Universität Münster

AMTLICHE BEKANNTMACHUNGEN

Jahrgang 2025 | Ausgegeben zu Münster am 22. Oktober 2025 | Nr. 49

Inhalt

	Seite
Prüfungsordnung für das Fach **Philosophie** zur Rahmenordnung für die **Bachelorprüfungen** innerhalb des **Zwei-Fach-Modells** an der Universität Münster vom 01.09.2025	4026
Prüfungsordnung für das Fach **Geographie** zur Rahmenordnung für die Prüfungen im Studium für **das Lehramt an Gymnasien und Gesamtschulen** mit dem **Abschluss „Master of Education“** an der Universität Münster vom 14.10.2025	4070
Prüfungsordnung für das Fach **Geographie** zur Rahmenordnung für die Prüfungen im Studium für **das Lehramt an Haupt-, Real-, Sekundar- und Gesamtschulen** mit dem **Abschluss „Master of Education“** an der Universität Münster vom 14.10.2025	4088
Ordnung für den **Zertifikatslehrgang „Datenschutzrecht und Künstliche Intelligenz“** an der **Rechtswissenschaftlichen Fakultät** der Universität Münster vom 15.10.2025	4101

Herausgegeben vom
Rektor der Universität Münster
Schlossplatz 2, 48149 Münster
AB Uni 2025/49
http://www.uni-muenster.de/Rektorat/abuni/index.html

Ordnung für den Zertifikatslehrgang „Datenschutzrecht und Künstliche Intelligenz“ an der Rechtswissenschaftlichen Fakultät der Universität Münster vom 15.10.2025

Auf Grund der §§ 2 Abs. 4 und 62 Abs. 1 und Abs. 4 des Gesetzes über die Hochschulen des Landes Nordrhein-Westfalen (Hochschulgesetz - HG) in der Fassung des Hochschulzukunftsgesetzes vom 16. September 2014 (GV. NRW. S. 547), zuletzt geändert durch Artikel 1 des Gesetzes vom 29. Oktober 2024 (GV. NRW. S. 704), hat die Universität Münster folgende Ordnung erlassen:

Inhaltsverzeichnis:

§ 1 Geltungsbereich
§ 2 Ziel des Lehrgangs und Zweck der Prüfung
§ 3 Teilnahmevoraussetzungen
§ 4 Zuständigkeit
§ 5 Zulassungs- und Prüfungsausschuss
§ 6 Executive Board
§ 7 Aufbau, Umfang und Inhalt des Lehrgangs
§ 8 Prüfungsleistungen
§ 9 Bewertung der Prüfungsleistung
§ 10 Wiederholung von Prüfungsleistungen
§ 11 Nachteilsausgleich
§ 12 Prüferinnen/Prüfer, Beisitzerinnen/Beisitzer
§ 13 Abschluss
§ 14 Zertifikat und Teilnahmebescheinigung
§ 15 Zertifizierung und Führen des Titels
§ 16 Einsicht in die Studienakten
§ 17 Versäumnis, Rücktritt, Täuschung, Ordnungsverstoß
§ 18 Ungültigkeit von Einzelleistungen
§ 19 Inkrafttreten und Veröffentlichung
Anhang: Beschreibung des Zertifikatslehrgangs

§ 1
Geltungsbereich

Diese Ordnung gilt für den Zertifikatslehrgang „Datenschutzrecht und Künstliche Intelligenz“ der Universität Münster an der Rechtswissenschaftlichen Fakultät (Institut für Internationales Wirtschaftsrecht – IWR III).

§ 2
Ziel des Lehrgangs und Zweck der Prüfung

(1) [1]Der Zertifikatslehrgang soll den Teilnehmenden, aufbauend auf einem abgeschlossenen grundständigen Studium oder ergänzend zum aktuellen, einschlägigen Tätigkeitsbereich, Grundlagen und aktuelle Fragestellungen aus dem Bereich Datenschutzrecht und KI-Recht vermitteln. [2]Die Wissensvermittlung verfolgt hier sowohl einen wissenschaftlichen als auch einen praxisbezogenen Ansatz und zeichnet sich durch Interdisziplinarität aus. [3]Der Lehrgang beleuchtet die Thematik des Datenschutzes sowie des Rechts der Künstlichen Intelligenz aus juristischer Sicht und vermittelt neben den rechtlichen Grundlagen auch Spezialwissen, beispielsweise zur Datenschutzaufsicht, den Datenschutzbeauftragten sowie rechtlichen Fragestellungen im Zusammenhang mit Künstlicher Intelligenz. [4]Der Lehrgang soll die Teilnehmenden dazu befähigen, Angelegenheiten ihres Berufsalltags fundierter analysieren und fallgerecht entscheiden zu können.

(2) [2]Durch die Prüfungen soll festgestellt werden, inwieweit die Teilnehmenden die Lehrinhalte des Zertifikatslehrgangs nachvollzogen haben und die für die Anwendung in der Berufspraxis erforderlichen Kenntnisse und Fähigkeiten einsetzen können.

§ 3
Teilnahmevoraussetzungen

(1) [1]Für die Teilnahme am Zertifikatslehrgang wird

a) einschlägige Berufserfahrung von mindestens drei Jahren oder

b) ein abgeschlossenes Hochschulstudium und ein Jahr einschlägige Berufserfahrung

vorausgesetzt. [2]Über die Einschlägigkeit der Berufserfahrung entscheidet der Zulassungs- und Prüfungsausschuss. [3]Sie ist insbesondere anzunehmen, wenn diese bei einer Kanzlei mit

Schwerpunkt für Datenschutz-, KI- oder IT-Recht ausgeübt wurde. [4]Auch eine Tätigkeit in Unternehmen kann als einschlägig angesehen werden, wenn der/die Teilnehmende mit Fragestellungen aus dem Curriculum in Berührung gekommen ist. [5]Absolvierte Praktika oder Berufsausbildungen können zu Teilen angerechnet werden, wenn sie inhaltlichen Bezug zum Lehrgang aufweisen.

(2) [1]Die Mindestteilnehmendenzahl beträgt 15, die maximale Teilnehmendenzahl 40 Personen. [2]Die Plätze werden nach Eingang der Anmeldung vergeben.

(3) [1]Die Teilnahme ist an eine verbindliche Anmeldung und an die Zahlung der im Anmeldeformular angegebenen Teilnahmegebühr geknüpft. [2]Einzelheiten hierzu regelt der zwischen der/dem Teilnehmenden und der JurGrad gGmbH geschlossene Teilnahmevertrag.

§ 4
Zuständigkeit

(1) [1]Der Fachbereich Rechtswissenschaften bildet für die inhaltliche Planung und Gestaltung des Zertifikatslehrgangs einen Zulassungs- und Prüfungsausschuss. [2]Dieser Ausschuss entscheidet über die Zulassungen zum Lehrgang und ist zugleich für die Organisation der Prüfungen zuständig.

(2) [2]Der Zertifikatslehrgang wird in Kooperation mit der JurGrad gGmbH durchgeführt.

§ 5
Zulassungs- und Prüfungsausschuss

(1) [1]Die Mitglieder des Zulassungs- und Prüfungsausschusses werden aus der Gruppe der Hochschullehrerinnen/Hochschullehrer des Fachbereichs Rechtswissenschaften gewählt. [2]Der Zulassungs- und Prüfungsausschuss setzt sich aus der/dem Vorsitzenden, ihrem/seinem Stellvertreter bzw. ihrer/seiner Stellvertreterin und einem weiteren Mitglied zusammen. [3]Die Amtszeit der Mitglieder beträgt drei Jahre. [4]Wiederwahl ist zulässig.

