

Leitfaden zum Personenzertifizierungsprogramm
Datenschutzpersonal (TÜV®)
gemäß DSGVO und BDSG-neu

1. Allgemein	3
2. Anwendungsbereich	3
3. Empfohlene Vorkenntnisse	4
4. Voraussetzung für die Zertifikatserteilung	4
5. Prüfungsgegenstand und Prüfungshilfsmittel	5
6. Prüfungsübersicht	5
7. Schriftliche Präsenzprüfung	6
8. Schriftliche Online-Prüfung	7
9. Mündliche Prüfung	7
10. Gesamtbewertung	8
11. Zertifizierungsentscheidung und Zertifikatserteilung	8
12. Gültigkeit der Personenzertifikate	9
13. Anforderungen an die Rezertifizierung	9
14. Mitgeltende Unterlagen	10
15. Anlage 1: Themen des Lehrgangs und Prüfungsmodalitäten der schriftlichen Prüfung Datenschutzbeauftragter (TÜV®)	11
16. Anlage 2: Themen des Lehrgangs und Prüfungsmodalitäten der schriftlichen Prüfung Datenschutzauditor (TÜV®)	17
17. Anlage 2b: Themen des Lehrgangs und Prüfungsmodalitäten der mündlichen Prüfung Datenschutzauditor (TÜV®)	21

Guideline for the Certification Scheme of Persons
Data protection personnel (TÜV®)
according to DSGVO and BDSG-neu

1. General information	3
2. Scope	3
3. Recommended prior knowledge	4
4. Requirements for the granting of the certificate	4
5. Subject of examination and aids permitted for an exam	5
6. Overview of Examination	5
7. Written face-to-face examination	6
8. Written live-online examination	7
9. Oral examination	7
10. Overall evaluation	8
11. Certification and certificate issuance	8
12. Validity of certifications of persons	9
13. Requirements for recertification	9
14. Applicable documents	10
15. Annex 1: Topics of the course and examination modalities of the written examination Data Protection Officer (TÜV®)	14
16. Annex 2: Topics of the course and examination modalities of the written examination Data Protection Auditor (TÜV®)	19
17. Annex 2b: Topics of the course and examination modalities of the oral/practical examination Data Protection Auditor (TÜV®)	21

TÜV NORD CERT – Personal certification

Herausgeber und Eigentümer:

TÜV NORD CERT GmbH

Zertifizierungsstelle für Personen

Am TÜV 1

45307 Essen

E-Mail: TNCERT-PZ@tuev-nord.de / perszert@tuev-nord.de

Rev. 11

Status: freigegeben / released, BM 27.10.2025

Gültig ab: 01.01.2026

Publisher and owner:

TÜV NORD CERT GmbH

Certification body of persons

Am TÜV 1

45307 Essen

E-mail: TNCERT-PZ@tuev-nord.de / perszert@tuev-nord.de

Rev. 11

Status: freigegeben / released, BM 27.10.2025

Valid from: 01/01/2026

Leitfaden zum Personenzertifizierungsprogramm

Datenschutzpersonal (TÜV®)

gemäß DSGVO und BDSG-neu

1. Allgemein

Das BDSG-neu (Bundesdatenschutzgesetz-neu) regelt in § 38 die Bestellung von Datenschutzbeauftragten. Das Gesetz verlangt die angemessene Fachkunde und Zuverlässigkeit für die Erfüllung der Aufgaben als Datenschutzbeauftragter.

Durch den Umgang mit personenbezogenen Daten können die verfassungsrechtlich geschützten Persönlichkeitsrechte dieser Personen beeinträchtigt werden. Der Datenschutz wirkt dem entgegen. Auf welche Weise dies zu geschehen hat, legen das BDSG-neu, die DSGVO (Datenschutzgrundverordnung) und die weiteren Bestandteile des Datenschutzrechts fest.

Der Datenschutzbeauftragte ist Teil des wirksamen Datenschutzes, indem er als Vermittler und Berater zwischen Management, Betroffenen, Betriebsrat, Mitarbeitern und Aufsichtsbehörde tätig ist.

Mithilfe von Datenschutzaudits lässt sich die Einhaltung der DSGVO und des BDSG-neu überprüfen. Neben einer Kontrolle der rechtlichen Anforderungen müssen auch organisatorische Regelungen und technische Aspekte überprüft werden, um den Datenschutz im Betrieb zu gewährleisten.

2. Anwendungsbereich

Dieser Leitfaden gilt für alle Zertifizierungsverfahren zum Erlangen des Personenzertifikats Datenschutzbeauftragter (TÜV) und Datenschutzauditor (TÜV) im Rahmen von anerkannten Lehrgängen. Die Lehrgänge können sowohl als Präsenzschulung, Blended Learning als auch Online anerkannt sein.

Guideline for the Certification Scheme for persons

Data protection personnel (TÜV®)

according to DSGVO and BDSG-neu

1. General information

Section 38 of the BDSG-neu (Federal Data Protection Act-new) regulates the appointment of data protection officers. The law requires appropriate expertise and reliability to fulfil the duties of a data protection officer.

