Modulhandbuch

zum weiterbildenden Masterstudiengang

Datenschutzrecht (LL.M.)

der

FernUniversität in Hagen

Stand: 01.08.2024

Module des Masterstudiengangs Datenschutzrecht (LL.M.)

Exemplarischer Studienverlaufsplan

60-ECTS-Variante (Zugang mit 240 ECTS)

Vollzeitstudium

Lfd. Nr.	Modul-Nr.	Titel	ECTS
		1. SEMESTER	
1		Einführung und Grundlagen des Datenschutzrechts	10
2		Rechtlicher Rahmen für Datenverarbeitung und Informationspflichten	10
3		Betroffenenrechte, Beschäftigtendatenschutz, technischer Datenschutz	10
		2. SEMESTER	
4		Wahlmodul	10
5		Masterarbeit	20
		SUMME	60

Teilzeitstudium

Lfd. Nr.	Modul-Nr.	Titel	ECTS
		1. SEMESTER	
1		Einführung und Grundlagen des Datenschutzrechts	10
2		Rechtlicher Rahmen für Datenverarbeitung und Informationspflichten	10
		2. SEMESTER	
3		Betroffenenrechte, Beschäftigtendatenschutz, technischer Datenschutz	10
4		Wahlmodul	10
		3. SEMESTER	
5		Masterarbeit	20
		SUMME	60

90-ECTS-Variante (Zugang mit 210 ECTS)

Vollzeitstudium

Lfd. Nr.	Modul-Nr.	Titel	ECTS
		1. SEMESTER	
1		Einführung und Grundlagen des Datenschutzrechts	10
2		Rechtlicher Rahmen für Datenverarbeitung und Informationspflichten	10
3		Betroffenenrechte, Beschäftigtendatenschutz, technischer Datenschutz	10
		2. SEMESTER	
4		Zivil-, verwaltungs- und sanktionsrechtliche Folgen bei Verstößen gegen datenschutzrechtliche Bestimmungen und Rechtsschutz	10
5		Leading Cases Datenschutzrecht	10
6		Wahlmodul	10
		3. SEMESTER	
7		Wahlmodul	10
8		Masterarbeit	20
		SUMME	90

Teilzeitstudium

Lfd. Nr.	Modul-Nr.	Titel	ECTS
		1. SEMESTER	
1		Einführung und Grundlagen des Datenschutzrechts	10
2		Rechtlicher Rahmen für Datenverarbeitung und Informationspflichten	10
		2. SEMESTER	
3		Betroffenenrechte, Beschäftigtendatenschutz, technischer Datenschutz	10
4		Zivil-, verwaltungs- und sanktionsrechtliche Folgen bei Verstößen gegen datenschutzrechtliche Bestimmungen und Rechtsschutz	10
		3. SEMESTER	
5		Leading Cases Datenschutzrecht	10
6		Wahlmodul	10
		4. SEMESTER	
7		Wahlmodul	10
		5. SEMESTER	
8		Masterarbeit	20
		SUMME	90

Modulbeschreibungen

I. Pflichtmodule

<table>
<tr><th colspan="7">Einführung und Grundlagen des Datenschutzrechts</th></tr>
<tr><td colspan="2">Kennnummer
71101</td><td>Workload
300 Stunden</td><td>ECTS
10</td><td>Studiensemester
1. Semester</td><td>Häufigkeit des Angebots
Jedes Semester</td><td>Dauer
1 Semester</td></tr>
<tr><td>1</td><td colspan="2">Fernstudienkurse
Teil 1: Einführung in das Datenschutzrecht (Geschichte und Überblick)
Teil 2: Grundlagen des Datenschutzrechts I – Anwendungsbereich und Grundsätze
Teil 3: Grundlagen des Datenschutzrechts II – Wesentliche Begriffe, Beteiligte Personen
Teil 4: Grundlagen des Datenschutzrechts III - Rechtsfolgen von Datenschutzverstößen
Modulabschlussprüfung</td><td colspan="2">Workload
75 h
90 h
90 h
15 h
30 h</td><td colspan="2">Kreditpunkte
2,5
3
3
0,5
1</td></tr>
<tr><td>2</td><td colspan="6">Lernergebnisse (learning outcomes) / Kompetenzen:
Die Studierenden sind über die geschichtliche Entwicklung und den Aufbau des Datenschutzrechts einschließlich seiner Querbezüge sowie über die Grundlagen zu den Rechtsfolgen bei Datenschutzverstößen im Bilde und verfügen über solide Kenntnisse über die grundlegenden Begriffe des Datenschutzrechts, um sich im weiteren Verlauf mit den Fragestellungen über die Rechtmäßigkeit der Datenverarbeitung auseinanderzusetzen und besondere Erscheinungsformen des Datenschutzes in der Praxis lösungsorientiert zu würdigen.</td></tr>
<tr><td>3</td><td colspan="6">Inhalte:

<u>Teil 1: Einführung in das Datenschutzrecht (Geschichte und Überblick)</u>

Teil 1 behandelt die Geschichte des Datenschutzrechts von seinen Ursprüngen im Privat- und Geheimsphärenschutzes bis zu den ersten nationalen Datenschutzregelungen (1.1), um anschließend den Fokus auf den Einfluss des Unionsrechts (1.2) und insbesondere die europäische Datenschutzreform des Jahres 2016 zu lenken. Der Blick auf die Geschichte des Datenschutzrechts hilft dabei, die Frage zu beantworten, wovor das Datenschutzrecht schützen soll sowie bei der Auslegung seiner Regelungen.
Unter Bezugnahme auf die Rechtsprechung wird herausgearbeitet, dass die Übermittlung von personenbezogenen Daten ein Eingriff in ein Grundrecht darstellt, der einer Rechtfertigung bedarf und</td></tr>
</table>

dass das Prinzip der Zweckbindung gilt, wonach ein bestimmter Zweck im Voraus feststehen muss, um einen Datenverarbeitungsvorgang rechtfertigen zu können.
Es wird klargestellt, wann es erstmals einen Datenschutzbeauftragten gab, nämlich mit dem hessischen Willi Birkelbach im Jahre 1971. Die gesetzgeberische Entwicklung des im Datenschutzrecht geltenden Prinzips des Verbots mit Erlaubnisvorbehalt wird nachvollzogen.
Dargestellt werden wesentliche Punkte wie die Verabschiedung des ersten Bundesdatenschutzgesetzes (1977), das Volkszählungsurteil des Bundesverfassungsgerichts vom 15. Dezember 1983, welches das Grundrecht auf informationelle Selbstbestimmung als Bestandteil des allgemeinen Persönlichkeitsrechtes gemäß Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG formulierte, sowie das Inkrafttreten des zweiten Bundesdatenschutzgesetzes im Jahre 1991.

Teil 1 gibt einen **Überblick über das geltende Recht**. Die datenschutzrechtlichen Regelungen werden in ihren Quellen und ihrer Systematik sowie in ihren Querbezügen erörtert und von anderen Regelungsbereichen abgegrenzt. Es werden die wichtigsten Rechtsquellen auf internationaler Ebene (2.1) im Unionsrecht (2.1.1) und Völkerrecht (2.1.2) sowie auf nationaler Ebene (2.2) im Verfassungsrecht (2.2.1) und einfachen Recht (2.2.2) behandelt.

Zunächst wird der Einfluss des Unionsrechts und dort die Datenschutzrichtlinie von 1995 sowie natürlich die Datenschutzgrundverordnung, welche die Richtlinie mit Wirkung zum 25. Mai 2018 aufhob, thematisiert. Des Weiteren wird auf die Datenschutzrichtlinie für Justiz und Inneres eingegangen. In Bezug auf das Völkerrecht ist die Europäische Menschenrechtskonvention und dort Art. 8 Abs. 1 sowie die Datenschutzkonvention des Europarats relevant.

Auf nationaler Ebene sind verfassungsrechtliche wie einfachgesetzliche Vorgaben für den Datenschutz zu beachten. Im deutschen Verfassungsrecht ist für den Datenschutz vor allem das Recht auf informationelle Selbstbestimmung maßgeblich. Einfachgesetzliche nationale Regelungen nutzen die Öffnungsklauseln der DSGVO bzw. die Umsetzungsspielräume der Datenschutzrichtlinie für Justiz und Inneres. Zentrales Regelwerk auf Bundesebene ist das Bundesdatenschutzgesetz. Es gilt grundsätzlich für öffentliche Stellen des Bundes und für nicht-öffentliche Stellen. Die Landesdatenschutzgesetze gelten für öffentliche Stellen der Länder. Für die Abgrenzung von Bundes- und Landesdatenschutzgesetzen kommt es darauf an, wer die Verarbeitung personenbezogener Daten vornimmt.