(2) [1]Der Zulassungs- und Prüfungsausschuss achtet darauf, dass die Bestimmungen dieser Ordnung eingehalten werden, und sorgt für die ordnungsgemäße Durchführung der Prüfung. [2]Er berichtet dem Fachbereich Rechtswissenschaften regelmäßig über die Entwicklung des Zertifikatslehrgangs und gibt Anregungen zur Aktualisierung der Prüfungsordnung. [3]Der Zulassungs- und Prüfungsausschuss kann die Erledigung seiner Aufgaben für alle Regelfälle seiner/seinem

Vorsitzenden übertragen; dies gilt nicht für Entscheidungen über Widersprüche.

(3) [1]Der Zulassungs- und Prüfungsausschuss ist beschlussfähig, wenn neben der/dem Vorsitzenden oder ihrer/seiner Stellvertreterin bzw. ihrem/seinem Stellvertreter mindestens ein zweites Mitglied anwesend ist. [2]Er beschließt mit einfacher Mehrheit; bei Stimmgleichheit entscheidet die Stimme der/des Vorsitzenden und im Falle ihrer/seiner Abwesenheit die Stimme der/des stellvertretenden Vorsitzenden.

(4) [1]Die Mitglieder des Zulassungs- und Prüfungsausschusses haben das Recht, der Abnahme der Prüfungen beizuwohnen.

(5) [1]Die Mitglieder des Zulassungs- und Prüfungsausschusses unterliegen der Amtsverschwiegenheit. [2]Die Sitzungen des Zulassungs- und Prüfungsausschusses sind nicht öffentlich.

§ 6
Executive Board

(1) [1]Das Executive Board ist ein Gremium mit beratender Funktion, das sich aus der/dem Vorsitzenden des Zulassungs- und Prüfungsausschusses sowie weiteren Hochschullehrerinnen/Hochschullehrern und Praktikerinnen/Praktikern zusammensetzt.

(2) [1]Die Mitglieder des Executive Boards werden von der wissenschaftlichen Leiterin/dem wissenschaftlichen Leiter des Zertifikatslehrgangs für die Dauer von drei Jahren ernannt. [2]Eine Verlängerung der Amtszeit ist möglich. [3]Das Executive Board gibt der wissenschaftlichen Leitung Impulse hinsichtlich der Anpassung des Zertifikatslehrgangs an die aktuellen Entwicklungen und Bedürfnisse des Marktes. [4]Insbesondere wird das Executive Board in folgenden Angelegenheiten beratend und unterstützend tätig:

1. bei der Prüfung und Aktualisierung der Inhalte des Zertifikatslehrgangs
2. bei der Auswahl der Dozentinnen/Dozenten des Zertifikatslehrgangs
3. bei der Entscheidung über Rezertifizierungen

(3) [1]Das Executive Board wählt eine/n Vorsitzende/n. [2]Es kann die Erledigung seiner Aufgaben auf die/den Vorsitzende/n übertragen.

§ 7
Aufbau, Umfang und Inhalt des Lehrgangs

(1) [1]Der Zertifikatslehrgang unterteilt sich in zwei Blockveranstaltungen, mit 40 Unterrichtsstunden (30 Zeitstunden) im ersten Block und 45 Unterrichtsstunden (33,75 Zeitstunden) im zweiten Block.

(2) [1]Für den erfolgreichen Abschluss des Zertifikats werden sieben Leistungspunkte vergeben. [2]Leistungspunkte sind ein quantitatives Maß für die Gesamtbelastung der/des Teilnehmenden. [3]Sie umfassen sowohl den unmittelbaren Unterricht als auch die Zeit für die Vor- und Nachbereitung des Lehrstoffes (Präsenz- und Selbststudium), die Prüfungsvorbereitungen sowie die Prüfung selbst. [4]Für den Erwerb eines Leistungspunkts wird im Zertifikatslehrgang ein Arbeitsaufwand von 25 Zeitstunden zugrunde gelegt. [5]Das Gesamtvolumen des Zertifikatslehrgangs entspricht einem Arbeitsaufwand von 175 Zeitstunden. [6]Ein Leistungspunkt entspricht einem Credit-Point nach dem ECTS (European Credit Transfer System).

(3) Die Inhalte des Zertifikatslehrgangs sind der Beschreibung im Anhang zu entnehmen.

(4) [1]Es werden im Wesentlichen Seminare durchgeführt. [2]Die Seminare dienen der gemeinsamen Erarbeitung von Fragestellungen. [3]Sie beinhalten Diskussionen im Plenum, die der anwendungsorientierten und praxisnahen Erörterung und Vertiefung der zuvor erworbenen Kenntnisse dienen. [4]Es werden auch weitere Lehrformate, beispielsweise Vorlesungen, angeboten. [5]Die Vorlesungen dienen der Vermittlung von Kenntnissen in den verschiedenen Bereichen mit Datenschutzrecht-Bezug.

§ 8
Prüfungsleistungen

(1) [1]Die beiden Prüfungsleistungen werden in Form einer Präsentationsprüfung und einer Einsendeaufgabe (schriftliche Hausarbeit) erbracht.

(2) [1]Im Anschluss an die letzte Blockveranstaltung findet die Präsentationsprüfung statt. [2]Diese bezieht sich auf sämtliche Lehreinheiten und wird in Form einer Gruppenarbeit erbracht. [3]Die einzelnen Gruppen erhalten unterschiedliche Aufgaben, für deren Bearbeitung 30 Minuten zur Verfügung stehen. [4]Im Anschluss trägt die Gruppe das Ergebnis der Ausarbeitung vor. [5]Die Vortragsdauer liegt bei max. 10 Minuten. [6]Im Anschluss sind 10 Minuten für weitergehende Fragen durch die Prüfenden vorgesehen. [7]Die Fragen können sich an die Gruppe oder an einzelne Mitglieder der Gruppe richten.

(3) [1]Der Zertifikatslehrgang schließt mit einer Einsendeaufgabe ab. [2]Die schriftliche Hausarbeit soll zeigen, dass der/die Prüfungskandidat/in in der Lage ist, ein rechtswissenschaftliches Problem aus den Bereichen „Datenschutz“ und „Künstliche Intelligenz“ in vorgegebener Zeit selbstständig zu bearbeiten. [3]Das Thema der Hausarbeit wird vom Zulassungs- und Prüfungsausschuss gestellt. [4]Die Ausarbeitung hat einen Umfang von 10 bis 12 Textseiten im DIN A4-Format. [5]Die Bearbeitungszeit beträgt einen Monat.

(4) [1]Mit beiden Prüfungsformen stellen die Teilnehmenden unter Beweis, dass sie ein vorgegebenes Problemfeld im Bereich des Datenschutzrechts und rechtliche Fragestellungen, die mit dem Einsatz Künstlicher Intelligenz einhergehen, innerhalb eines begrenzten Zeitraums erarbeiten und eigenständige Lösungsansätze entwickeln können. [2]Das Durchdringen der Materie, das selbstständige Setzen von Schwerpunkten sowie die pointierte und verständliche Darstellung sind Teil der Prüfungsleistung.

§ 9
Bewertung der Prüfungsleistungen

(1) [1]Für die Präsentationsprüfung wird keine Note vergeben. [2]Der individuelle Beitrag der Teilnehmenden wird mit „bestanden“ bzw. „nicht bestanden“ bewertet.