The constitutionally protected personal rights of these persons can be impaired by the handling of personal data. Data protection counteracts this. The BDSG-neu, the GDPR (General Data Protection Regulation) and the other components of data protection law stipulate how this must be done.

The data protection officer is part of effective data protection by acting as a mediator and advisor between management, data subjects, the works council, employees and the supervisory authority.

Data protection audits can be used to check compliance with the GDPR and the new BDSG. In addition to checking the legal requirements, organizational regulations and technical aspects must also be reviewed in order to ensure data protection in the company.

2. Scope

This guideline applies to all certifications for obtaining the personal certificate Data Protection Officer (TÜV) and Data protection auditor (TÜV) within the scope of recognized training courses. The courses can be recognized as face-to-face training, blended learning or live-online training.

3. Empfohlene Vorkenntnisse

	Ausbildung / ersatzweise Berufserfahrung für fehlende Ausbildung	Zusätzliche Berufserfahrung
Datenschutzbeauftragter (TÜV)	Abgeschlossene Berufsausbildung oder vergleichbarer Abschluss	2 Jahre
Datenschutzauditor (TÜV)	Abgeschlossene Berufsausbildung oder vergleichbarer Abschluss	2 Jahre

Die empfohlenen Vorkenntnisse müssen nicht nachgewiesen werden, sind aber für die Teilnahme an Schulung und Prüfung sinnvoll.

4. Voraussetzung für die Zertifikatserteilung

	Bestandene Prüfung	Schulung im Zertifizierungsgebiet
Datenschutzbeauftragter (TÜV)		fachbezogener Lehrgang mit mind. 32 UE* und erfolgreichem Abschluss*
Datenschutzauditor (TÜV)	zum Datenschutzbeauftragten (TÜV)	fachbezogener Lehrgang mit mind. 24 UE* und erfolgreichem Abschluss

Hinweise zur Tabelle:

- *1 UE entspricht einer Unterrichtseinheit von 45 Minuten.
- „Erfolgreicher Abschluss“ bedeutet das Bestehen der zum Lehrgang bzw. zur Zertifizierung gehörenden Abschlussprüfung gemäß diesem Personenzertifizierungsprogramm.

Die Erfüllung der Anforderungen muss durch objektive Nachweise bestätigt werden.

3. Recommended prior knowledge

	training / alternatively work experience for lack of education	Additional work experience
Data Protection Officer (TÜV)	completed professional training / equivalent	2 years
Data Protection Auditor (TÜV)	completed professional training / equivalent	2 years

The recommended prior knowledge does not have to be proven but is useful for participation in the training and examination.

4. Requirements for the granting of the certificate

	Passed Exam	Training in area of certification
Data Protection Officer (TÜV)		specialized training with at least 32 TU* and successful completion
Data Protection Auditor (TÜV)	Data Protection Officer (TÜV)	specialized training with at least 24 TU* and successful completion

Notes on the table:

- *1 TU corresponds to a teaching unit of 45 minutes.
- “Successful completion” means passing the final examination associated with the course or certification in accordance with this certification scheme.

The fulfilment of the requirements must be confirmed by objective evidence.

5. Prüfungsgegenstand und Prüfungshilfsmittel

Die Präsenzprüfungen nach Präsenzlehrgängen finden in der Regel am letzten Lehrgangstag oder am Tag nach dem letzten Lehrgangstag am Ort des Lehrgangs statt.

Für Online-Prüfungen werden entsprechende separate Termine angeboten.

Aktuelle technische Voraussetzungen finden sich unter folgendem Link: [FAQ - Personenzertifizierung I TÜV NORD](#)

Als Hilfsmittel sind in der Prüfung Datenschutzbeauftragter (TÜV) Lehrgangsunterlagen, Lehrbücher, die relevanten normativen Dokumente sowie eigene Aufzeichnungen in Papierform zugelassen. Die Nutzung digitaler Unterlagen ist nicht gestattet. Bei Bedarf sind Taschenrechner erlaubt, andere elektronische Hilfsmittel sind nicht zulässig.

Als Hilfsmittel sind in der Prüfung Datenschutzauditor (TÜV) nur die relevanten Rechtstexte in Papierform zugelassen. Die Nutzung digitaler Unterlagen ist nicht gestattet. Bei Bedarf sind Taschenrechner erlaubt, andere elektronische Hilfsmittel sind nicht zulässig.

6. Prüfungsübersicht

Prüfung Datenschutzbeauftragter (TÜV)	schriftlich:
Dauer:	75 min.
Anzahl der Prüfungsaufgaben gesamt:	40
MC-Aufgaben:	40
Offene Aufgaben:	
Höchstpunktzahl:	40
Mindestpunktzahl:	24 (60 %)

5. Subject of examination and aids permitted for an exam

The face-to-face examination following face-to-face training usually take place on the last day of the course or on the day after the last day of the course at the location of the course.

Live-online examinations are offered with individual dates and timings.

Current technical requirements can be found under the following link: [FAQ - Personenzertifizierung I TÜV NORD](#)

Course materials, textbooks, the relevant legal texts, and the candidate's own notes in paper form are permitted as auxiliary means in the Data Protection Officer (TÜV) examination. The use of digital documents is not permitted. If required, calculators are permitted; other electronic means are not allowed.