Schließlich werden die **Querbezüge** des „engen" Datenschutzrechts zu anderen Regelungsbereichen des Daten- und Informationstechnikrechts (etwa zum Data Act, Digital Services Act, zur KI-Verordnung oder zum IT-Sicherheitsrecht) dargelegt. Diese gesamtheitliche Betrachtung nimmt angesichts der zunehmenden Verflechtung der Regelungsbereiche und der rechtlich wie tatsächlich zu bewältigenden Sachverhalte stetig an Bedeutung zu.

Der Studienbrief zu Teil 1 enthält am Ende eine Aufstellung über weitere Lern- und Erkenntnisquellen, die für das weitere Studium, aber auch darüber hinaus für die persönliche und berufliche Weiterbildung nützlich sind.

<u>Teil 2: Grundlagen des Datenschutzrechts I – Anwendungsbereich und Grundsätze</u>

Mit diesem Teil beginnt der Einstieg in das Studium der Datenschutz-Grundverordnung (DS-GVO). Der Studienbrief folgt dabei den Regelungen der DS-GVO: vom sachlichen über den räumlichen Anwendungsbereich bis zu den Grundsätzen der DS-GVO.

Der **sachliche Anwendungsbereich** (Art. 2) ist sehr weit. Zwar scheint die DS-GVO durch ihre Beschränkung auf automatisierte Datenverarbeitungen zumindest die Arbeit mit Papier von ihrer Anwendung auszunehmen. Jedoch erfasst sie auch nichtautomatisierte Datenverarbeitungen, wenn sie in einem Dateisystem erfolgen. Das bedeutet, dass die DS-GVO nicht nur für Daten im Computer, sondern auch für Daten in Papierakten gilt. Im Ergebnis gibt es kaum noch einen Lebens- und Arbeitsbereich, der nicht von der DS-GVO erfasst wird. Allerdings gibt es verschiedene Ausnahmen:

- Auf Lebenssachverhalte, für die die EU keine Regelungskompetenz hat, findet die DS-GVO keine Anwendung. Gleiches gilt für den Bereich der Gemeinsamen Außen- und Sicherheitspolitik.

- Die sogenannte „Haushaltsausnahme" nimmt rein private Tätigkeiten vom Anwendungsbereich aus. Hier stellen sich spannende Abgrenzungsfragen insbesondere bei der Nutzung sozialer Medien.

- Für Polizei und Justiz gilt nicht die DS-GVO, sondern die Datenschutz-Richtlinie 2016/280. Auch hier stellen sich spannende Abgrenzungsfragen. Auch für das Handeln der EU-Einrichtungen gilt nicht die DS-GVO. Hier gibt es mit der Richtlinie 2018/1725 ebenfalls eine eigene Rechts-grundlage.

- Schließlich stellen sich komplizierte Abgrenzungsfragen bei Datenverarbeitungen des elektro-nischen Geschäftsverkehrs. Hierfür gilt derzeit noch die ePrivacy-Richtlinie 2000/31, die aber überarbeitet wird und durch eine Verordnung abgelöst werden soll.

Der **räumliche Anwendungsbereich** (Art. 3) ist ebenfalls sehr weit. Nach dem sogenannten „Marktortprinzip" reicht es für die Anwendung der DS-GVO aus, dass ein Verantwortlicher in der EU Waren oder Dienstleistungen anbietet oder das Verhalten eines Betroffenen in der EU beobachtet.

Ein Schwerpunkt dieses Teils ist die Erörterung der **Grundsätze der Datenverarbeitung** (Art. 5). Die Rechtsqualität der Grundsätze ist zwar unklar und umstritten. Anhand der Grundsätze „Rechtmäßigkeit", „Treu und Glauben", „Transparenz", „Zweckbindung", „Datenminimierung", „Richtigkeit", „Speicherbegrenzung", „Integrität und Vertraulichkeit" und „Rechenschaftspflicht" lässt sich jedoch ein Großteil des Datenschutzrechts erläutern. Hierfür werden exemplarisch Bezüge der jeweiligen Grundsätze zu einzelnen Regelungen der DS-GVO aufgezeigt. Die Bedeutung der Grundsätze wird anhand von Beispielsfällen anschaulich gemacht.

<u>Teil 3: Grundlagen des Datenschutzrechts II – Wesentliche Begriffe, Beteiligte Personen</u>

Teil 3 behandelt in einem ersten Abschnitt die **Grundbegriffe des Datenschutzrechts**. Dabei werden insbesondere die „personenbezogene Daten" (Art. 4 Nr. 1 DSGVO) und die „Verarbeitung" (Art. 4 Nr. 2 DSGVO), einschließlich ihrer jeweiligen datenschutzrechtlich relevanten Abstufungen, thematisiert. Es werden die an der Verarbeitung Beteiligten, nämlich Verantwortlicher, Auftragsverarbeiter, Dritte und Empfänger dargestellt (Art. 4 Nr. 7 bis 11 DSGVO). Überdies erfolgt eine Einordnung von Unternehmen und Konzernen einerseits und von Behörden und sonstigen öffentlichen Stellen andererseits in die Systematik des Datenschutzrechts. In Bezug auf letztere wird die DSGVO maßgeblich durch das BDSG ergänzt.

Ein Schwerpunkt von Teil 3 liegt in der **Darstellung des Verhältnisses von betroffenen Personen, Verantwortlichen und Auftragsverarbeitern**. Dabei wird die in der Praxis wichtige Abgrenzung von (Einzel-)Verantwortlichkeit, gemeinsamer Verantwortlichkeit und Auftragsverarbeitung vorgenommen. Es werden die wesentlichen datenschutzrechtlichen Pflichten der jeweils beteiligten Akteure, soweit sie nicht in anderen Teilen behandelt werden, beleuchtet.

	Im Rahmen der gemeinsamen Verantwortlichkeit i. S. d. Art. 4 Nr. 7 und Art. 26 DSGVO werden die maßgeblichen Kriterien, der Umfang und die Rechtsfolgen unter Berücksichtigung der einschlägigen Rechtsprechung des Europäischen Gerichtshofs (insbesondere „Wirtschaftsakademie Schleswig-Holstein" und „Fashion ID") dargestellt. Es wird die Rechtsfigur der Auftragsverarbeitung beleuchtet (Art. 4 Nr. 8 und Art. 28 DSGVO). Hierbei liegt der Fokus auf den formellen und materiellen Anforderungen an die Einschaltung von Dienstleistern, ihren Rechtsfolgen und der Einbindung von Unter-Auftragnehmern. In beiden Szenarien der datenschutzrelevanten Kollaboration mehrerer Akteure stellen sich spezifische Haftungsfragen. Die in der Praxis bedeutsamem Haftungsregelungen und damit einhergehende Herausforderungen bei der Vertragsgestaltung werden dargestellt. Zuletzt skizziert Teil 3 in einem Überblick die **Rolle der Datenschutzaufsichtsbehörden**. Es wird auf die verschiedenen Aufsichtsbehörden in Deutschland und in der Europäischen Union, einschließlich ihrer Gremien, eingegangen. Zudem werden der Mechanismus der Bestimmung der zuständigen Aufsichtsbehörde sowie die Aufgaben und Befugnisse der Aufsichtsbehörden, einschließlich der Sanktionierung von Datenschutzverstößen, dargestellt. <u>Teil 4: Grundlagen des Datenschutzrechts III – Rechtsfolgen von Datenschutzverstößen</u> Neben den verschriftlichen Teilen zu den oben genannten Themen enthält Modul 71101 auch Video-Vorlesungen über die **Grundlagen zu den Rechtsfolgen von Datenschutzverstößen**. Angesichts der überragenden Bedeutung der Folgen eines datenschutzrechtswidrigen Verhaltens gilt es, in einem ersten Überblick die jeweiligen Perspektiven im Zivil-, Verwaltungs- und Sanktionenrecht einzeln zu beleuchten und an entsprechenden Stellen das Ineinandergreifen verschiedener Rechtsfolgen in Ansätzen darzustellen. Ein besonderes Augenmerk liegt dabei konsequenterweise auf den Abwehrmöglichkeiten durch effektiven Rechtsschutz, dessen Grundzüge ebenfalls behandelt werden.
4	**Lehr-/Lernformen und Lehrmaterialien:** Fernstudium im Blended-Learning Mix, bestehend aus schriftlichen Lehreinheiten, denen eine Lernzielbestimmung im Video-Format vorgeschaltet wird. Lehrbegleitend wird ein Online-Angebot auf der virtuellen Lernplattform *Moodle*, eingesetzt, dieses besteht u. a. aus hybriden Betreuungsveranstaltungen.
5	**Teilnahmevoraussetzungen:** Siehe § 5 der Prüfungsordnung für den weiterbildenden Masterstudiengang Datenschutzrecht (LL.M)
6	**Prüfungsformen:** (Kurz-)Hausarbeit
7	**Voraussetzungen für die Vergabe von Leistungspunkten:** Bearbeitung des Moduls und Bestehen der Modulabschlussprüfung
8	**Verwendung des Moduls:** Weiterbildender Masterstudiengang Datenschutzrecht (LL.M.)
9	**Stellenwert der Note für die Endnote:** Siehe § 23 der Prüfungsordnung für den weiterbildenden Masterstudiengang Datenschutzrecht (LL.M.)
10	**Modulverantwortliche:** 1. Prof. Dr. Golla 2. Prof. Dr. Golland 3. Dr. Veil