(2) [1]Für die Bewertung der Einsendeaufgabe sind folgende Noten zu verwenden:

sehr gut	(1,0)
gut	(2,0)
befriedigend	(3,0)
ausreichend	(4,0)
nicht bestanden	(5,0)

[2]Zur differenzierten Bewertung von Prüfungsleistungen können durch Erniedrigen oder Erhöhen der einzelnen Noten um 0,3 Zwischenwerte gebildet werden; die Noten 4,3, 4,7 und 5,3 sind dabei ausgeschlossen.

§ 10
Wiederholung von Prüfungsleistungen

(1) [1]Prüfungen, die bestanden wurden, können nicht wiederholt werden.

(2) [1]Erstmals nicht bestandene schriftliche Prüfungen können zweimal wiederholt werden. [2]Wird eine Prüfungsleistung auch im zweiten Wiederholungsfall nicht mit mindestens „ausreichend (4,0)“ bewertet, ist der Zertifikatslehrgang endgültig nicht bestanden. [3]Wiederholungsprüfungen, bei deren endgültigem Nichtbestehen keine weitere Wiederholungsmöglichkeit vorgesehen ist, sind von mindestens zwei Prüferinnen/Prüfern im Sinne des § 12 dieser Ordnung zu bewerten. [4]Bei einer Notendivergenz wird das arithmetische Mittel aus den Einzelbewertungen gebildet und zur nächstgelegenen Notenstufe gerundet, sofern die Differenz nicht mehr als eine ganze Notenstufe beträgt. [5]Beträgt die Differenz zwischen Erst- und Zweitgutachten mehr als eine ganze Notenstufe oder lautet eine Bewertung „nicht bestanden“ und die andere „bestanden“ oder besser, erfolgt eine Beratung der beiden Prüferinnen oder Prüfer. [6]Können sich diese nicht einigen, wird die Note endgültig von einer dritten Prüferin oder einem dritten Prüfer festgelegt, die oder der von der Vorsitzenden oder dem Vorsitzenden des Zulassungs- und Prüfungsausschusses bestimmt wird.

(3) [1]Im Falle einer nicht abgeleisteten oder nicht bestandenen Präsentationsprüfung wird die Wiederholungsprüfung in Form einer mündlichen Prüfung erbracht. [2]Die Prüfungsdauer beträgt 30 Minuten. [3]Das Prüfungsgespräch kann digital mittels Video-Konferenz durchgeführt werden. [4]Für die mündliche Prüfung wird keine Note vergeben, sie wird mit „bestanden” bzw. „nicht bestanden” bewertet.

(4) [1]Die mündliche Prüfung kann einmal wiederholt werden. [2]Wird die Prüfungsleistung auch im Wiederholungsfall mit „nicht bestanden“ bewertet, ist der Zertifikatslehrgang endgültig nicht bestanden. [3]Wiederholungsprüfungen sind von mindestens zwei Prüfern/Prüferinnen im Sinne des § 12 dieser Ordnung durchzuführen.

§ 11
Nachteilsausgleich

(1) [1]Macht eine Teilnehmerin/ein Teilnehmer glaubhaft, dass sie bzw. er wegen einer chronischen Krankheit oder einer Behinderung nicht in der Lage ist, die Prüfungsleistung ganz oder teilweise in der vorgesehenen Weise abzulegen, muss der Zulassungs- und Prüfungsausschuss auf Antrag der/des Teilnehmenden unter Berücksichtigung des Grundsatzes der Chancengleichheit

bedarfsgerechte Abweichungen hinsichtlich der Form und Dauer sowie der Nutzung von Hilfsmitteln oder Hilfspersonen gestatten.

(2) [1]Bei Entscheidungen nach Absatz 1 ist auf Wunsch der/des Teilnehmenden die/der Fachbereichsbeauftragte für Studierende mit Beeinträchtigung der Universität zu beteiligen.

(3) [1]Der Nachteilsausgleich gemäß Absatz 1 wird einzelfallbezogen gewährt; zur Glaubhaftmachung einer chronischen Krankheit oder Behinderung kann die Vorlage geeigneter Nachweise verlangt werden. [2]Hierzu zählen insbesondere ärztliche Atteste oder, falls vorhanden, Behindertenausweise.

(4) [1]Soweit eine Teilnehmerin auf Grund mutterschutzrechtlicher Bestimmungen nicht in der Lage ist, Studien- oder Prüfungsleistungen ganz oder teilweise in der vorgesehenen Weise abzulegen, gelten die Absätze 1 bis 3 entsprechend.

§ 12
Prüferinnen/Prüfer, Beisitzerinnen/Beisitzer

(1) [1]Der Zulassungs- und Prüfungsausschuss bestellt für die Prüfungsleistung die Prüferinnen/Prüfer sowie, soweit es um mündliche Prüfungen geht, die Beisitzerinnen/Beisitzer. [2]Er kann die Bestellung auf die Vorsitzende/den Vorsitzenden delegieren.

(2) [1]Prüfer/innen und Beisitzer/innen sind Hochschullehrer/innen und wissenschaftliche Mitarbeiter/innen der Rechtswissenschaftlichen Fakultät. [2]Dozierende aus der Praxis, die an dem Zertifikatslehrgang mitwirken, können Prüfer/innen sein, wenn sie ein rechtswissenschaftliches oder wirtschaftswissenschaftliches Studium an einer Hochschule erfolgreich mit zumindest einem Staatsexamen, einer Diplom- oder einer Masterprüfung abgeschlossen haben.

(3) Die Prüfer/innen und Beisitzer/innen sind in ihrer Prüfungstätigkeit unabhängig.

(4) [1]Die Gruppenprüfung wird vor einer Prüferin/einem Prüfer in Gegenwart einer Beisitzerin/eines Beisitzers abgelegt. [2]Die wesentlichen Aspekte des Vortrags und der anschließenden Fragen durch die Prüfer/innen sind ebenso wie das Ergebnis der Prüfung in einem Protokoll festzuhalten, welches von der Prüferin/dem Prüfer und der Beisitzerin/dem Beisitzer zu unterzeichnen ist.

§ 13
Abschluss

Den Zertifikatslehrgang hat erfolgreich abgeschlossen, wer an den Präsenzveranstaltungen zu 75 % teilgenommen, die beiden Abschlussprüfungen erfolgreich abgelegt und 7 ECTS-Punkte erworben hat.

§ 14
Zertifikat und Teilnahmebescheinigung

(1) Über den erfolgreichen Abschluss des Zertifikatslehrgangs stellt das das Institut für Internationales Wirtschaftsrecht der Rechtswissenschaftlichen Fakultät ein Zertifikat nach § 62 Abs. 4 HG aus.

(2) [1]Das Zertifikat trägt das Datum des Tages, an dem die letzte Prüfungsleistung erbracht worden ist. [2]Es wird von der wissenschaftlichen Leiterin/dem wissenschaftlichen Leiter unterzeichnet und mit dem Siegel des Fachbereichs versehen.

(3) Hat eine Teilnehmerin/ein Teilnehmer den Zertifikatslehrgang endgültig nicht bestanden, wird ihr/ihm die Teilnahme an den im Zertifikatslehrgang belegten Lehreinheiten bescheinigt.

§ 15
Zertifizierung und Führen des Titels

(1) [1]Mit Abschluss des Lehrgangs erwerben die Teilnehmenden zwei Titel. [2]Die Titel lauten „Zertifizierter Datenschutzbeauftragter (Univ. Münster)“ und „Zertifizierter AI-Officer (Univ. Münster)“.