Only the relevant legal texts in paper form are permitted as auxiliary means in the Data Protection Auditor (TÜV) examination. The use of digital documents is not permitted. If required, calculators are permitted; other electronic means are not allowed.

6. Overview of Examination

Examination Data Protection Officer (TÜV)	written:
Duration:	75 min.
Total number of examination questions:	40
MC tasks:	40
Open tasks:	
Maximum score:	40
Minimum score:	24 (60 %)

Prüfung Datenschutzauditor (TÜV)	schriftlich:	mündlich:
Dauer:	75 min.	60 min: 30 min. Vorbereitung 10-15 min. Prüfung je Kandidat
Anzahl der Prüfungsaufgaben gesamt:	21	
MC-Aufgaben:	20	
Offene Aufgaben / Dokumentenprüfung:	0 / 1	
Höchstpunktzahl:	40	15
Mindestpunktzahl:	24 (60 %)	9 (60 %)

Details s. Anlagen

7. Schriftliche Präsenzprüfung

Die Prüfungsaufgaben sind in deutscher Sprache gestellt. Die Prüfungsaufgaben werden in einem separaten Aufgabenheft vorgelegt. Die Lösungen zu jeder Prüfungsaufgabe werden auf den Seiten des Einzelberichts eingetragen. Nur die Antworten auf dem Einzelbericht werden gewertet.

Die MC-Aufgaben sind im Singular formuliert, sodass ein Rückschluss auf die Anzahl der richtigen Lösungen nicht möglich ist. Es muss unter mehreren vorgegebenen Auswahlmöglichkeiten durch Ankreuzen jede richtige Lösung ausgewählt werden. Es können eine, mehrere oder alle Auswahlmöglichkeiten richtig sein. Für jede richtig beantwortete MC-Aufgabe gibt es einen Punkt. Eine Aufgabe ist richtig gelöst, wenn die Kreuze an den richtigen Stellen der Tabelle gesetzt sind. Gar nicht oder nicht vollständig richtig gelöste Aufgaben erhalten null Punkte. Es gibt keine Bruchteile von Punkten.

Examination Data Protection Auditor (TÜV)	written:	oral:
Duration:	75 min.	60 min: 30 min. preparation 10-15 min. examination per candidate
Total number of examination questions:	21	
MC tasks:	20	
Open tasks / document review:	0 / 1	
Maximum score:	40	15
Minimum score:	24 (60 %)	9 (60 %)

Details see attachment

7. Written face-to-face examination

The examination questions are set in German. The examination questions are presented in a separate question booklet. The candidate enters the solutions to each examination question on the pages of the individual report. Only the answers on the individual report will be scored.

The MC questions are formulated in the singular, so it is not possible to infer the number of correct answers. Each correct solution must be selected from several given options by ticking the appropriate box. One, several or all options can be correct. One point is awarded for each correctly answered MC question. A question is solved correctly if the markings are placed correctly in the table. Questions that are not solved at all or not solved completely receive zero points. There are no fractional points.

Bei der Dokumentenprüfung wird im Rahmen eines Audits ein Auszug aus einem Managementhandbuch auf Nonkonformitäten zu den relevanten Normen und auf Mängel untersucht. Der Befund wird in freier schriftlicher Form mit Erläuterungen bzw. Begründungen niedergelegt. Die Feststellungen müssen formale und inhaltliche Mängel mit Normenbezug enthalten. Die weitere Vorgehensweise als Auditor muss beschrieben werden. Die Sachverhalte werden vom Prüfer mit einer Mustervorlage verglichen und bewertet.

8. Schriftliche Online-Prüfung

Die Prüfungsaufgaben erscheinen einzeln auf dem Bildschirm. Die Lösungen zu jeder Prüfungsaufgabe werden direkt zur Aufgabe eingetragen.

Die MC-Aufgaben sind im Singular formuliert, sodass ein Rückschluss auf die Anzahl der richtigen Lösungen nicht möglich ist. Es muss unter mehreren vorgegebenen Lösungen durch Anklicken jede richtige markiert werden. Es können eine, mehrere oder alle Auswahlmöglichkeiten richtig sein. Für jede richtig beantwortete MC-Aufgabe gibt es einen Punkt. Eine Aufgabe ist richtig gelöst, wenn die Markierungen an den richtigen Stellen gesetzt sind. Gar nicht oder nicht vollständig richtig gelöste Aufgaben erhalten null Punkte. Es gibt keine Bruchteile von Punkten. Die Aufgaben werden automatisch gewertet.

Bei der Dokumentenprüfung wird im Rahmen eines Audits ein Auszug aus einem Managementhandbuch auf Nonkonformitäten zu den relevanten Normen und auf Mängel untersucht. Der Befund wird in freier schriftlicher Form mit Erläuterungen bzw. Begründungen niedergelegt. Die Feststellungen enthalten formale und inhaltliche Mängel mit Normenbezug. Die weitere Vorgehensweise als Auditor wird beschrieben. Die Sachverhalte werden vom Prüfer mit einer Mustervorlage verglichen und bewertet.

9. Mündliche Prüfung

Die mündliche Prüfung erfolgt in Teams von je zwei Kandidaten in Form eines simulierten Audits. Die Prüfer vergeben Punkte für verschiedene Kriterien. Details s. Anlage 2b.