	4. Dr. Koreng 5. Dr. Ihwas 6. Schild
11	**Sonstige Informationen:**

Rechtlicher Rahmen für Datenverarbeitung und Informationspflichten

Kennnummer	Workload	ECTS	Studiensemester	Häufigkeit des Angebots	Dauer
71102	300 Stunden	10	1. Semester	Jedes Semester	1 Semester

1	Fernstudienkurse	Workload	Kreditpunkte
	Teil 1: Materielle Rechtmäßigkeit von Datenverarbeitung I	90 h	3
	Teil 2: Materielle Rechtmäßigkeit von Datenverarbeitung II	90 h	3
	Teil 3: Informations- und Dokumentationspflichten	90 h	3
	Modulabschlussprüfung	30 h	1

2 Lernergebnisse (learning outcomes) / Kompetenzen:

Die Studierenden haben die Kompetenz, sicher mit den materiell-rechtlichen Grundlagen der Datenverarbeitung umzugehen. Sie können erkennen, auf welche Erlaubnistatbestände abzustellen ist und welche Besonderheiten dabei bestehen, die zu beachten sind. Sie erlernen daneben den kompetenten Umgang mit den datenschutzrechtlichen Informations- und Dokumentationspflichten. Insgesamt sind sie nach Bearbeitung des Moduls in der Lage, den Massenanfall von Daten im (Geschäfts-)Alltag rechtlich einzuordnen und für etwaige Konfliktfälle problembewusste Vorschläge zu erarbeiten.

3 Inhalte:

Teil 1: Materielle Rechtmäßigkeit von Datenverarbeitung I

Teil 1 behandelt im ersten Abschnitt den **Zweckbindungsgrundsatz** und im zweiten Abschnitt den **Grundsatz einer Rechtsgrundlage für jede Verarbeitung I**, wobei der Autor stets neben inhaltlichen Ausführungen einen Bezug zu Praxisfällen durch Fallbeispiele herstellt, die der Verständlichkeit dienen.

Nach Bearbeitung des Abschnitts zum „Zweckbindungsgrundsatz" sind die Studierenden in der Lage rechtlich zu bewerten, ob in einem praktischen Fall gegen den Grundsatz der Zweckbindung verstoßen wird und (schon) deswegen eine Verarbeitung personenbezogener Daten materiell rechtswidrig ist. Es werden die zwei „Teil-Grundsätze", aus denen der Zweckbindungsgrundsatz besteht – Zweckfestlegung und Zweckbindung im engeren Sinne – erläutert. Nach einem vergleichenden Blick auf die Rechtslage vor Geltungsbeginn der DSGVO werden jeweils der Anwendungsbereich sowie die Voraussetzungen der „Teil-Grundsätze" Zweckfestlegung und Zweckbindung im engeren Sinne erläutert. Schließlich werden ihre Rechtsfolgen verdeutlicht. Im Anschluss geht es um Ausnahmen vom Zweckbindungsgrundsatz im engeren Sinne, die – anders als für den Grundsatz der Zweckfestlegung – durch Rechtsnormen vorgesehen sind.

Nach Bearbeitung des Abschnitts zum „Grundsatz einer Rechtsgrundlage für jede Verarbeitung I" sind die Studierenden in der Lage rechtlich zu beurteilen, ob in einem praktischen Fall eine Rechtsgrundlage für die Verarbeitung personenbezogener Daten gegeben ist und was das für die materielle Rechtmäßigkeit der Verarbeitung bedeutet. Sie lernen vor allem die für die unternehmerische

Tätigkeit wichtigsten Rechtsgrundlagen in Art. 6 Abs. 1 lit. b und lit. f DSGVO und deren Voraussetzungen kennen und können überprüfen, ob diese im Einzelfall vorliegen. Die Studierenden werden zudem befähigt, die Bedeutung des Fehlens oder Gegeben-Seins einer Rechtsgrundlage zu erkennen und Schlüsse hieraus zu ziehen. Darüber hinaus werden die Studierenden die Grundzüge des Art. 9 DSGVO beherrschen, der die Verarbeitung sog. sensibler Daten regelt. Die Rechtsgrundlage der Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO ist Teil 2 über die materielle Rechtmäßigkeit von Datenverarbeitung II vorbehalten. Wie bereits im ersten Abschnitt wird auch in diesem Kapitel ein Blick auf die Rechtslage vor Geltungsbeginn der DSGVO geworfen, da diesbezügliche Rechtsprechung und Literatur im Wege der historischen Auslegung datenschutzrechtlicher Vorschriften Bedeutung erlangen. Im Rahmen des Anwendungsbereichs wird klargestellt, dass der Grundsatz, dass jede Verarbeitung jedweder personenbezogenen Daten einer Rechtsgrundlage gem. Art. 6 Abs. 1 lit. a bis f DSGVO bedarf, in der Praxis allgegenwärtig ist und welche Konsequenzen dies für den datenschutzrechtlichen Berater mit sich bringt. Vor der Darstellung einzelner Rechtsgrundlagen findet eine Abgrenzung zu anderen Grundsätzen bzw. Vorgaben, die die materielle Rechtmäßigkeit von Datenverarbeitungen ebenfalls betreffen, statt. Neben dem Zweckbindungsgrundsatz sind dies der Grundsatz der Datenminimierung und der Grundsatz der (zeitlichen) Speicherbegrenzung. Außerdem wird das Verhältnis der Rechtsgrundlagen gem. Art. 6 Abs. 1 DSGVO zu Art. 9 DSGVO diskutiert. Am Ende wird ein Ausblick auf Teil 2 „Materielle Rechtmäßigkeit von Datenverarbeitung II“ gegeben.

Teil 2: Materielle Rechtmäßigkeit von Datenverarbeitung II

Teil 2 behandelt im ersten Abschnitt den Grundsatz einer **Rechtsgrundlage für jede Verarbeitung II** und im zweiten Abschnitt den **Grundsatz eines angemessenen Schutzniveaus für Übermittlungen in Drittländer**. Neben den inhaltlichen Ausführungen stellt der Autor stets einen Praxisbezug durch zahlreiche Fallbeispiele her, welche der besseren Verständlichkeit dienen.

Nach der Bearbeitung des Abschnitts zum „Grundsatz einer Rechtsgrundlage für jede Verarbeitung II“ sind die Studierenden in der Lage rechtlich zu beurteilen, ob in einem praktischen Einzelfall eine der hier behandelten Rechtsgrundlagen für die Verarbeitung personenbezogener Daten gegeben ist. Zu diesem Zwecke wird an die in Teil 1 begonnene Darstellung wichtiger Normen angeknüpft. Der Blick liegt zunächst auf Art. 6 Abs. 1 lit. c DSGVO und sodann auf der Einwilligung gem. Art. 6 Abs. 1 lit. a DSGVO. Neben den jeweiligen Voraussetzungen dieser Normen werden im Rahmen der Einwilligung zudem grundsätzliche Erwägungen angestellt und eine Abgrenzung zu anderen Rechtsgrundlagen sowie Grundsätzen der materiellen Rechtmäßigkeit von Datenverarbeitung vorgenommen. Allem vorangestellt findet ein vergleichender Blick auf die Rechtslage vor Geltungsbeginn der DSGVO statt.