(2) [1]Das Recht zur Titelführung erlischt für beide Abschlüsse nach Ablauf von drei Jahren. [2]Eine Beantragung der Rezertifizierung beider Titel nach Ablauf der drei Jahre ist möglich. [3]Der Antrag ist an die/den Vorsitzende/n des Zulassungs- und Prüfungsausschusses zu richten.

(3) Voraussetzung für die Rezertifizierung des Titels sind jeweils

1. eine mindestens einjährige einschlägige Tätigkeit seit der erstmaligen Verleihung des Titels bzw. seit der letzten Rezertifizierung und
2. der Nachweis jährlicher einschlägiger Fortbildungen im Umfang von mindestens 6 Zeitstunden.

(4) [1]An den in Abs. 3 Nr. 2 erforderlichen fachspezifischen Fortbildungen müssen die Antragsteller/innen hörend oder dozierend teilgenommen haben. [2]Die hörende Teilnahme setzt eine anwaltsorientierte oder interdisziplinäre Veranstaltung in den Bereichen „Datenschutz“ und „Künstliche Intelligenz“ voraus. [3]Bei Fortbildungsveranstaltungen, die nicht in Präsenzform durchgeführt wurden, muss die Möglichkeit der Interaktion der Vortragenden mit den Teilnehmenden und die Interaktion der Teilnehmenden untereinander sichergestellt sein. [4]Der Nachweis der durchgängigen Teilnahme muss erbracht werden.

(5) [1]Über die Anerkennung der Rezertifizierung entscheidet die/der Vorsitzende des Zulassungs- und Prüfungsausschusses. [2]Sie/er kann sich hierbei mit den Mitgliedern des Executive Boards beraten.

(6) [1]Dem Antrag auf Rezertifizierung sind eine aktuelle Tätigkeitsbescheinigung sowie ein Nachweis der in den zurückliegenden drei Kalenderjahren besuchten Fortbildungen beizufügen. [2]Bestehen Zweifel bzgl. der Geeignetheit oder Einschlägigkeit der besuchten Weiterbildungen, kann der Zulassungs- und Prüfungsausschuss dies durch ein Gespräch mit der Antragstellerin/dem Antragsteller überprüfen.

§ 16
Einsicht in die Studienakten

(1) [1]Der Kandidat/die Kandidatin hat die Möglichkeit, Einsicht in seine/ihre schriftlichen Prüfungsleistungen zu nehmen. [2]Die korrigierte Einsendeaufgabe und das Gutachten zur Präsentationsprüfung werden in den geschützten Bereich des Intranets hochgeladen.

(2) [1]Darüber hinaus ist eine Einsicht in die gesamte Prüfungsakte binnen eines Monats nach Aushändigung des Zertifikats möglich. [2]Diese Einsichtnahme erfolgt in den Büroräumen der JurGrad gGmbH während der Geschäftszeiten. [3]Das Anfertigen einer Kopie oder einer sonstigen originalgetreuen Reproduktion im Rahmen der Akteneinsicht ist grundsätzlich zulässig. [4]Der Zeitpunkt der Einsichtnahme wird dokumentiert.

§ 17
Versäumnis, Rücktritt, Täuschung, Ordnungsverstoß

(1) [1]Eine Prüfungsleistung gilt als „nicht bestanden“, wenn die/der Teilnehmende ohne triftige Gründe nicht zu dem festgesetzten Termin erscheint oder wenn sie/er nach Beginn der Prüfung ohne triftige Gründe von ihr zurücktritt. [2]Als triftiger Grund kommen insbesondere krankheitsbedingte Prüfungsunfähigkeit und die Inanspruchnahme von Fristen des Bundeselterngeld- und Elternzeitgesetzes oder die Pflege oder Versorgung der Ehegattin/des Ehegatten, der eingetragenen Lebenspartnerin oder des eingetragenen Lebenspartners oder eines in gerader Linie Verwandten oder ersten Grades Verschwägerten, wenn diese oder dieser pflege- oder versorgungsbedürftig ist, in Betracht.

(2) Sofern die Universität Münster eine Teilnehmerin gemäß den Bestimmungen des Mutterschutzgesetzes nicht im Rahmen ihrer Ausbildung tätig werden lassen darf, ist die Durchführung einer Prüfung unzulässig.

(3) [1]Die für den Rücktritt oder das Versäumnis nach Absatz 1 geltend gemachten Gründe müssen dem Zulassungs- und Prüfungsausschuss unverzüglich schriftlich angezeigt und glaubhaft gemacht werden. [2]Bei Krankheit der/des Teilnehmenden kann der Zulassungs- und Prüfungsausschuss ein ärztliches Attest verlangen. [3]Erkennt der Zulassungs- und Prüfungsausschuss die Gründe an, wird der/dem Teilnehmenden dies schriftlich mitgeteilt.

(4) [1]Versuchen Teilnehmende, das Ergebnis einer Prüfungsleistung durch Täuschung, zum Beispiel Benutzung nicht zugelassener Hilfsmittel, zu beeinflussen, gilt die betreffende Leistung als nicht erbracht und als „nicht bestanden“ bewertet. [2]Wer die Abnahme einer Prüfungsleistung stört, kann von den jeweiligen Lehrenden oder Aufsichtführenden in der Regel nach Abmahnung von der Fortsetzung der Erbringung der Einzelleistung ausgeschlossen werden; in diesem Fall gilt die betreffende Prüfungsleistung als nicht erbracht und mit „nicht bestanden“ (5,0) bewertet. [3]In schwerwiegenden Fällen kann der Zulassungs- und Prüfungsausschuss die/den Teilnehmenden von der Zertifikatsprüfung insgesamt ausschließen. [4]Die Zertifikatsprüfung ist in diesem Fall endgültig nicht bestanden. [5]Die Gründe für den Ausschluss sind aktenkundig zu machen.

(5) [1]Belastende Entscheidungen sind den Betroffenen von dem Zulassungs- und Prüfungsausschuss unverzüglich schriftlich mitzuteilen, zu begründen und mit einer Rechtsbehelfsbelehrung zu versehen. [2]Vor einer Entscheidung ist den Betroffenen Gelegenheit zur Stellungnahme zu geben.

§ 18
Ungültigkeit von Einzelleistungen

(1) [1]Hat die/der Teilnehmende bei einer der Prüfungsleistungen getäuscht und wird diese Tatsache erst nach der Aushändigung des Zertifikats bekannt, kann der Zulassungs- und Prüfungsausschuss das nachträglich entsprechend berücksichtigen und diese Leistung ganz oder teilweise für nicht bestanden erklären.

(2) [1]Der/dem Teilnehmenden ist vor einer Entscheidung Gelegenheit zur Stellungnahme zu geben.

§ 19
Inkrafttreten und Veröffentlichung

[1]Diese Ordnung tritt am Tage nach ihrer Veröffentlichung in den Amtlichen Bekanntmachungen der Universität Münster (AB Uni) in Kraft. [2]Sie gilt für alle, die ab dem Jahr 2026 an dem Zertifikatslehrgang teilnehmen.

Ausgefertigt aufgrund des Beschlusses des Fachbereichsrats des Fachbereichs Rechtswissenschaften vom 01.07.2025.

Die vorstehende Ordnung wird hiermit verkündet.