During the document review, an extract from a management manual is examined for non-conformities to the relevant standards and for deficiencies. The findings are recorded in free written form with explanations or reasons. The findings contain formal and substantive deficiencies with reference to standards. The further procedure as auditor is described. The auditor compares the facts with a sample template and evaluates them.

8. Written live-online examination

The examination questions appear individually on the screen. The candidate enters solutions to each examination question directly in the question.

The MC questions are formulated in the singular, so it is not possible to infer the number of correct answers. One, several or all options can be correct. One, several or all correct options must always be marked. One point is awarded for each correctly answered MC question. A question is solved correctly if the marking are placed correctly in the table. Questions that are not solved at all or not solved completely receive zero points. There are no fractional points. The tasks are scored automatically.

During the document review, an extract from a management manual is examined for non-conformities to the relevant standards and for deficiencies. The findings are recorded in free written form with explanations or reasons. The findings contain formal and substantive deficiencies with reference to standards. The further procedure as auditor is described. The auditor compares the facts with a sample template and evaluates them.

9. Oral examination

The oral examination takes place in teams of two candidates in the form of a simulated audit. The examiners award points for various criteria. See Appendix 2b for details.

10. Gesamtbewertung

Die Prüfung Datenschutzbeauftragter (TÜV) ist bestanden, wenn die schriftliche Prüfung bestanden ist.

Die Prüfung Datenschutzauditor (TÜV) ist bestanden, wenn die schriftliche und mündliche Prüfung bestanden sind.

Es erfolgt keine Mitteilung über Einzelergebnisse oder Punktzahlen.

Maßgeblich für die Bewertung sind bei nachträglichen Korrekturen, die erreichten 60 %, nicht die auf- oder abgerundete Punktzahl.

11. Zertifizierungsentscheidung und Zertifikatserteilung

Bei bestandener Prüfung und Erfüllung der weiteren Anforderungen wird durch die TÜV NORD CERT ein Personenzertifikat ausgestellt.

Das Personenzertifikat enthält folgende Angaben:

- a) Personalien der zertifizierten Person
(Titel, Vorname, Name, Geburtsdatum)
- b) Bezeichnung der Qualifikation
- c) Prüfungsinhalte
- d) Unterschrift der Fachleitung Personenzertifizierung
- e) Ausstellungsdatum
- f) Gültigkeit
- g) Datum der Erstzertifizierung (bei Rezertifizierung)

Jedes Personenzertifikat erhält eine eindeutige Nummer:

44-10151125-tt.mm.jjjj-DE02-12345 (Beispiel)

Die Nummer setzt sich wie folgt zusammen:

44	TÜV NORD CERT GmbH-Personenzertifizierung
10151125	Kurzkennzeichnung des Zertifizierungsgebietes
tt.mm.jjjj	Letzter Tag der Prüfung
DE01/02	Kennzahl des Prüfungszentrums
12345	Prüfungszentrumsspezifische Kandidaten identifikationsnummer

10. Overall evaluation

The examination Data Protection Officer (TÜV) is passed when the written and the oral/practical examination have/has been passed.

The examination Data Protection Auditor (TÜV) is passed when the written and the oral examination have been passed.

There will be no notification about individual results or markings.

The 60 % achieved is decisive for the assessment, not the number of points rounded up or down.

11. Certification and certificate issuance

The candidate will be issued a certificate of persons by TÜV NORD CERT when the examination is passed and the other requirements are met.

The certificate of person contains the following information:

- a) Personal information of the candidate
(title, first name, last name, date of birth)
- b) Designation of the qualification
- c) Contents of the examination
- d) Signature of the person in charge for certification of persons
- e) Date of issue
- f) Validity
- g) Date of initial certification (in case of recertification)

Each certificate of person is assigned a unique number:

44-10151125-dd.mm.yyyy-DE02-12345 (example)

The number is composed as follows:

44	TÜV NORD CERT GmbH-Certification of Persons
10151125	Product number
dd.mm.yyyy	Last examination day
DE01/02	Code of the examination center
12345	Specific examination center candidate identification number

Das Personenzertifikat darf nur in der zur Verfügung gestellten Form verwendet werden. Es darf nicht nur teil- oder auszugsweise benutzt werden. Änderungen des Personenzertifikats dürfen nicht vorgenommen werden. Das Personenzertifikat darf nicht irreführend verwendet werden.

12. Gültigkeit der Personenzertifikate

Das jeweilige Personenzertifikat ist 3 Jahre gültig.

Die Gültigkeit eines in der Erstzertifizierung erlangten Zertifikats beginnt mit dem Tag der positiven Zertifizierungsentscheidung und gilt bis 3 Jahre nach erfolgreicher Prüfung minus 1 Tag.

13. Anforderungen an die Rezertifizierung

Bei Ablauf der Gültigkeit des Personenzertifikats kann auf Antrag der zertifizierten Person eine Rezertifizierung erfolgen.