Nach Bearbeitung des Abschnitts zum „Grundsatz eines angemessenen Schutzniveaus für Übermittlungen in Drittländer“ sind die Studierenden in der Lage rechtlich zu bewerten, ob in einem praktischen Fall gegen diesen verstoßen wird und deswegen die betreffende Übermittlung personenbezogener Daten materiell rechtswidrig ist. Es erfolgt zunächst eine kurze Einführung in die Thematik ehe dann näher auf den Grundsatz im Einzelnen eingegangen wird. Innerhalb dessen findet eine ausführliche Darstellung des Anwendungsbereiches sowie der notwendigen Voraussetzungen des Grundsatzes eines angemessenen Schutzniveaus und der Rechtsfolge im Falle eines Verstoßes statt. Abschließend erfolgt ein kurzer Überblick über mögliche Angemessenheitsbeschlüsse der Europäischen Kommission nach Art. 45 DSGVO. Wie bereits im ersten Abschnitt wird auch in diesem Kapitel ein Blick auf die Rechtslage vor Geltungsbeginn der DSGVO geworfen, da sich vor allem Art. 25 f. der EG-Datenschutzrichtlinie für die Auslegung der Art. 44 ff. DSGVO als hilfreich erweist. Als Alternative zum angemessenen Schutzniveau werden die Studierenden sodann mit den im Einzelfall

	„geeigneten Garantien" gem. Art. 46 Abs. 1 DSGVO vertraut gemacht. Im Rahmen dessen werden die für Datenübermittlungen durch Unternehmen wichtigsten geeigneten Garantien erläutert. Für das Vorliegen der Übermittlung personenbezogener Daten an einen Empfänger außerhalb des EWR, welche weder durch den Grundsatz eines angemessenen Schutzniveaus noch durch geeignete Garantien gedeckt sind, werden zusätzlich Ausnahmen gem. Art. 49 DSGVO aufgezeigt. Der Abschnitt endet sodann mit dem Vergleich zwischen den Anforderungen für Übermittlungen personenbezogener Daten in Länder außerhalb des EWR und dem ausdrücklichen Verbot ebensolcher Anforderungen für Übermittlungen an einen Empfänger in der EU. Teil 3: Informations- und Dokumentationspflichten Teil 3 behandelt im ersten Abschnitt die **Informationspflichten** und im zweiten Abschnitt die **Dokumentationspflichten** des geltenden Datenschutzrechts. Hinsichtlich der Informationspflichten wird zunächst die primärrechtliche Verwurzelung der Transparenz behandelt, da personenbezogene Daten in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden müssen und dieser Grundsatz seine Grundlage in der europäischen Grundrechtecharta findet. Anschließend geht es um die einzelnen Informationspflichten in der DSGVO als Ausprägung des Transparenzgrundsatzes und deren Form und Inhalt. Es werden zunächst die beiden prominentesten Informationspflichten aus den Artikeln 13 und 14 DSGVO beleuchtet. Danach werden Verstöße gegen Informationspflichten samt Rechten bzw. Ansprüchen von Betroffenen nach Verstößen, Sanktionen und Rechtsschutzmöglichkeiten thematisiert. Schließlich geht es um das Auskunftsrecht aus Art. 15 DSGVO, welches sich von den Informationspflichten aus Artt. 13 und 14 DSGVO dadurch unterscheidet, dass der Verantwortliche nach Art. 15 DSGVO erst nach einem von der betroffenen Person geltend gemachten Auskunftsverlangen verpflichtet wird, während er zur Informationserteilung nach Artt. 13 und 14 DSGVO auch ohne vorherige Handlung der betroffenen Person verpflichtet ist. Sodann werden weitere aktive Informationspflichten aus der DSGVO dargestellt. Abschließend werden einzelne Anwendungsbeispiele wie Informationspflichten bei der Einwilligung, die Datenschutzerklärung auf Internetseiten, Informationspflichten in der App und bei der Videoüberwachung behandelt. Im Rahmen der Dokumentationspflichten geht es insbesondere um den Inhalt von Verarbeitungsverzeichnissen. Hierbei wird zwischen Verarbeitungsverzeichnissen von Verantwortlichen einerseits und Verarbeitungsverzeichnissen von Auftragsverarbeitern andererseits differenziert.
4	**Lehr-/Lernformen und Lehrmaterialien:** Fernstudium im Blended-Learning Mix, bestehend aus schriftlichen Lehreinheiten, denen eine Lernzielbestimmung im Video-Format vorgeschaltet wird. Lehrbegleitend wird ein Online-Angebot auf der virtuellen Lernplattform *Moodle*, eingesetzt, dieses besteht u. a. aus hybriden Betreuungsveranstaltungen.
5	**Teilnahmevoraussetzungen:** Siehe § 5 der Prüfungsordnung für den weiterbildenden Masterstudiengang Datenschutzrecht (LL.M)
6	**Prüfungsformen:** (Kurz-)Hausarbeit
7	**Voraussetzungen für die Vergabe von Kreditpunkten:** Bearbeitung des Moduls und Bestehen der Modulabschlussprüfung
8	**Verwendung des Moduls:** Weiterbildender Masterstudiengang Datenschutzrecht (LL.M.)
9	**Stellenwert der Note für die Endnote:**

	Siehe § 23 der Prüfungsordnung für den weiterbildenden Masterstudiengang Datenschutzrecht (LL.M.)
10	**Modulverantwortliche:** 1. Dr. Ziegenhorn 2. Dr. Ziegenhorn 3. Dr. Werner
11	**Sonstige Informationen:**

Betroffenenrechte, Beschäftigtendatenschutz, technischer Datenschutz

Kennnummer	Workload	ECTS	Studiensemester	Häufigkeit des Angebots	Dauer
71103	300 Stunden	10	1.-2. Semester (je nach Var.)	Jedes Semester	1 Semester

1	Fernstudienkurse	Workload	Kreditpunkte
	Teil 1: Beschäftigtendatenschutz	90 h	3
	Teil 2: Rechte der betroffenen Personen & Datenschutzbeauftragter	90 h	3
	Teil 3: Technische und organisatorische Maßnahmen (TOM)	90 h	3
	Modulabschlussprüfung	30 h	1

2 Lernergebnisse (learning outcomes) / Kompetenzen:

Nachdem sich die Studierenden in den vorherigen Modulen mit den rechtlichen Grundbegriffen und -lagen des Datenschutzrechtes vertraut gemacht haben, wenden sie ihre Erkenntnisse in Teil 1 auf eine sehr praxisrelevante besondere Erscheinungsform des Datenschutzes im Arbeitsalltag an: Beschäftigtendatenschutz. Sie erlernen beispielhaft, wie das Grundlagenwissen in spezifischen Bereichen anzuwenden ist und welche (zusätzlichen) Besonderheiten dabei zu beachten sind. Im zweiten Teil nehmen die Studierenden die Perspektive von Betroffenen ein und erwerben sich Kenntnisse darüber, welche Rechte dem Betroffenen zustehen und wie diese ggf. durchzusetzen sind. In Teil 3 geht es um die Umsetzung der rechtlichen Vorgaben in die technische Praxis: Die Studierenden erlernen, wie normative Erfordernisse des Datenschutzrechts technisch und organisatorisch flankiert werden, damit sie im Alltag ihre praktische Wirkung entfalten können.

3 Inhalte:

Teil 1: Beschäftigtendatenschutz

Im ersten Abschnitt von Teil 1 wird in die **Grundlagen** des Beschäftigtendatenschutzes eingeführt. Zunächst erfolgt eine Einführung in die gesetzlichen Grundlagen, die sich aufgrund der Gesetzgebungshoheit der Mitgliedstaaten in diesem Bereich überwiegend in den nationalen deutschen Gesetzen finden. Im Folgenden wird auf die einzelnen allgemeinen Rechtfertigungsgrundlagen zur Datenverarbeitung im Beschäftigtenverhältnis eingegangen, im Einzelnen den gesetzlichen Erlaubnistatbeständen, der Einwilligung sowie kollektiver Instrumente wie Betriebsvereinbarungen und Tarifverträge. Ein Abschnitt widmet sich auch dem Umgang mit Datenverarbeitungen in Krisenfällen, wie nationalen oder internationalen Pandemien. Den Abschluss des ersten Abschnitts bilden die Informationspflichten des Arbeitgebers.