Es wird darauf hingewiesen, dass gemäß § 12 Abs. 5 des Gesetzes über die Hochschulen des Landes Nordrhein-Westfalen (Hochschulgesetz – HG NRW) eine Verletzung von Verfahrens- oder Formvorschriften des Hochschulgesetzes NRW oder des Ordnungs- oder des sonstigen autonomen Rechts der Hochschule nach Ablauf eines Jahres seit dieser Bekanntmachung nicht mehr geltend gemacht werden kann, es sei denn

1. die Ordnung ist nicht ordnungsgemäß bekannt gemacht worden,
2. das Rektorat hat den Beschluss des die Ordnung beschließenden Gremiums vorher beanstandet
3. der Form- oder Verfahrensmangel ist gegenüber der Hochschule vorher gerügt und dabei die verletzte Rechtsvorschrift und die Tatsache bezeichnet worden, die den Mangel ergibt, oder
4. bei der öffentlichen Bekanntmachung der Ordnung ist auf die Rechtsfolge des Rügeausschlusses nicht hingewiesen worden.

Münster, den 15.10.2025

Der Rektor

Prof. Dr. Johannes W e s s e l s

Anhang: Beschreibung des Zertifikatslehrgangs

Zertifikatslehrgang	**Datenschutzrecht und KI**
1 Basisdaten	
Leistungspunkte (LP)	7
Workload (h) insgesamt	175
Dauer des Lehrgangs	Zwei Blöcke mit 4 bzw. 5 Tagen | je Veranstaltungstag 5-10 Unterrichtsstunden
Status (P/WP)	P

2 Profil
Zielsetzung des Lehrgangs
Die Teilnehmerinnen und Teilnehmer erhalten einen Überblick über den Tätigkeitsbereich Datenschutzrecht und das Recht der Künstlichen Intelligenz sowie über die rechtlichen Zusammenhänge innerhalb dieser Arbeitsfelder. Entscheidend ist dabei insbesondere die interdisziplinäre Aufarbeitung der Lerninhalte. Neben den rechtlichen Grundlagen werden auch Strategien zur praxistauglichen Umsetzung des Datenschutzes sowie der rechtlichen Aspekte im Umgang mit KI-Technologien vermittelt, um eine erweiterte Beratungsmöglichkeit in der Berufspraxis zu gewährleisten. Diese Vermittlung erfolgt anhand von Fallbeispielen, sodass die Teilnehmenden ihre neuen Kenntnisse bestmöglich in ihren Berufsalltag integrieren können. Die Teilnehmenden sollen zudem in die Lage versetzt werden, relevante Gerichtsentscheidungen und Beiträge in der Fachliteratur sowohl zum Datenschutzrecht als auch zu rechtlichen Fragestellungen im Bereich Künstliche Intelligenz einzuordnen und in ihre spätere Beratung einzubinden.
Lehrinhalte
Die Lerninhalte sollen den breit gefächerten Themenbereich Datenschutzrecht sowie das Recht der Künstlichen Intelligenz möglichst umfassend aufarbeiten. Durch die Vermittlung von Grundwissen und ausgewählten Spezialfragen – insbesondere Fragen der KI-Technologie – sollen die Teilnehmenden in die Lage versetzt werden, unbekannte Rechtsprobleme selbstständig zu bearbeiten. Der Lehrgang vermittelt die theoretischen Lehrinhalte zumeist anhand praxisbezogener Fallbeispiele, die sowohl datenschutzrechtliche als auch KI-rechtliche Fragestellungen berücksichtigen, und unterteilt sich in verschiedene Themenblöcke. **Einführung und Grundlagen in das Datenschutzrecht** Die Teilnehmenden erhalten eine Einführung in das Rechtsgebiet Datenschutz und lernen die internationalen, europäischen und nationalen Rechtsquellen sowie die allgemeinen Begriffe des Themenfelds kennen. Der Fokus liegt dabei auf der DSGVO und dem BDSG sowie deren Regelungsgegenständen. Die Teilnehmenden lernen die verschiedenen Verarbeitungstatbestände und Pflichten des Verarbeiters kennen. Ihnen werden die Grundprinzipien des Datenschutzrechts – wie beispielsweise die Grundsätze der Zweckbindung und Datenminimierung – vermittelt. Nach Abschluss dieser Einheit wissen die Teilnehmenden um die Bedeutung der Datenschutzregelungen insgesamt sowie eines Datenschutzkonzepts in der Beratungspraxis.

Zudem kennen sie die allgemeinen Begrifflichkeiten des Rechtsgebiets und sind dadurch in der Lage, sich selbstständig weiteres Wissen im Bereich des Datenschutzrechts anzueignen.

Einführung in die rechtlichen Grundlagen von KI
Die Teilnehmenden erhalten eine Einführung in die grundlegenden Konzepte der Künstlichen Intelligenz und deren Anwendungsbereiche. Sie lernen, wie KI-Systeme Daten verarbeiten und welche datenschutzrechtlichen Fragestellungen hierbei relevant sind. Ein besonderer Schwerpunkt liegt auf der zum 2. Februar 2025 in Kraft tretenden KI-Verordnung. Es folgt eine Einführung in § 4 KI-VO, welcher eine sogenannte KI-Kompetenz in Unternehmen fordert, die mit KI umgehen. Zudem werden die Grundfunktionen von KI und die rechtlichen Begrifflichkeiten in diesem Zusammenhang vermittelt.
Die Teilnehmenden werden mit den Herausforderungen hinsichtlich Transparenz, Fairness und Nachvollziehbarkeit von KI-Modellen vertraut gemacht und erlangen ein Verständnis dafür, wie Datenschutzbeauftragte die Nutzung von KI im Einklang mit datenschutzrechtlichen Vorgaben gestalten können. Am Ende des Lehrgangs können die Teilnehmenden die datenschutzrechtlichen Implikationen von KI-Systemen erkennen und geeignete Maßnahmen zur Risikominimierung entwickeln.

Kundendatenschutz (inkl. Datenschutz im Marketing)
Die Veranstaltung widmet sich datenschutzrechtlichen Sachverhalten, die im Zusammenhang mit dem Marketing eines Unternehmens auftreten. Dies betrifft neben der Verarbeitung von Kunden- und Interessentendaten insbesondere Aspekte im Zusammenhang mit Online-Marketing. Die Teilnehmenden lernen die Anforderungen des Datenschutzes an Websites (Impressum, Cookies, Datenschutzerklärung), Social-Media-Auftritte sowie Werbekampagnen (z. B. E-Mail-Newsletter) und deren Auswertung (z. B. Google Analytics) kennen. Dabei werden ihnen die Betroffenenrechte nach der DSGVO vermittelt. Zudem werden bereichsspezifische Spezialvorschriften wie das nationale TDDDG vorgestellt und aktuelle Entscheidungen des EuGH, die sich mit der Datenverarbeitung zu Werbezwecken befassen (z. B. Schrems III), besprochen.