Hierzu muss die zertifizierte Person der Zertifizierungsstelle für Personen folgendes nachweisen:

	Nachweis der praktischen Tätigkeit	Schulung im Zertifizierungsgebiet
Datenschutzbeauftragter (TÜV)	im zurückliegenden Zeitraum mind. 1 Jahr im zertifizierten Bereich	Mind. 8 UE Schulung/Erfahrungsaustausch/Symposium etc., in der Neuerungen/Vertiefungen/Weiterentwicklungen im Zertifizierungsgebiet behandelt wurden
Datenschutzauditor (TÜV)	im zurückliegenden Zeitraum mind. 2 Jahre im zertifizierten Bereich und mind. 3 Audits mit einer Auditdauer von insgesamt 3 Personentagen	Mind. 8 UE Schulung/Erfahrungsaustausch/Symposium etc., in der Neuerungen/Vertiefungen/Weiterentwicklungen im Zertifizierungsgebiet behandelt wurden

The certificate of person may only be used in the form issued. It may not be used only in part or in extracts. Changes to the certificate of person may not be made. The certificate of person may not be used in a misleading manner.

12. Validity of certifications of persons

The respective certificate of person is valid for 3 years.

The validity of a certificate acquired during the initial certification begins on the day of the positive certification decision and is valid for 3 years after the successful examination minus 1 day.

13. Requirements for recertification

When a certificate of person expires, it can be recertified upon request of the certificate holder.

For this purpose, the certificate holder must prove the following to the certification body of persons:

	Verification of practical activity	Training in the certification area
Data Protection Officer (TÜV)	In the past period at least 1 year in the certified area	At least 8 TU of training/exchange of experience/symposium, etc., dealing with innovations/advance-ments/further developments in the field of certification.
Data Protection Auditor (TÜV)	In the past period at least 2 years in the certified area and at least 3 audits with a total audit duration of 3 days on site	At least 8 TU of training/exchange of experience/symposium, etc., dealing with innovations/advance-ments/further developments in the field of certification.

Die Erfüllung der Anforderungen muss durch objektive Nachweise bestätigt werden.

Bei Unklarheiten ist die Zertifizierungsstelle für Personen berechtigt, weitere Nachweise anzufordern und/oder die zertifizierte Person zu einem Gespräch einzuladen.

Z. B. sind interne bzw. externe Audits bzgl. Zeitpunkt, Dauer, Art des Audits, Funktion der zertifizierten Person im Audit und Name der auditierten Organisation durch den Arbeitgeber oder Auditauftraggeber schriftlich zu bestätigen.

Bei Unklarheiten ist die Zertifizierungsstelle für Personen berechtigt, weitere Nachweise anzufordern und/oder die zertifizierte Person zu einem Gespräch einzuladen.

Nicht absolvierte Schulungen können bis 12 Monate nach Ablauf der Gültigkeit nachgeholt werden.

14. Mitgeltende Unterlagen

Allgemeine Prüfungsordnung (TÜV®)

Gebührenordnung für Prüfungen (TÜV®)

Erklärung zur Zertifikatserteilung

Re-Zertifizierungsantrag

The fulfilment of the requirements must be confirmed by objective evidence.

In case of ambiguities, the certification body of persons is entitled to request further evidence and/or to invite the certificate holder to an interview.

For example, the employer or audit client must confirm internal or external audits in writing regarding time, duration, type of audit, function of the applicant in the audit, and name of the audited organization.

In case of ambiguities, the certification body of persons is entitled to request further evidence and/or to invite the certificate holder to an interview.

Training courses that have not been completed can be made up for up to 12 months after the expiry date of the certificate of persons.

14. Applicable documents

General examination regulation (TÜV®)

Fee schedule for examinations (TÜV®)

Declaration of certificate issuance

Re-Certification application

**15. Anlage 1: Themen des Lehrgangs und Prüfungsmodalitäten der schriftlichen Prüfung
Datenschutzbeauftragter (TÜV®)**

	Anzahl der UE*	Anzahl der Aufgaben MC*/o*
Themenbereich und Lerninhalte		
1-2. Datenschutzrecht Formelle Datenschutzerfordernisse und Datenschutz-Kontrollinstanzen (RG) Grundlagen • Europäisches Datenschutzrecht und Verhältnis zum nationalen Recht • Einführung in die Datenschutzrechtsordnung: anwendbares Recht für nichtöffentliche Stellen inklusive Kollektivvereinbarungen • Struktur BDSG • Kirchliche Regelungsbefugnis • Sachlicher und räumlicher Anwendungsbereich der DSGVO • Wichtige Begriffe und Prinzipien des Datenschutzrechts (Art. 4 und 5 DSGVO) Personenbezogene Daten, Verantwortlicher, Gemeinsam Verantwortliche, Zweckbindungsgebot, Verarbeitung • Begriff und vertragliche Anforderungen zur Auftragsverarbeitung Rechtswirksame Einwilligungen • Form und Bestimmtheit der Einwilligung • Aufklärungspflichten und Kopplungsverbot • Widerrufsrecht des Betroffenen • Fortgeltung vor dem 25.05.2018 erteilter Einwilligungen • Besonderheiten der Beschäftigteneinwilligung Kernbereiche des Datenschutzes • Übersicht zu den Erlaubnisnormen • Grundlagen zur Verarbeitung von Kunden- und Interessentendaten Erforderliche Daten im Vertragskontext Werbung Verarbeitung von besonderen Datenkategorien • Grundlagen zum Beschäftigtendatenschutz nach § 26 BDSG Zulässige Bewerberdaten Leistungs- und Verhaltenskontrolle im Arbeitsverhältnis Heimliche Überwachung von Mitarbeitern Eckpunkte zu den Mitbestimmungsrechten des Betriebsrats Whistleblowing Hotlines • Übermittlung in Drittländer • Telemedien: Wichtige Pflichten beim Betrieb von Webseiten	16 UE	18 MC

