fortbildung und ggf. zum Erfahrungsaustausch

Der Sachverständige ist verpflichtet sich nachweisbar auf dem Sachgebiet, auf dem er zertifiziert ist, im erforderlichen Umfang ständig fortzubilden. Der Schwerpunkt soll auf der fachspezifischen Fortbildung liegen.

Für die nachgewiesene Fortbildung erhält der Sachverständige Punkte nach dem folgenden Schlüssel. Eine Unterrichtseinheit (UE) wird mit je 45 Minuten angerechnet.

Hierbei wird unterschieden zwischen

- Präsenzveranstaltungen, Webinaren (Live-Webinar, indem ein Dozent/Referenten einen Vortrag hält und Teilnehmer die Möglichkeit haben aktiv Fragen stellen können);
- Online-Seminare (selbstständige Weiterbildung über Internetportale, welche nicht aktiv durch einen Dozenten/Referenten geführt werden);
- Fachvorträge (Veranstaltungen mit Themenschwerpunkten, Workshops und/oder Kurzvorträgen);
- Fachliteratur (CD, DVDs, Online-Kurse, Webinare – ohne Teilnahmebescheinigung)

Dauer von Präsenzveranstaltungen und Webinaren (mit Teilnahmebescheinigung)	**Anzahl der zu erwerbenden Fortbildungspunkte**
2-4 UE	2 Punkte
4-7 UE	4 Punkte
ab 8 UE	8 Punkte
für jeden weiteren Tag	8 Punkte
Online-Seminare (mit Teilnahmebescheinigung)	**Anzahl der zu erwerbenden Fortbildungspunkte**
1-2 UE	1 Punkt
3-4 UE	2 Punkte
5-7 UE	4 Punkte
ab 8 UE	8 Punkte
Fachvorträge (mit Teilnahmebescheinigung)	**Anzahl der zu erwerbenden Fortbildungspunkte**
ab 2 UE	2 Punkte
Fachliteratur, Online-Kurse, Webinare (ohne Teilnahmebescheinigung)	**Anzahl der zu erwerbenden Fortbildungspunkte**
pro Kurs / Literatur	1 Punkt

Darüber hinaus vergibt die Zertifizierungsstelle für Veranstaltungen oder Tätigkeiten, die besonders qualifiziert sind, weitere Fortbildungspunkte.

Innerhalb des Zertifikatszeitraums (3 Jahre) müssen Sachverständige mindestens 24 Fortbildungspunkte, Analysten mindestens 16 Fortbildungspunkte erworben haben.

9. Haftung und Versicherung

Für die Richtigkeit und Vollständigkeit seiner Aufgabenerfüllung hat der Sachverständige die volle Verantwortung zu übernehmen. Ein Haftungsausschluss oder eine Haftungseinschränkung ist nur für die Fälle einfacher Fahrlässigkeit in Form einer einzelvertraglichen Vereinbarung zulässig.

Der Sachverständige trägt für die Tätigkeit seiner Mitarbeiter die volle Verantwortung. Er muss daher seine Mitarbeiter hinsichtlich ihrer fachlichen Eignung und persönlichen Zuverlässigkeit sorgfältig auswählen, einweisen, anleiten, überwachen und fortbilden. Art, Inhalt und Umfang der Pflicht zur Überwachung und Anweisung der Hilfskräfte im Einzelfall bestimmen sich nach dem Maß ihrer Sachkunde und Erfahrung sowie der Gegebenheiten und Schwierigkeiten des konkreten Gutachtenauftrags. Für dieses Haftungsrisiko hat der Sachverständige eine Berufshaftpflichtversicherung in angemessenem Umfang abzuschließen und während der Dauer seiner Zertifizierung aufrechtzuerhalten. Steht der Sachverständige in einem Angestelltenverhältnis, genügt eine entsprechende Haftungsabsicherung durch den Arbeitgeber.

10. Zertifikats- und Siegelnutzung, Bekanntmachung, Werbung

- Der Sachverständige ist berechtigt, im Rahmen seiner Zertifizierungstätigkeit auf Briefbogen, auf Drucksachen und in Werbeanzeigen auf die Zertifizierung hinzuweisen und unter das Gutachten das die Zertifizierung ausweisende Siegel zu setzen. Bei Abbildungen der Zertifizierungsurkunde muss diese vollständig dargestellt werden. Eine Verkleinerung der Urkunde darf nur insoweit erfolgen, als ihr Inhalt noch lesbar ist.