Im zweiten Abschnitt werden spezifische, in der Praxis häufig vorkommende **Datenverarbeitungsvorgänge** im Beschäftigtenverhältnis behandelt. Im Einzelnen wird hier auf die Fragerechte des Arbeitsgebers, den Datenabgleich zu Compliance-Zwecken, wie z.B. zur Aufdeckung von Straftaten, den Anforderungen an eine Videoüberwachung am Arbeitsplatz, Bring Your Own Device sowie Datenschutz und Mitbestimmungsrechte eingegangen.

Die einzelnen Kapitel enthalten stets auch Tipps und Hinweise zur praktischen Umsetzung sowie Fallbeispiele.

Teil 2: Rechte der betroffenen Personen & Datenschutzbeauftragte/r

Im ersten Abschnitt von Teil 2 werden die **Rechte** der von Datenverarbeitungen betroffenen Personen behandelt. Im Einzelnen sind dies die Rechte auf Information, Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit und Widerspruch. Im Folgenden wird die Haftung der Verantwortlichen und Auftragsverarbeiter für Verstöße gegen Datenschutzvorschriften thematisiert, da sie im Zusammenhang mit der Durchsetzung einzelner Rechte gesehen werden muss. Ebenso verhält es sich mit zur Verfügung stehenden Rechtsbehelfen wie dem Recht auf Beschwerde bei einer Aufsichtsbehörde sowie dem Recht auf einen wirksamen Rechtsbehelf gegen Maßnahmen von Aufsichtsbehörden bzw. gegen Maßnahmen von Verantwortlichen und Auftragsverarbeitern. Es werden ebenso Fragen zum Rechtsweg erläutert.

Im zweiten Abschnitt von Teil 2 geht es um den **Datenschutzbeauftragten** und im Einzelnen um das Anforderungsprofil, die von Art. 37 DSGVO Fälle, in denen zwingend ein Datenschutzbeauftragter vom Verantwortlichen bzw. vom Auftragsverarbeiter zu benennen ist (Bestellpflicht), die Unterschiede zwischen internen und externen Datenschutzbeauftragten und weitere besondere Kategorien wie Gruppen- oder Konzernbeauftragte bzw. gemeinsame Datenschutzbeauftragte, Aufgaben und die Stellung, den Schutz von Datenschutzbeauftragten sowie Haftungsfragen. Am Ende dieses Abschnitts findet sich ein Interview eines internen (behördlichen) Datenschutzbeauftragten sowie ein Interview eines extern tätigen Datenschutzbeauftragten.

Teil 3: Technische und organisatorische Maßnahmen (TOM)

Teil 3 geht zunächst auf die Grundlagen der Anforderungen an die „Sicherheit der Verarbeitung" nach Art. 32 DSGVO ein. Dabei werden sowohl die **technischen** als auch die **organisatorischen Aspekte** thematisiert, bspw. die Fragestellungen „Pseudonymisierung und Verschlüsselung", „Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit", „Wiederherstellung" sowie „Verfahren zur Überprüfung von Maßnahmen". Anschließend wird mit konkreten Beispielen illustriert, wie die Anforderungen der DSGVO in der Praxis umgesetzt werden können, bspw. im Rahmen der Diskussion, welche Verschlüsselungsmechanismen in welchem Verarbeitungskontext angemessen und erforderlich sind.

Der zweite Abschnitt betrachtet dann, in welchen **weiteren Regelungen der DSGVO** die Fragestellungen der "technisch und organisatorischen Maßnahmen" ebenfalls noch zu berücksichtigen sind. Zu nennen sind hier insbesondere das „Recht auf Löschung" nach Art. 17 DSGVO und das „Verzeichnis von Verarbeitungstätigkeiten" nach Art. 30 DSGVO. Letzteres eignet sich gleichzeitig auch für die Dokumentation der bei der Verarbeitung der personenbezogenen Daten getroffenen technischen und organisatorischen Maßnahmen. Darüber hinaus sind technische und organisatorische Maßnahmen auch im Rahmen des Datenschutzes durch Technikgestaltung nach Art. 25 DSGVO und bei der Bewertung von Datenschutzpannen im Zusammenhang mit Art. 33 DSGVO relevant.

Zum Abschluss geht dieser Teil noch auf die Möglichkeit der **Zertifizierung** nach Art. 42 DSGVO ein, bietet diese doch die Möglichkeit, mit standardisierten technischen und organisatorischen Maßnahmen die Anforderungen zu erfüllen. Dabei wird insbesondere auch vermittelt, wie das Zusammenspiel der verschiedenen Akteure im deutschen Rechtsrahmen ist.

4	**Lehr-/Lernformen und Lehrmaterialien:** Fernstudium im Blended-Learning Mix, bestehend aus schriftlichen Lehreinheiten, denen eine Lernzielbestimmung im Video-Format vorgeschaltet wird. Lehrbegleitend wird ein Online-Angebot auf der virtuellen Lernplattform *Moodle*, eingesetzt, dieses besteht u. a. aus hybriden Betreuungsveranstaltungen.
5	**Teilnahmevoraussetzungen:** Siehe § 5 der Prüfungsordnung für den weiterbildenden Masterstudiengang Datenschutzrecht (LL.M)
6	**Prüfungsformen:** Klausur oder (Kurz-)Hausarbeit
7	**Voraussetzungen für die Vergabe von Leistungspunkten:** Bearbeitung des Moduls und Bestehen der Modulabschlussprüfung
8	**Verwendung des Moduls:** Weiterbildender Masterstudiengang Datenschutzrecht (LL.M.)
9	**Stellenwert der Note für die Endnote:** Siehe § 23 der Prüfungsordnung für den weiterbildenden Masterstudiengang Datenschutzrecht (LL.M.)
10	**Modulverantwortliche:** 1. Dr. Nink 2. Prof. Kreße / Dr. Laue 3. Dr. Wegener
11	**Sonstige Informationen:**

II. Pflicht-/Wahlmodule

<table>
<tr><td colspan="7">Zivil-, verwaltungs- und sanktionsrechtliche Folgen bei Verstößen gegen datenschutzrechtliche Bestimmungen und Rechtschutz</td></tr>
<tr><td colspan="2">Kennnummer
71104</td><td>Workload
300 Stunden</td><td>ECTS
10</td><td>Studiensemester
1.-2. Semester (je nach Var.)</td><td>Häufigkeit des Angebots
Jedes Semester</td><td>Dauer
1 Semester</td></tr>
<tr><td>1</td><td colspan="2">Fernstudienkurse
Teil 1: Zivilrecht
Teil 2: Verwaltungsrecht
Teil 3: Sanktionenrecht
Modulabschlussprüfung</td><td colspan="2">Workload
90 h
90 h
90 h
30 h</td><td colspan="2">Kreditpunkte
3
3
3
1</td></tr>
<tr><td>2</td><td colspan="6">Lernergebnisse (learning outcomes) / Kompetenzen:
Während im Modul 77103 die Betroffenenrechte näher erläutert werden, setzt sich dieses Modul zum Ziel, die „gegenüberliegende Seite“ der gegen datenschutzrechtliche Bestimmungen verstoßenden Partei näher zu betrachten. Konsequenzen eines Verstoßes gegen Vorgaben des Datenschutzrechtes können sich auf allen Ebenen ergeben: Daher werden in drei Teilen die jeweiligen Perspektiven im Zivil-, Verwaltungs- und Sanktionenrecht einzeln beleuchtet und an entsprechenden Stellen das Ineinandergreifen verschiedener Rechtsfolgen für ein datenschutzwidriges Verhalten dargestellt. Ein besonderes Augenmerk liegt dabei konsequenterweise auf den Abwehrmöglichkeiten durch effektiven Rechtsschutz. Die Studierenden erlangen in diesem Modul die Kompetenz, datenschutzwidriges Handeln einzuordnen und mithin zur Vermeidung solchen Handelns beizutragen. Sie lernen, Haftungsfolgen wegen rechtswidrigen Verhaltens im Datenschutz umfassend zu bewerten, die zivil-, verwaltungs- und ggf. sanktionsrechtliche Dimension des Vorgangs zu erfassen und dementsprechend Sorge dafür zu tragen, dass es zu keinem nachteiligen Haftungsfall kommt oder wenn ein solcher eingetreten sind, die Konsequenzen beherrscht und abgemildert werden. Schließlich erlernen sie einen sicheren Umgang mit den rechtlichen Instrumentarien, die beim Schutz datenschutzrechtlicher Belange zum Zuge kommen. Die DGSVO sowie das BDSG enthalten diverse solche Möglichkeiten, etwa Widerspruchsrechte, Möglichkeiten für Beschwerden bei den Aufsichtsbehörden oder auch gerichtlicher Rechtschutz. Der Kurs vermittelt das Wissen über das System der Rechtsbehelfe, die Kompetenz, den zulässigen Weg für das jeweils zu erreichende Rechtsschutzziel zu wählen und die Konkurrenz zu allgemeinen Verfahrensordnungen korrekt einzuordnen.</td></tr>
<tr><td>3</td><td colspan="6">Inhalte:

<u>Teil 1: Zivilrecht</u>

Bei einem Verstoß gegen datenschutzrechtliche Normen, insbesondere die Datenschutz-Grundverordnung (DSGVO) können zivilrechtliche Folgen drohen. Betroffene können in diesem Fall Schadensersatzansprüche geltend machen, wenn sie durch den Verstoß einen materiellen oder immateriellen Schaden erlitten haben. Es ist daher wichtig, dass Unternehmen und Einzelpersonen sich an die Vorgaben der DSGVO halten und angemessene Maßnahmen ergreifen, um die persönlichen Daten von Nutzern und Kunden zu schützen und sicherzustellen, dass sie entsprechend der DSGVO verarbeitet werden. Der Kurs vermittelt die Fähigkeit zur Einordnung und Einschätzung von zivilrechtlichen Haftungsfolgen und befähigt die Studierenden insbesondere zur Vermeidung solcher</td></tr>
</table>

	beizutragen. Sie erlangen insoweit besondere Kennnisse sowohl im Bezug auf das materielle als auch prozessuale Recht. Teil 2: Verwaltungsrecht Bei einem Verstoß gegen datenschutzrechtliche Normen, insbesondere die Datenschutz-Grundverordnung (DSGVO) können auch verwaltungsrechtliche Folgen drohen. Die zuständige Datenschutzbehörde hat die Befugnis, in solchen Fällen Sanktionen zu verhängen, die von einem Verweis bis hin zu empfindlichen Geldbußen reichen können. Die Datenschutzbehörde kann das Unternehmen oder die betroffene Person zur Einhaltung der DSGVO auffordern und gegebenenfalls auch anordnen, dass bestimmte Maßnahmen umgesetzt werden müssen, um den Datenschutz zu verbessern. Die Datenschutzbehörde kann auch Bußgelder verhängen, die bis zu 20 Millionen Euro oder 4 % des weltweiten Jahresumsatzes betragen können, je nachdem welcher Betrag höher ist. Die Höhe des Bußgeldes hängt von verschiedenen Faktoren ab, wie zum Beispiel der Art und Schwere des Verstoßes, dem Ausmaß der Schäden, die den Betroffenen entstanden sind, und der Kooperationsbereitschaft des Unternehmens oder der betroffenen Person. Es ist daher wichtig, dass Unternehmen und Einzelpersonen die Vorgaben der DSGVO beachten und angemessene Maßnahmen ergreifen, um die persönlichen Daten von Nutzern und Kunden zu schützen und sicherzustellen, dass sie entsprechend der DSGVO verarbeitet werden. Der Kurs vermittelt die Fähigkeit zur Einordnung und Einschätzung von öffentlich-rechtlichen Haftungsfolgen und befähigt die Studierenden insbesondere zur Vermeidung solcher beizutragen. Sie erlangen insoweit besondere Kennnisse sowohl im Bezug auf das materielle als auch prozessuale Recht. Teil 3: Sanktionsrecht Der Kurs vermittelt die grundlegenden Kenntnisse zu den Sanktionen im Datenschutzrecht. Art 84 der DGSVO schreibt vor, dass Sanktionen bei Verstößen gegen datenschutzrechtliche Bestimmungen „wirksam, verhältnismäßig und abschreckend" sein müssen. Die Studierenden beherrschen nach der Bearbeitung die Grundlagen für den sicheren Umgang mit dem speziell für das Datenschutzrecht geregelten Straf- und Ordnungswidrigkeitenrecht. Ebenso erlernen Sie zur Abwehr möglicher hoher Geldbußen oder gar Strafen die einzelnen effektiven Rechtsschutzmöglichkeiten sowie unterschiedliche zweckmäßige Vorgehensweisen zur interessengerechten Erledigung von Konfliktfällen mit Behörden.
4	**Lehr-/Lernformen und Lehrmaterialien:** Fernstudium im Blended-Learning Mix, bestehend aus schriftlichen Lehreinheiten, denen eine Lernzielbestimmung im Video-Format vorgeschaltet wird. Lehrbegleitend wird ein Online-Angebot auf der virtuellen Lernplattform *Moodle*, eingesetzt, dieses besteht u. a. aus hybriden Betreuungsveranstaltungen. Ebenso enthalten die verschiedenen Teile Hinweise zu weiterführenden wissenschaftlichen Beiträgen und ggf. einschlägiger Rechtsprechung, die im Selbststudium zu bearbeiten sind.
5	**Teilnahmevoraussetzungen:** Siehe § 5 der Prüfungsordnung für den weiterbildenden Masterstudiengang Datenschutzrecht (LL.M)
6	**Prüfungsformen:** Klausur oder (Kurz-)Hausarbeit
7	**Voraussetzungen für die Vergabe von Leistungspunkten:** Bearbeitung des Moduls und Bestehen der Modulabschlussprüfung
8	**Verwendung des Moduls** Weiterbildender Masterstudiengang Datenschutzrecht (LL.M.)
9	**Stellenwert der Note für die Endnote:**

	Siehe § 23 der Prüfungsordnung für den weiterbildenden Masterstudiengang Datenschutzrecht (LL.M.)
10	**Modulverantwortliche:** 1. Dr. Koreng 2. Schild 3. Dr. Ihwas
11	**Sonstige Informationen:** Dieses Modul stellt ein Wahlmodul innerhalb der 60-ECTS-Variante und ein Pflichtmodul innerhalb der 90-ECTS-Variante dar.

Leading Cases Datenschutzrecht

Kennnummer	Workload	ECTS	Studiensemester	Häufigkeit des Angebots	Dauer
71105	300 Stunden	10	1.-3. Semester (je nach Var.)	Jedes Semester	1 Semester

1	Fernstudienkurse	Workload	Kreditpunkte
	Teil 1: Arbeitsrecht und übriges Privatrecht	90 h	3
	Teil 2: Polizei- und Ordnungsbehördenrecht	90 h	3
	Teil 3: Verfassungs- und Europarecht	90 h	3
	Modulabschlussprüfung	30 h	1

2 Lernergebnisse (learning outcomes) / Kompetenzen:

Nach der Lektüre der Leading Cases sind die Teilnehmer geschult in der Analyse komplexer Sachverhalte aus unterschiedlichen Bereichen des Datenschutzrechts. Sie können Fragestellungen nicht nur in ihrem rechtlichen Kontext erfassen, sondern auch in ihrer wissenschaftlichen, gesellschaftlichen, sozialen und politischen Dimension einordnen.

Weiterhin sind sie in der Lage, wesentliche Aspekte von unwesentlichen, insbesondere nicht entscheidungserheblichen Fragen, sauber zu trennen. Ihnen sind die Unterschiede zwischen der gutachtlichen Bearbeitung von Fällen und der Urteilstechnik bewusst. Sie haben größere Sicherheit bei der Auslegung von Normen gewonnen. Sie kennen die Möglichkeiten und Grenzen richterlicher Rechtsfortbildung und wissen um den prägenden Einfluss der europäischen Rechtsprechung auf die Interpretation zahlreicher nationaler Regelungen.