Rechte der Betroffenen • Transparenzpflichten gegenüber dem Betroffenen • Recht auf Datenübertragbarkeit • Löschung und Recht auf Vergessen • Widerspruchsrecht • Automatisierte Einzelentscheidung und Profiling • Schadenersatz Der betriebliche Datenschutzbeauftragte • Benennungspflichten und freiwillige Benennung • Voraussetzungen für einen Konzerndatenschutzbeauftragten • Erforderliches Fachwissen und Vermeidung von Interessenkonflikten • Aufgaben • Stellung im Unternehmen einschließlich Verhältnis zum Betriebsrat • Schweigepflichten und Zeugnisverweigerungsrecht • Abberufungs- und Kündigungsschutz Reichweite der Datenschutz-Organisationspflichten • Melde- und Dokumentationspflichten bei Datensicherheitsvorfällen • Rechenschafts- und Nachweispflichten • Anweisungspflicht Die Aufsichtsbehörde • Aufgaben und Befugnisse • Sanktionen • KI und Datenschutz • Aktivitäten von Aufsichtsbehörden		
3. Datenschutzmanagement und -organisation (DS) Datenschutzgerechte Geschäftsprozesse • Erfüllung der Informationspflichten • Gewährleistung von Rechten betroffener Personen Auskunft Berichtigung / Löschung / Einschränkung der Verarbeitung Recht auf Datenübertragbarkeit Widerspruch Verzeichnis der Verarbeitungstätigkeiten • Voraussetzungen / Zweck • Inhalt • Anforderungen an die Form • Erstellung und Aktualisierung Risikobetrachtung • Begriff Risiko • Abgrenzung Unternehmens- / Betroffenen-Risiken • Methodik der Risikodefinition: Bewertungsmatrix, Risikoklassen, Gesamt- / tolerierbares / Restrisiko Datenschutzfolgenabschätzung • Voraussetzungen • Entscheidung / Begründung und Dokumentation • Durchführung und Organisation	8 UE	11 MC

Umsetzung der Rechenschaftspflicht • Erforderliche Dokumente • Gestaltung der Dokumentation • Audits und Zertifizierungen Arbeitsorganisation des Datenschutzbeauftragten • Ansprechpartner • Durchführung / Dokumentation von Kontrollen - Einbindung in die Geschäftsprozesse		
4. Informationssicherheit (IS) Begriffe und Schutzziele • Begriff Informationssicherheit • Informationssicherheit und Datenschutz • Schutzziele: Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität • Beispiele für weitere Schutzziele • Abhängigkeiten der Schutzziele Gefährdungen der Informationssicherheit • Begriffe • Verbreitete Schwachstellen • Häufige Bedrohungen: Social Engineering, Angriffe auf Passworte, Malware, Hacking, ungewollte Veröffentlichungen Technische und organisatorische Maßnahmen • Angemessenheit der Maßnahmen • Pseudonymisierung • Verschlüsselung • Dokumentation der TOM Hilfs- / Arbeitsmittel für den DSB • Orientierungshilfen der Aufsichtsbehörden • IT-Grundschutzkataloge des BSI Weitere Hilfsmittel	8 UE	11 MC
6. Abschlussprüfung		
schriftlich	75 min.	40 MC

*

UE: Unterrichtseinheit à 45 Minuten

MC: Multiple-Choice-Aufgaben

o: offene Aufgaben

In der Tabelle „Themen des Lehrgangs und Prüfungsmodalitäten der schriftlichen Prüfung“ handelt es sich bei den Angaben der Unterrichtseinheiten um Richtwerte, die in Einzelfällen bedingt durch Zusammensetzung der Teilnehmenden, Vorkenntnisse und Teilnehmerzahl geringfügig abweichen können. Die hier dargestellte Reihenfolge der Themen muss nicht der Reihenfolge der Themen des Lehrgangs entsprechen.