- Als zertifizierter Sachverständiger darf er nur in den Fällen auftreten, in welchen er auf dem Zertifizierungsgebiet gutachterliche Tätigkeiten erbringt. Der Sachverständige ist daher verpflichtet, bei Sachverständigenleistungen auf anderen Sachgebieten oder bei Leistungen im Rahmen seiner sonstigen beruflichen oder gewerblichen Tätigkeit jedweden Hinweis auf die Zertifizierung sowie die Nutzung des die Zertifizierung ausweisenden Siegels zu unterlassen.

- Der Sachverständige hat zu dulden, dass seine Zertifizierung, sein Sachgebiet, sein Name und seine Anschrift von der Zertifizierungsstelle gespeichert und in Listen oder auf sonstigen Datenträgern veröffentlicht und auf Anfrage jedermann zur Verfügung gestellt wird.

- Werbliche Hinweise des Sachverständigen auf seine Tätigkeit müssen sich in Inhalt und Aufmachung an den Vorgaben des Gesetzes gegen den unlauteren Wettbewerb orientieren. Der Hinweis auf seine Zertifizierung hat dabei unter der Angabe des Sachgebiets, der Zertifizierungsstelle und der Zertifizierungsnorm (soweit vorhanden) zu erfolgen.

11. Aufzeichnungs- und Aufbewahrungspflichten

Der Sachverständige hat über jede von ihm angeforderte Leistung Aufzeichnungen zu machen. Aus diesen müssen ersichtlich sein:

- der Name des Auftraggebers- der Tag der Auftragserteilung
- der Gegenstand des Auftrags- der Tag, an dem die Leistung erbracht wurde oder die Gründe, aus denen sie nicht erbracht worden ist

- Beanstandungen an der Tätigkeit des Sachverständigen und
- Beschwerden über den Inhalt und das Ergebnis der gutachterlichen Leistung.

Der Sachverständige ist verpflichtet, die vorgenannten Aufzeichnungen sowie eins vollständigen Exemplars seines Gutachtens oder Prüfberichts 10 Jahre lang aufzubewahren.

12. Anzeigepflichten

Der Sachverständige hat der Zertifizierungsstelle unverzüglich anzuzeigen:

- die Änderung seiner Büroanschrift
- die Änderung seiner Privatadresse
- die Änderung seiner beruflichen Betätigungsform (z. B. Sozietät, Angestelltenverhältnis)
- den Verlust des Zertifikats oder des die Zertifizierung ausweisenden Stempels
- die Leistung einer eidesstattlichen Versicherung nach § 807 ZPO - die Stellung eines Insolvenzantrags
- die Einleitung eines staatsanwaltlichen Ermittlungsverfahrens
- die rechtskräftige Verurteilung in einem Strafverfahren
- eine andere Berufszulassung, eine staatliche Anerkennung oder eine öffentliche Bestellung bzw. deren Widerruf.

13. Auskunftspflichten, Überlassung von Unterlagen und Duldung der Nachschau

Der Sachverständige hat der Zertifizierungsstelle auf deren Verlangen jederzeit die zur Überwachung seiner Tätigkeit und der Einhaltung seiner Pflichten erforderlichen mündlichen und schriftlichen Auskünfte innerhalb der gesetzten Frist unentgeltlich zu erteilen und die angeforderten Unterlagen vorzulegen. Er kann die Auskunft auf solche Fragen verweigern, deren Beantwortung ihn selbst oder einen seiner Angehörigen (§ 52 StPO) der Gefahr strafgerichtlicher Verfolgung oder eines Verfahrens nach dem OWiG aussetzen würde.

Der Sachverständige hat auf Verlangen der Zertifizierungsstelle die aufbewahrungspflichtigen Unter- lagen (vgl. Nr. 11) vorzulegen und eine angemessene Zeit zwecks Überprüfung zu überlassen. Die Zertifizierungsstelle hat in diesem Zusammenhang sicherzustellen, dass die Vorschriften des Datenschutzes und der in Nr. 7 geregelten Schweigepflicht eingehalten werden. Die Beauftragten der Zertifizierungsstelle können auch während der üblichen Geschäftszeit die Geschäftsräume des Sachverständigen betreten und durch Stichproben von Unter- lagen und Akten prüfen, ob der Sachverständige seinen Pflichten nachgekommen ist.

14. Rückgabepflicht von Zertifikat und Siegel

Der Sachverständige hat nach Erlöschen der Zertifizierung das Zertifikat und das die Zertifizierung ausweisende Siegel unverzüglich der Zertifizierungsstelle zurückzugeben.

Personen im Angestelltenverhältnis
Die vorstehenden Rechte und Pflichten sind von Personen im Angestelltenverhältnis bei Bewertungstätigkeiten im Auftrage ihrer Dienstherren sinngemäß anzuwenden.

Stand 08/2019