Beschäftigtendatenschutz
Die Einheit befasst sich mit sämtlichen Aspekten des Datenschutzes im Verhältnis zwischen Arbeitgeber und Arbeitnehmer. Die Teilnehmenden setzen sich mit den berechtigten Interessen des Arbeitgebers an einer Datenverarbeitung, den Anforderungen an eine wirksame Einwilligung durch Beschäftigte sowie den Grenzen der Datenverarbeitung – insbesondere im Hinblick auf besondere Kategorien personenbezogener Daten gemäß Art. 9 DSGVO – auseinander. Weitere Schwerpunkte sind die datenschutzrechtliche Bewertung von Mitarbeiterüberwachung, der Einsatz von KI-Systemen im Personalbereich (z. B. automatisierte Entscheidungsfindung) sowie die damit verbundenen Mitbestimmungsrechte. Ziel der Veranstaltung ist es, die Teilnehmenden zu befähigen, datenschutzrechtliche Herausforderungen im Beschäftigungskontext zu erkennen, rechtskonforme Lösungen zu entwickeln und zukünftige Entwicklungen, etwa durch ein Beschäftigtendatenschutzgesetz, einordnen zu können.

Datenschutz-Folgenabschätzung und Datenschutz durch Technik (inkl. KI)
Die Teilnehmenden lernen den risikobasierten Ansatz der DSGVO sowie die Voraussetzungen einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO kennen und erfahren, welche Anforderungen die Aufsichtsbehörden und Gerichte an diese stellen. Der Fokus liegt auf der praktischen Durchführung und Dokumentation solcher Abschätzungen sowie auf dem Risikomanagement. Unternehmen haben bei der Datenschutz-Folgenabschätzung den Verarbeitungsprozess zu dokumentieren, Risiken für die Betroffenen zu identifizieren und geeignete Abhilfemaßnahmen darzustellen. Weitere Inhalte sind die Pflichten von Betreibern Hochrisiko-KI-

Systemen nach Art. 26 der KI-Verordnung, insbesondere im Hinblick auf technische und organisatorische Maßnahmen (TOMs) sowie menschliche Aufsicht, sowie die Grundrechtefolgenabschätzung nach Art. 27 KI-VO. Mit Abschluss dieser Einheit sind die Teilnehmenden in der Lage, eine Datenschutz-Folgenabschätzung durchzuführen, zu dokumentieren, eine Risikoprüfung vorzunehmen und mögliche Abhilfemaßnahmen aus Unternehmenssicht zu ergreifen.

KI und Datenschutz: Die Herausforderungen
Künstliche Intelligenz stellt das Datenschutzrecht vor neue Herausforderungen. Die Teilnehmenden lernen anhand praktischer Fallbeispiele, wie datenschutzrechtliche Grundsätze wie Datenminimierung, Zweckbindung und Transparenz bei der Entwicklung und Nutzung von KI-Systemen eingehalten werden können. Es werden typische Problemstellungen, etwa bei der Nutzung von Trainingsdaten, der Erklärbarkeit von Ergebnissen sowie der Überwachung durch KI, behandelt. Die Teilnehmenden lernen, diese Problemlagen zu identifizieren und mit praxistauglichen Lösungsvorschlägen zu versehen. Zudem erlernen sie Methoden der Risikoanalyse im Umgang mit KI und erhalten das Rüstzeug, um als Datenschutzbeauftragte KI-Projekte in Unternehmen rechtlich fundiert zu begleiten.

Der/Die Datenschutzbeauftragte
Während dieser Einheit werden rechtliche Grundlagen der/des Datenschutzbeauftragten und deren/dessen Einbindung in Unternehmensstruktur dargestellt. Die Teilnehmenden lernen die Aufgaben der/des Datenschutzbeauftragten kennen und unter welchen Voraussetzungen diese/r geeignet für die Tätigkeit ist und bestellt bzw. abberufen werden kann. Zudem wird die Haftung der/des Datenschutzbeauftragten und die Verantwortung für Datenschutzverstöße im Unternehmen oder Konzern thematisiert. Abgeschlossen wird die Einheit mit der Behandlung praktischer Anwendungsfälle, damit auch in diesem Themenbereich die praktische Anwendung des theoretischen Wissens geschult wird und die Teilnehmenden ihre Transferkompetenz stärken. Hierdurch werden die Teilnehmenden auf eine eigene Tätigkeit als Datenschutzbeauftragte/r bzw. die Zusammenarbeit mit einer/einem Datenschutzbeauftragten vorbereitet.

Datenaufbewahrung und Datensicherheit
Im Fokus der Veranstaltung steht die Frage, durch welche technisch-organisatorischen Mittel die Datensicherheit im Unternehmen gewährleistet werden kann. Die Teilnehmenden lernen unterschiedliche Instrumente zur Verbesserung kennen und können dadurch ihre „Toolbox“ in der Beratung erweitern. Neben den rechtlichen Rahmenbedingungen werden insbesondere die Aspekte der Datenschutzaudits (Varianten, Planung, Ablauf, …), der Dokumentation und Umsetzung der Sicherheitskonzepte in der Praxis sowie mögliche Löschkonzepte dargestellt. So kann die Datensicherheit während der Aufbewahrung sichergestellt werden und verhindert werden, dass technische und datenschutzrechtliche Anforderungen an Löschkonzepte missachtet werden. Es wird zudem auf die Aspekte Outsourcing/Cloud Computing, Auftragsdatenverarbeitung (Art. 28 DSGVO) und IT Security (Art. 32 DSGVO) eingegangen. Einen Schwerpunkt der Veranstaltung bildet dabei die technische Weiterbildung der Teilnehmenden. Sie lernen die technischen Standards in der Datensicherheit (bspw. Backupverfahren, Anonymisierung und Cloud Computing) kennen und werden im Umgang mit Sicherheitslücken und Cyberangriffen geschult. Neben den technischen Grundlagen werden auch Aspekte der personellen Sicherheit (bspw. Kontrollen und Meldewege) thematisiert. In diesem Rahmen steht eine praxisnahe Weiterbildung der Teilnehmenden im Fokus der Veranstaltung, um in der späteren Beratungspraxis die Etablierung einer individuellen unternehmensinternen Lösung zu ermöglichen. Die Teilnehmenden sind nach der Einheit in der Lage, das eigene Unternehmen

in diesem Bereich zu beraten oder als externer Rechtsberater tätig zu werden.

Im zweiten Teil erhalten die Teilnehmenden nach einer Einführung in die Bedeutung des Datenschutzes für Transaktionen vermittelt, welcher datenschutzrechtlicher Rahmen bei Unternehmenstransaktionen zu beachten ist und welche Risiken für die Beteiligten bei etwaigen Verstößen bestehen. Die Teilnehmenden erlernen hierbei, durch welche Instrumente sie derartigen Verstößen präventiv begegnen können. Hierdurch wird ihnen eine praxisnahe Beratung im Rahmen von kommerziellen Transaktionen ermöglicht. Sie kennen mit Abschluss der Einheit die Bedeutung des Datenschutzes in den verschiedenen Phasen einer Transaktion und können rechtliche Risiken bei Transaktionen identifizieren und minimieren.

Rechte und Pflichten bei der Nutzung von KI in Unternehmen
In der Veranstaltung „Rechte und Pflichten bei der Nutzung von KI in Unternehmen“ werden die rechtlichen und datenschutzrechtlichen Anforderungen an Unternehmen beim Einsatz von Künstlicher Intelligenz behandelt. Die Teilnehmenden lernen die Verantwortlichkeiten der Unternehmen bei der Nutzung von KI und die Notwendigkeit zur Durchführung einer Datenschutz-Folgenabschätzung (DSFA) kennen. Ein weiterer Schwerpunkt liegt auf der Sicherstellung der Datenqualität und Transparenz in KI-Systemen, sowie der Einhaltung der Prinzipien der DSGVO bei der Implementierung von KI-Technologien. Die Einheit behandelt auch die Datensicherheit und den Schutz vor unbefugtem Zugriff auf KI-Daten und geht auf die Herausforderungen bei der automatisierten Entscheidungsfindung und Profiling gemäß der DSGVO ein. Zudem wird die Sicherstellung von Rechenschaftspflichten und Dokumentation im Zusammenhang mit KI-Systemen behandelt, um den rechtlichen Anforderungen gerecht zu werden und eine vertrauensvolle Nutzung von KI im Unternehmen zu gewährleisten.