**15. Annex 1: Topics of the course and examination modalities of the written examination
Data Protection Officer (TÜV®)**

Topics and learning content	Number of TU* Number of questions MC*/o*	Number of questions MC*/o*
1-2. data protection law Formal data protection requirements and data protection supervisory authorities (RG) Basic principles • European data protection law and relationship to national law • Introduction to data protection law: applicable law for non-public bodies including collective agreements • Structure of the BDSG • Ecclesiastical regulatory authority • Material and territorial scope of application of the GDPR • Important terms and principles of data protection law (Art. 4 and 5 GDPR) Personal data, controller, joint controllers, purpose limitation requirement, processing • Concept and contractual requirements for order processing Legally effective consent • Form and specificity of consent • Duty to provide information and prohibition of tying • Right of cancellation of the data subject • Continued validity of consent given before 25 May 2018 • Special features of employee consent Core areas of data protection • Overview of the authorisation standards • Principles for processing customer and prospective customer data Required data in the context of a contract Advertising Processing of special categories of data • Basics of employee data protection according to § 26 BDSG Permissible applicant data Performance and behaviour monitoring in the employment relationship Secret surveillance of employees Key points on the co-determination rights of the works council Whistleblowing hotlines • Transmission to third countries • Telemedia: Important obligations when operating websites	16 TU	18 MC

Rights of the data subject • Transparency obligations towards the data subject • Right to data portability • Right to erasure and right to be forgotten • Right to object • Automated individual decision-making and profiling • Compensation for damages The company data protection officer • Appointment obligations and voluntary appointment • Requirements for a Group Data Protection Officer • Necessary expertise and avoidance of conflicts of interest • Responsibilities • Position in the company including relationship with the works council • Duty of confidentiality and right to refuse to testify • Dismissal and dismissal protection Scope of data protection organizational duties • Reporting and documentation obligations in the event of data security incidents • Accountability and verification obligations • Duty to issue instructions The supervisory authority • Tasks and powers • Sanctions • AI and data protection • Activities of supervisory authorities		
3. data protection management and organisation (DS) Data protection-compliant business processes • Fulfilment of information obligations • Guaranteeing the rights of data subjects Information Rectification / erasure / restriction of processing Right to data portability Right to object List of processing activities • Requirements / Purpose • Contents • Requirements for the form • Creation and updating Risk assessment • Concept of risk • Differentiation between company / affected party risks • Methodology of risk definition: evaluation matrix, risk classes, overall / tolerable / residual risk Data protection impact assessment • Prerequisites • Decision / justification and documentation • Implementation and organisation	8 TU	11 MC

Implementation of accountability • Required documents • Organisation of the documentation • Audits and certifications Work organisation of the data protection officer • Contact person • Implementation / documentation of controls - Integration into the business processes		
4. information security (IS) Terms and protection goals • The term information security • Information security and data protection • Protection goals: Confidentiality, integrity, availability, authenticity • Examples of further protection goals • Dependencies of the protection goals Threats to information security • Terms • Common vulnerabilities • Common threats: Social engineering, attacks on passwords, malware, hacking, unwanted publications Technical and organisational measures • Appropriateness of the measures • Pseudonymisation • Encryption • Documentation of the TOM Aids / tools for the DPO • Guidance from the supervisory authorities • IT baseline protection catalogues of the BSI Further aids	8 TU	11 MC
6. final exam		
written	75 min.	40 MC

*

TU: 1 TU corresponds to a teaching unit of 45 minutes.

MC: Multiple Choice questions

o: open question

In the table "Topics of the course and examination modalities of the written examination", the details of the teaching units are approximate values which may deviate slightly in individual cases due to the composition of the participants, prior knowledge and number of participants. The order of the topics presented here does not necessarily correspond to the order of the topics of the course.

**16. Anlage 2: Themen des Lehrgangs und Prüfungsmodalitäten der schriftlichen Prüfung
Datenschutzauditor (TÜV®)**

		Anzahl der UE*	Anzahl der Aufgaben MC*/o*
Themenbereich und Lerninhalte			
1. Das Audit (AUD) Grundlagen • Sinn und Zweck des Audits • Aufgaben und persönliche Haftung des Auditors • Zielsetzung von Audits • Unterscheidung in interne Audits Vorbereitung des Datenschutzaudits • Orientierungsgespräch • Audit des Auftragsverarbeiters • Ansprechpartner identifizieren • Auditpläne und Mustervorlagen vorbereiten Durchführung von Audits • Gesprächsunterteilung in: Einführung, Hauptteil, Abschlussgespräch und Prognose • Dokumentation der Feststellungen Psychologische Gesprächsführung • Bewältigung von Problemsituationen im Audit • Fragetechnik und Trichtermethodik		6 UE	
2. Das Datenschutzmanagementsystem (DMS) Grundlagen • Sinn und Zweck des Datenschutzmanagementsystems • Elemente eines Datenschutzmanagementsystems Aufbau eines Datenschutzmanagementsystems • Implementierung eines Datenschutzkonzeptes • Arbeits- und Hilfsmittel • Ist-Erfassung und –Analyse, Schwachstellenermittlung, Risikoanalyse • Prozessmodelle Dokumentation im Datenschutzmanagementsystem • Datenschutzkonzept • Verfahrens- und Arbeitsanweisungen Nachbereitung des Audits • Auswertung der Feststellungen des Audits • Maßnahme-Empfehlungen • Erstellung des Auditberichts		4 UE	

3. Dokumentenprüfungen • Datenschutzerklärung • Einwilligung • Verzeichnis der Verarbeitungstätigkeiten • Datenschutzfolgeabschätzung • Auftragsverarbeitungsvertrag	6 UE	
4. Nutzung der Auditpläne Auditplan • Besprechung der Auditpläne • Selbständige Entwicklung eines eigenen Auditplanes • Prüfung der technischen Ausstattung • Prüfung der Aufbau- und Ablauforganisation • Prüfung der technischen und organisatorischen Sicherungsmaßnahmen Praxisübungen	8 UE	
6. Abschlussprüfung		
schriftlich	75 min.	20 MC / 1 Doku
mündlich	60 min.	