3 Inhalte:

Gegenstand des Moduls sind höchstrichterliche Entscheidungen unterschiedlicher Gerichte, die für den jeweiligen Bereich besonders prägend waren. Diese haben beispielsweise bereits seit längerem strittige Fragestellungen entschieden und/oder über den konkreten Fall hinaus eine weitere Entwicklung angestoßen. Die Analyse der jeweiligen Entscheidung beschränkt sich dabei nicht auf die Darstellung des Sachverhalts und der tragenden Gründe. Es wird im Weiteren auch die dogmatische Bedeutung sowie die Konsequenzen für Wissenschaft und Praxis dargelegt. Wo dies sinnvoll erscheint, wird dabei auch auf vorhergehende und nachfolgende Entscheidungen sowie weiterführende Literatur zum Thema eingegangen.

Die Auswahl der zu besprechenden Leitentscheidungen erfolgt zweigleisig: Einerseits enthält das Modul historische Grundlagenentscheidungen, die das Datenschutzrecht national wie auf EU-Ebene nachhaltig geprägt haben. Diese gehören zu den festen Modulbestandteilen. Andererseits soll pro Semester zumindest eine aktuelle Entscheidung bearbeitet werden, die das Potenzial hat, entweder selbst zu einem Leading Case zu werden und die bestehenden Leading Cases inhaltlich weiterzuentwickeln.

4 Lehr-/Lernformen und Lehrmaterialien:

	Fernstudium im Blended-Learning Mix, bestehend aus schriftlichen Lehreinheiten, denen eine Lernzielbestimmung im Video-Format vorgeschaltet wird. Lehrbegleitend wird ein Online-Angebot auf der virtuellen Lernplattform *Moodle*, eingesetzt, dieses besteht u. a. aus hybriden Betreuungsveranstaltungen.
5	**Teilnahmevoraussetzungen:** Siehe § 5 der Prüfungsordnung für den weiterbildenden Masterstudiengang Datenschutzrecht (LL.M)
6	**Prüfungsformen:** Case-Study in Form einer häuslichen Arbeit
7	**Voraussetzungen für die Vergabe von Leistungspunkten:** Bearbeitung des Moduls und Bestehen der Modulabschlussprüfung
8	**Verwendung des Moduls** Weiterbildender Masterstudiengang Datenschutzrecht (LL.M.)
9	**Stellenwert der Note für die Endnote:** Siehe § 23 der Prüfungsordnung für den weiterbildenden Masterstudiengang Datenschutzrecht (LL.M.)
10	**Modulverantwortliche:** 1. Wette 2. Tech
11	**Sonstige Informationen:** Dieses Modul stellt ein Wahlmodul innerhalb der 60-ECTS-Variante und ein Pflichtmodul innerhalb der 90-ECTS-Variante dar.

III. Wahlmodule

<table>
<tr><td colspan="7">e-Privacy / Datenschutzgerechte Vertragsgestaltung / Datenschutzrecht der freien Berufe</td></tr>
<tr><td colspan="2">Kennnummer
71106</td><td>Workload
300 Stunden</td><td>ECTS
10</td><td>Studiensemester
1.-4. Semester (je nach Var.)</td><td>Häufigkeit des Angebots
Jedes Semester</td><td>Dauer
1 Semester</td></tr>
<tr><td>1</td><td colspan="2">Fernstudienkurse
Teil 1: ePrivacy
Teil 2: Datenschutzgerechte Vertragsgestaltung
Teil 3: Datenschutzrecht der freien Berufe
Modulabschlussprüfung</td><td colspan="2">Workload
90 h
90 h
90 h
30 h</td><td colspan="2">Kreditpunkte
3
3
3
1</td></tr>
<tr><td>2</td><td colspan="6">Lernergebnisse (learning outcomes) / Kompetenzen:
Die Studierenden haben eine sichere Basis im Umgang mit den relevanten datenschutzrechtlichen Vorgaben im Bereich der Telemedien und der Telekommunikation sowie mit Vertragsgestaltung unter Beachtung datenschutzrechtlicher Vorgaben; ferner sind sie vertraut mit den Erfordernissen des Datenschutzes bei freien Berufen. Sie verfügen die Kompetenz, die ineinandergreifenden Aspekte aus unterschiedlichen Regelengsgebieten zu erkennen und entsprechende Lösungsvorschläge in etwaigen Konfliktfällen zu erarbeiten. Ein besonderes Augenmerk liegt dabei auf der Beachtung des prägenden Einflusses, den die EU-Vorgaben auf das betreffende nationale Recht ausüben, sowie auf der Einbeziehung internationaler Aspekte des Datenschutzes über den EU-Raum hinaus.</td></tr>
<tr><td>3</td><td colspan="6">Inhalte:

<u>Teil 1: ePrivacy</u>

Sonder-„Datenschutz“-Regelungen für Telemedien: Gemeint sind damit Regelungen zu Telemedien, die sich im TTDSG finden und im weitesten Sinn datenschutzrechtliche Vorgaben enthalten. Dazu gehören u. a. die Regeln zum technisch-organisatorischen Datenschutz (§ 19 TTDSG) und zu Auskunftsverfahren gegenüber Privatpersonen und Sicherheitsbehörden (§§ 21-14 TTDSG). Cookies bzw. Informationen in Endeinrichtungen: § 25 TTDSG gilt sowohl für Cookies als auch für sonstige in Endgeräten gespeicherte Informationen – was im „Internet der Dinge“ von großer Bedeutung ist. Es werden nach Darlegung der rechtlichen Grundlage Handlungsempfehlungen der Datenschutzbehörden zu diesem Thema sowie die einschlägige Rechtsprechung vorgestellt. Außerdem werden die rechtlichen Voraussetzungen für sog. „Dienste zur Einwilligungsverwaltung“ (§ 26 TTDSG) besprochen. Fernmeldegeheimnis und Telekommunikationsdatenschutz: Das in § 3 TTDSG niedergeschriebene Fernmeldegeheimnis ist ein Rechtsgut, das mit dem Datenschutz zwar nicht identisch, aber doch eng mit ihm verwandt ist. Hierzu werden verschiedene Aspekte beleuchtet, so z. B. die Frage, ob Arbeitgeber zur Wahrung des Fernmeldegeheimnisses verpflichtet sind. Des Weiteren wird beispielsweise der Schutz von Verkehrsdaten, d. h. Telekommunikations-Metadaten, thematisiert.</td></tr>
</table>