Regulierung digitaler Plattformen
In der Veranstaltung „Regulierung digitaler Plattformen und von Hochrisiko-KI-Systemen“ werden die rechtlichen Anforderungen und regulatorischen Herausforderungen im Umgang mit digitalen Plattformen und Hochrisiko-KI-Systemen behandelt. Die Teilnehmenden lernen die relevanten Vorschriften, wie den EU-Digital Services Act (DSA) und den EU-KI-Rechtsrahmen in Form des Art. 6 I KI-VO, kennen und erfahren, wie diese die Verantwortung der Betreiber und Entwickler regeln. Besonderes Augenmerk liegt auf den Anforderungen an Transparenz, Fairness und den Schutz von Nutzern, sowie der Risikobewertung in Bezug auf KI-Systeme.

Ethische Fragestellungen im Umgang mit KI
In der Einheit„Ethische Fragestellungen im Umgang mit KI“ werden grundlegende Aspekte digitaler Ethik sowie die ethischen Herausforderungen beim Einsatz von Künstlicher Intelligenz behandelt. Die Teilnehmenden setzen sich mit der Herleitung eines Werterahmens für ethische KI, den Risiken für digital-ethische Werte sowie mit konkreten Ansätzen zur Operationalisierung ethischer Anforderungen in Unternehmen auseinander – etwa durch digital-ethische Due Diligence, AI Ethics Codes oder unternehmensinterne Governance-Strukturen. Ergänzend werden methodische Zugänge wie das Value Sensitive Design (VSD) und Konzepte wie Human-in-the-Loop-Supervision (HILS) vermittelt. Ziel der Veranstaltung ist es, die Teilnehmenden zu befähigen, ethische Risiken beim Einsatz von KI zu erkennen, unternehmensethische Maßnahmen zu entwickeln und eine verantwortungsvolle KI-Nutzung im Einklang mit gesellschaftlichen Werten sicherzustellen.

Einsatz von KI in der Praxis
In der Veranstaltung „Einsatz von KI in der Praxis“ werden praktische Anwendungen von Künstlicher Intelligenz in der juristischen Arbeit behandelt. Die Teilnehmenden beschäftigen mit dem perspektivischen und tatsächlichen Einsatz von KI-gestützten Technologien in Bereichen wie Due Diligence, juristischer Recherche und Predictive Analytics. Weitere Aspekte umfassen das Prompting, die automatisierte Vertragserstellung, Übersetzungen, die Vorbereitung von E-Mails sowie die Erstellung von Gerichtsakten und anderen juristischen Dokumenten. Ziel ist es, den Teilnehmenden zu vermitteln, wie KI-Prozesse effizienter gestaltet und die Qualität der juristischen Arbeit unterstützt.

Datenschutz/KI und Compliance
In der Veranstaltung „Datenschutz/KI und Compliance“ werden zentrale Fragestellungen im Spannungsfeld von Datenschutzrecht, Künstlicher Intelligenz und unternehmensbezogener Compliance behandelt. Die Teilnehmenden setzen sich mit der Überwachung von KI-Systemen, der Durchführung von Risikoanalysen sowie dem Aufbau wirksamer Risikomanagementstrukturen auseinander. Zudem werden KI-basierte Lösungen zur Compliance-Überwachung thematisiert und deren rechtliche und praktische Herausforderungen analysiert. Ziel der Veranstaltung ist es, die Teilnehmenden zu befähigen, Risiken beim Einsatz von KI-Systemen im Hinblick auf Datenschutz und Compliance zu erkennen, zu bewerten und angemessen zu steuern.

Folgenabschätzung und Best Practices
In der Veranstaltung „Folgenabschätzung und Best Practices“ werden die besten Praktiken für die datenschutzkonforme Nutzung von Künstlicher Intelligenz sowie Strategien zur Einhaltung der Datenschutzanforderungen in der KI-Entwicklung behandelt. Die Teilnehmenden lernen, wie Datenschutz-Folgenabschätzungen (DSFA) effektiv durchgeführt werden und wie Unternehmen den Anforderungen der DSGVO und anderer relevanter Regelungen in der Entwicklung von KI-Systemen gerecht werden können. Zudem wird ein Ausblick auf zukünftige Entwicklungen im Bereich Datenschutz und KI gegeben, um den Teilnehmenden zu ermöglichen, proaktiv auf kommende Herausforderungen zugehen zu können.

Datenschutz bei kommerziellen Transaktionen & internationale Datenübermittlung
Nach einer Einführung in die Bedeutung des Datenschutzes für Transaktionen wird den Teilnehmenden vermittelt, welcher datenschutzrechtliche Rahmen bei Unternehmenstransaktionen zu beachten ist und welche Risiken für die Beteiligten bei etwaigen Verstößen bestehen. Die Teilnehmenden erlernen, durch welche Instrumente sie derartigen Verstößen präventiv begegnen können. Hierdurch wird ihnen eine praxisnahe Beratung im Rahmen von kommerziellen Transaktionen ermöglicht. Sie kennen mit Abschluss der Einheit die Bedeutung des Datenschutzes in den verschiedenen Phasen einer Transaktion und können rechtliche Risiken bei Transaktionen identifizieren und minimieren.
Die internationale Datenübermittlung spielt in der Berufspraxis eine wichtige Rolle, daher lernen die Teilnehmenden die Grundsätze der DSGVO zur Datenübermittlung ins europäische und internationale Ausland kennen. In diesem Zusammenhang wird die Bedeutung eines Angemessenheitsbeschlusses für einen Datentransfer in Staaten, die außerhalb des europäischen Wirtschaftsraums liegen, dargestellt und Standardvertragsklauseln erörtert. Besondere Bedeutung hat dabei der Datentransfer in die USA, dessen Besonderheiten anhand des Schrems II-Urteils des Europäischen Gerichtshofs, dargestellt wird. Die Teilnehmenden wissen mit Abschluss dieser Einheit, in welchen Fällen ein Datentransfer ins Ausland möglich ist und welche rechtlichen Herausforderungen es zu beachten gilt. Sie können die aktuellen Entwicklungen nachvollzie-

hen, kritisch bewerten und Fragestellungen zum Themenbereich Datentransfer anhand der vermittelten Grundlagen lösen.

Schutz der Betroffenen und Haftung für Datenschutzverstöße/KI-VO Verstöße
In dieser Einheit werden die rechtlichen Mechanismen zum Schutz der betroffenen Personen im Kontext von Datenschutz und Künstlicher Intelligenz behandelt. Die Teilnehmenden beschäftigen sich mit der Herausforderung, wie die Rechte der Betroffenen, insbesondere in Bezug auf Transparenz, Auskunft und Löschung von Daten, schonend behandelt werden können. Ein weiterer Fokus liegt auf der Haftung für Datenschutzverstöße, einschließlich der Haftung bei Verstößen gegen die KI-Verordnung (KI-VO), sowie der Frage, wie Unternehmen und Verantwortliche für nicht datenschutzkonforme KI-Systeme zur Verantwortung gezogen werden können. Ziel der Veranstaltung ist es, den Teilnehmenden ein fundiertes Verständnis über die Haftungsrisiken zu vermitteln.