*

UE: Unterrichtseinheit à 45 Minuten

MC: Multiple-Choice-Aufgaben

o: offene Aufgaben

In der Tabelle „Themen des Lehrgangs und Prüfungsmodalitäten der schriftlichen Prüfung“ handelt es sich bei den Angaben der Unterrichtseinheiten um Richtwerte, die in Einzelfällen bedingt durch Zusammensetzung der Teilnehmenden, Vorkenntnisse und Teilnehmerzahl geringfügig abweichen können. Die hier dargestellte Reihenfolge der Themen muss nicht der Reihenfolge der Themen des Lehrgangs entsprechen.

**16. Annex 2: Topics of the course and examination modalities of the written examination
Data Protection Auditor (TÜV®)**

Topics and learning content	Number of TU*	Number of questions MC*/o*
1. the audit (AUD) Basic principles • Meaning and purpose of the audit • Tasks and personal liability of the auditor • Objectives of audits • Differentiation between internal audits Preparation of the data protection audit • Orientation meeting • Audit of the processor • Identifying contact persons • Prepare audit plans and templates Carrying out audits • Subdivide the meeting into: Introduction, main part, final discussion and forecast • Documentation of the findings Psychological dialogue • Coping with problem situations in the audit • Questioning technique and funnel methodology	6 TU	
2. the data protection management system (DMS) The basics • Meaning and purpose of the data protection management system • Elements of a data protection management system Structure of a data protection management system • Implementation of a data protection concept • Working methods and tools • Recording and analysing the current situation, identifying weak points, risk analysis • Process models Documentation in the data protection management system • Data protection concept • Procedural and work instructions Follow-up of the audit • Evaluation of the audit findings • Recommendations for measures • Preparation of the audit report	4 TU	

3. document checks • Data protection declaration • Consent • Register of processing activities • Data protection impact assessment • Data processing agreement	6 TU	
4. utilisation of the audit plans Audit plan • Discussion of the audit plans • Independent development of your own audit plan • Checking the technical equipment • Checking the structural and process organisation • Checking of technical and organisational security measures Practical exercises	8 TU	
6. final exam		
written	75 min.	20 MC / 1 Docu
oral	60 min.	

*

TU: 1 TU corresponds to a teaching unit of 45 minutes.

MC: Multiple Choice questions

o: open question

In the table "Topics of the course and examination modalities of the written examination", the details of the teaching units are approximate values which may deviate slightly in individual cases due to the composition of the participants, prior knowledge and number of participants. The order of the topics presented here does not necessarily correspond to the order of the topics of the course.

17. Anlage 2b: Themen des Lehrgangs und Prüfungsmodalitäten der mündlichen Prüfung Datenschutzauditor (TÜV®)

Die mündliche Prüfung erfolgt in Teams von je zwei Kandidaten in Form eines simulierten Audits. Die gemeinsame Vorbereitungszeit des Audits beträgt max. 30 Minuten. Das Audit wird unterteilt in Einführung, Hauptteil 1, Hauptteil 2 und Abschluss. Der erste Kandidat führt die Einführung (ca. 2 Minuten) und die erste Hälfte des Hauptteils (ca. 8 Minuten) durch. Der zweite Kandidat schließt mit der zweiten Hälfte des Hauptteils (ca. 8 Minuten) an und beendet das simulierte Audit mit dem Abschlussgespräch (ca. 2 Minuten).

Die Lösung der Aufgabe wird nach den folgenden Kriterien beurteilt:

Kandidat 1:

- Gesprächseröffnung, Einführung, Gesamteindruck (6 Punkte)
- Fachliche Lösung, Bezug zu Rechtstexten und Fachbegriffen (9 Punkte)

Kandidat 2:

- Gesprächsabschluss, weiterer Ablauf, Gesamteindruck (6 Punkte)
- Fachliche Lösung, Bezug zu Rechtstexten und Fachbegriffen (9 Punkte)

Zum Bestehen der Prüfung muss der jeweilige Kandidat mindestens 9 der 15 Punkte erreichen (60 %).

17. Annex 2b: Topics of the course and examination modalities of the oral/practical examination Data Protection Auditor (TÜV®)

The oral examination takes place in teams of two candidates in the form of a simulated audit. The joint preparation time for the audit is a maximum of 30 minutes. The audit is divided into introduction, main part 1, main part 2 and conclusion. The first candidate conducts the introduction (approx. 2 minutes) and the first half of the main part (approx. 8 minutes). The second candidate continues with the second half of the main part (approx. 8 minutes) and ends the simulated audit with the final discussion (approx. 2 minutes).

The solution to the task is assessed according to the following criteria:

Candidate 1:

- Opening of the interview, introduction, overall impression (6 points)
- Technical solution, reference to legal texts and technical terms (9 points)

Candidate 2:

- Conclusion of conversation, further procedure, overall impression (6 points)
- Technical solution, reference to legal texts and technical terms (9 points)

To pass the examination, the respective candidate must achieve at least 9 of the 15 points (60 %).