Aufsicht und Rechtsschutz
In diesem Abschnitt werden die Befugnisse der Aufsichtsbehörden im Datenschutzrecht sowie im Bereich der Künstlichen Intelligenz behandelt. Dabei wird die Stellung und Funktion der Aufsichtsbehörden (Art. 51 ff. DSGVO), ihre Befugnisse (Art. 55 ff. DSGVO) und das Kooperationsverfahren (Art. 66 ff. DSGVO) erläutert. Ein weiterer Fokus liegt auf der Aufsicht gemäß der KI-Verordnung (KI-VO), welche spezifische Anforderungen an die Überwachung von KI-Systemen stellt. Die Teilnehmenden lernen, wie sie sich gegen Aufsichtsmaßnahmen wehren können und wie sie den Rechtsschutz im Datenschutz und bei KI-Verstößen effektiv nutzen. Mit Abschluss der Veranstaltung sind die Teilnehmenden in der Lage, datenschutz- und KI-rechtliche Konflikte kompetent zu bewerten und eine zielführende Beratung anzubieten.

Das Datenschutzstrafrecht
Die Teilnehmenden lernen die Strafvorschriften im Datenschutzrecht kennen, sowie die Adressaten von strafrechtlichen Sanktionen. Weiter beleuchtet die Veranstaltung strafrechtliche Sanktionslücken für den schnelllebigen Bereich der KI-Technologien. Die Teilnehmenden lernen anhand von Use Cases und aktuell anhängigen Verfahren klassische Problemfelder kennen, wie die unbefugte Verarbeitung personenbezogener Daten, den Datenmissbrauch, unterbleibende Datenlöschung und Verstöße gegen Transparenzpflichten.

Lernergebnisse
Die Teilnehmenden kennen die rechtlichen Grundlagen des Themenfeldes und können diese in die praktische Beratung einbinden. Sie sind in der Lage, rechtliche Risiken zu identifizieren und durch einzelfallorientierte Lösungsmodelle zu minimieren. Die Kenntnis der rechtlichen Grundlagen und der zentralen Spezialprobleme ermöglicht den Teilnehmenden die kritische Einordnung der Rechtsprechung und Fachliteratur zum gesamten Themenkomplex Datenschutzrecht und somit die stets aktuelle Beratung in der Berufspraxis. Sie haben die Grundvoraussetzungen zur Etablierung eines Datenschutzkonzeptes in einem Unternehmen erworben und sind sich der enormen Relevanz der unternehmensinternen Kommunikation und Kultur bewusst. Zudem verfügen die Teilnehmenden über fundierte KI-Kompetenz iSd. Art. 4 I KI-VO, welche sie dazu befähigt, einen verantwortungsvollen Einsatz von KI in Unternehmen zu prüfen, überwachen und sicherzustellen. Sie wissen um Risiken und Chancen bei Einsatz von künstlicher Intelligenz in verschiedensten Betätigungsfeldern. Ebenso sind ihnen die Verbindungen von Datenschutz und KI präsent.

3	Aufbau				
Komponenten des Lehrgangs					
Nr.	LV-Kategorie	Lehrveranstaltung	Status (P/WP)	Workload (h)	
				Präsenzzeit (h)	Selbststudium (h)
1.	Vorlesung	Einführung in das Datenschutzrecht	P	3,75	6,25
2.	Vorlesung	Einführung in die rechtlichen Grundlagen von KI	P	3,75	5,5
3.	Seminar	Kundendatenschutz (inkl. Datenschutz im Marketing)	P	3,75	3,75
4.	Seminar	Beschäftigtendatenschutz	P	3,75	3,75
5.	Seminar	Datenschutz-Folgenabschätzung und Datenschutz durch Technik	P	3,75	3,75
6.	Seminar	KI und Datenschutz: Die Herausforderungen	P	3,75	3,75
7.	Seminar	Der/Die Datenschutzbeauftragte	P	3,75	3,75
8.	Seminar	Datenaufbewahrung und Datensicherheit	P	3,75	3,75
9.	Seminar	Rechte und Pflichten bei der Nutzung von KI in Unternehmen	P	3,75	3,75
10.	Vorlesung	Regulierung digitaler Plattformen und von Hochrisiko KI-Systemen	P	1,5	1,5
11.	Seminar	Ethische Fragestellungen im Umgang mit KI	P	1,5	1,5
12.	Seminar	Einsatz von KI in der Praxis	P	1,5	1,5
13.	Seminar	Datenschutz/KI und Compliance	P	3,75	3,75
14.	Seminar	Folgenabschätzung und Best Practices	P	3,0	3,75
15.	Seminar	Datenschutz bei kommerziellen Transaktionen und internationale Datenübermittlung	P	3,75	3,75
16.	Seminar	Schutz der Betroffenen und Haftung für Datenschutzverstöße/KI-VO Verstöße	P	3,75	3,75
17.	Seminar	Datenschutzaufsicht und Rechtsschutz Aufsichtsrecht nach der KI-VO	P	3,75	3,75
18.	Seminar	Das Datenschutzstrafrecht	P	3,75	3,75
					50
				60	**115**
				175	
Wahlmöglichkeiten innerhalb des Lehrgangs			Keine		

4	Prüfungskonzeption				
Prüfungsleistung(en)					
Nr.	MAP/ MTP	Art	Dauer/ Umfang	ggf. Anbindung an LV Nr.	Gewichtung Note
1	MTP	Einsendeaufgabe	Dauer: 1 Monat Bearbeitungszeitraum zwischen zwei vorgegebenen Terminen wählbar, Umfang: 10-12 DIN A4-Seiten	-	100 %
2	MTP	Gruppen-Präsentationsprüfung	insgesamt 5 Stunden (bei 5 Gruppen): Bearbeitungszeit: 30 Minuten Vortrag pro Gruppe: 10 Minuten Rückfragen durch Prüfende: 10 Minuten Feedback: 10 Minuten	-	0 %
Gewichtung für die Gesamtnote		100 %			
Studienleistung(en)					
Nr.	Art		Dauer/ Umfang	ggf. Anbindung an LV Nr.	
	-				

5	Voraussetzungen
Teilnahmevoraussetzungen	Einschlägige Berufserfahrung von mindestens drei Jahren bzw. abgeschlossenes Hochschulstudium und einschlägige Berufserfahrung von mindestens einem Jahr
Vergabe von Leistungspunkten	Die Leistungspunkte werden vergeben, wenn der Lehrgang insgesamt erfolgreich abgeschlossen wurde, d.h., wenn der/die Teilnehmende an 75 % der Unterrichtsstunden teilgenommen hat und wenn durch das Bestehen der Prüfungsleistung nachgewiesen wurde, dass die zugeordneten Lernergebnisse erworben wurden.
Regelungen zur Anwesenheit	Anwesenheitspflicht an 75 % der Unterrichtseinheiten Anwesenheitspflicht während der Prüfung

6	Angebot des Lehrgangs
Turnus/Taktung	Jährlich
Lehrgangsbeauftragte/r	Prof. Dr. Jan-Frederick Göhsl LL.M. (UCL)
Anbietender Fachbereich	Rechtswissenschaften (FB 03)

7	**Mobilität/Anerkennung**
Verwendbarkeit in anderen Studiengängen	./.
Lehrgangssprache	**Deutsch**
Lehrgangstitel englisch	**Data Protection Law & AI**