	Teil 2: Datenschutzgerechte Vertragsgestaltung Cloud Computing, Software as a Service, externe Rechenzentren und die neue App: Welche datenschutzrechtlichen Regelungen brauchen wir in Verträgen, um digitale Lösungen datenschutzkonform einsetzen und anbieten zu können? Welche Best Practices gelten für Auftragsverarbeitungsverträge, Verträge über die gemeinsame Verantwortlichkeit und Sonderkonstellationen von Gewinnspielteilnahmebedingungen bis hin zum Bezahlen mit Daten? Das Datenschutzrecht nimmt auch auf all diese Themen der Vertragsgestaltung Einfluss, eine in der Praxis hoch relevante Fragestellung (bei uns berühren fast ein Viertel aller Mandate genau diese Fragestellungen mit – wir sehen gerade bei Datenschutzbeauftragten, dass die so wichtigen Kenntnisse in diesem Bereich oft fehlen). Abgehandelt werden in diesem Teil die unterschiedlichen datenschutzrechtlich relevanten Vertragstypen, ausgehend von der datenschutzrechtlichen Rollenverteilung bis hin zum datenschutzrechtlichen Einfluss auf die diversen Hauptverträge und natürlich auch das Erfordernis von vertraglichen Absprachen beim Datentransfer in Drittstaaten (Standardvertragsklauseln, zusätzliche Maßnahmen zur Absicherung eines ausreichenden Schutzes – Stichwort Microsoft, Google & Co., alles Anbieter mit US-Bezügen). Teil 3: Datenschutzrecht der freien Berufe Für viele der freien Berufe (§ 1 Abs. 2 PartGG) ist der Umgang mit personenbezogenen Daten berufsbildprägend. Die freien Berufe, zu denen unter anderem Rechtsanwälte (§ 2 Abs. 1 BRAO), Wirtschaftsprüfer (§ 1 Abs. 2 S. 1 WPO), Steuerberater (§ 32 Abs. 2 S. 3 StBerG) und Ärzte (§ 1 Abs. 2 BÄO) zählen, sind dem Datenschutz seit jeher in besonderer Weise verpflichtet. Die Mandats-, Geschäfts- bzw. Behandlungsbeziehungen der Freiberufler zu ihren Mandanten oder Patienten müssen von gegenseitigem Vertrauen geprägt sein, Mandanten oder Patienten müssen dem Freiberufler als Grundlage für dessen Beratungs- oder Behandlungsleistungen private oder geschäftliche Geheimnisse oder Details ihrer Vermögensangelegenheiten offenlegen. Basis dieses Vertrauens ist der – strafrechtlich flankierte (§ 203 StGB) – Berufsgeheimnisschutz: Alles, was dem Berufsgeheimnisträger in Wahrnehmung seiner Aufgabe vom Auftraggeber offenbart wird, unterliegt der Schweigepflicht. Die Verschwiegenheit der Rechtsanwälte, Wirtschaftsprüfer, Steuerberater, Ärzte und anderer freien Berufe ist daher eine sog. statusbildende Grundpflicht und unverzichtbare Bedingung der freiberuflichen Tätigkeit. So ist das in Art. 48 GRCh verbürgte europäische Grundrecht auf Beratung, Verteidigung und Vertretung im Rahmen rechtsstaatlicher Rechtsschutzverfahren ohne den Schutz der dafür dem Berufsgeheimnisträger offenbarten Daten nicht denkbar. Die Verschwiegenheitspflicht schützt umfassend die Daten des Mandanten oder Patienten und ist damit angewandtes Datenschutzrecht. Zugleich können das allgemeine Datenschutzrecht und der spezifische Berufsgeheimnisschutz miteinander konkurrieren. In diesem Modul werden daher auch diejenigen Regelungen behandelt, die den Vorrang der Verschwiegenheitspflichten sicherstellen, zudem Besonderheiten der Auftragsverarbeitung und die neuen Herausforderungen, welche die Digitalisierung der freiberuflichen Tätigkeit mit sich bringt: Berufsrechtsspezifische Fragen des Outsourcing gehören ebenso dazu wie die Grenzen des Einsatzes von Künstlicher Intelligenz in der Beratung.
4	**Lehr-/Lernformen und Lehrmaterialien:** Fernstudium im Blended-Learning Mix, bestehend aus schriftlichen Lehreinheiten, denen eine Lernzielbestimmung im Video-Format vorgeschaltet wird. Lehrbegleitend wird ein Online-Angebot auf der virtuellen Lernplattform *Moodle*, eingesetzt, dieses besteht u. a. aus hybriden Betreuungsveranstaltungen. Ebenso enthalten die verschiedenen Teile Hinweise zu weiterführenden wissenschaftlichen Beiträgen und ggf. einschlägiger Rechtsprechung, die im Selbststudium zu bearbeiten sind.
5	**Teilnahmevoraussetzungen:**

	Siehe § 5 der Prüfungsordnung für den weiterbildenden Masterstudiengang Datenschutzrecht (LL.M)
6	**Prüfungsformen:** (Kurz-)Hausarbeit
7	**Voraussetzungen für die Vergabe von Leistungspunkten:** Bearbeitung des Moduls und Bestehen der Modulabschlussprüfung
8	**Verwendung des Moduls** Weiterbildender Masterstudiengang Datenschutzrecht (LL.M.)
9	**Stellenwert der Note für die Endnote:** Siehe § 23 der Prüfungsordnung für den weiterbildenden Masterstudiengang Datenschutzrecht (LL.M.)
10	**Modulverantwortliche:** 1. Dr. Assion 2. Dr. Schreiber 3. Prof. Dr. Uwer / Dr. Dröß̈ler
11	**Sonstige Informationen:**

<table>
<tr><td colspan="7">Verarbeitung besonderer Kategorien personenbezogener Daten, insbesondere Gesundheits- und Sozialdatenschutzrecht</td></tr>
<tr><td colspan="2">Kennnummer
71107</td><td>Workload
300 Stunden</td><td>ECTS
10</td><td>Studiensemester
1.-4. Semester (je nach Var.)</td><td>Häufigkeit des Angebots
Jedes Semester</td><td>Dauer
1 Semester</td></tr>
<tr><td>1</td><td colspan="2">Fernstudienkurse
Teil 1: Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DS-GVO)
Teil 2: Datenschutz in medizinischen Einrichtungen
Teil 3: Sozialdatenschutz
Modulabschlussprüfung</td><td colspan="2">Workload
90 h
90 h
90 h
30 h</td><td colspan="2">Kreditpunkte
3
3
3
1</td></tr>
<tr><td>2</td><td colspan="6">Lernergebnisse (learning outcomes) / Kompetenzen:
Nachdem sich die Studierenden insbesondere im Modul 71102 mit den allgemeinen Voraussetzungen der Rechtsmäßigkeit der Datenverarbeitung beschäftigt haben, erlernen sie in diesem Modul die verschärften Vorgaben zum Umgang mit besonderen Kategorien personenbezogener Daten. In der Gesamtbetrachtung erwerben sich die Studierenden nach Abschluss dieses Moduls die Kompetenz, die besonders sensiblen Bezugspunkte bei der Verarbeitung personenbezogener Daten zu erkennen, die Regelkonformität beim Umgang mit ihnen zu sichern und unter Beachtung der gesetzlichen Vorgaben Lösungsvorschläge für etwaige Konfliktfälle zu erarbeiten.</td></tr>
<tr><td>3</td><td colspan="6">Inhalte:

<u>Teil 1: Verarbeitung besonderer Kategorien personenbezogener Daten nach Art. 9 DSGVO</u>

Art. 9 Abs. 2 DSGVO schreibt vor, dass die Verarbeitung personenbezogener Daten, „aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person“ generell untersagt ist und konstituiert gleichzeitig in Abs. 2 bestimmte Ausnahmen. Nach Bearbeitung des ersten Teils dieses Moduls erlangen die Studierenden die Kompetenz, dieses Regel- und Ausnahmeverhältnis zu beherrschen. Im zweiten und dritten Teil des Moduls soll dann die Verarbeitung besonderer Kategorien am Beispiel des Datenschutzes im Gesundheitswesen in einem praktisch bedeutsamen Bereich ausführlich unter verschiedenen Perspektiven beleuchtet werden.

<u>Teil 2: Gesundheitsdatenschutz</u>

Medizinische Versorgungszentren, Krankenhäuser und Rehabilitationseinrichtungen erheben zunehmend Daten beginnend bereits mit der Aufnahme von Patientinnen und Patienten, bei der Anamnese, während der Therapie, bei der Kommunikation mit anderen Einrichtungen und übrigen medizinischem Personal bis hin zu Fragen der Abrechnung und dem Datenaustausch mit Kranken-</td></tr>
</table>

	kassen. Hinzu kommen Datenerfassungen im Rahmen der Gewähr von Internetanschlüssen, Telefon- und übrigen Teledienstleistungen für Patientinnen und Patienten bis hin zur digitalen Aufnahme von Ernährungsgewohnheiten und dergleichen mehr. Diese Fülle von persönlichen, überwiegend auch sehr sensiblen Daten, erfordert im Besonderen den Schutz der Patientinnen und Patienten. Dieser Teil vermittelt den Studierenden diejenigen Grundlagen, die für einen datenschutzkonformen Umgang solcher Daten erforderlich sind. Der Teil berücksichtigt dabei insbesondere die oftmals in den medizinischen Einrichtungen vorzufindende komplexe Personalstruktur sowie das dauerwährende Fortschreiten der Digitalisierung. <u>Teil 3: Sozialdatenschutz</u> In diesem Teil werden zunächst die sog. Sozialdaten bestimmt (§ 35 SGB I), dies in Abgrenzung zu den besonderen Arten personenbezogener Daten und der Klärung der unterschiedlichen bereichsspezifischen nationalen Datenschutznormen im Bereich des SGB (besonders SGB X) in Abgrenzung zu dem allgemeinen Datenschutzrecht (BDSG) und dem weiteren spezifischen Datenschutzrecht im Steuerrecht (AO). Es wird ermittelt, wie die unterschiedlichen Rechtswege sind und welche ggf. einzuhalten sind (Sozialgericht, Verwaltungsgericht, Finanzgericht, ordentliche Gerichtsbarkeit), dies mit dem Schwerpunkt der Sozialgerichtsbarkeit. Dabei sind die gerichtlichen Zuständigkeiten (sachlich und örtlich) zu klären, sowie die Unterschiede bei den Klageverfahren aus der Sicht der betroffenen Person und aus der Sicht eines Sozialleistungsträgers gegen eine Aufsichtsbörde. Dies mit dem Unterpunkt vorläufiger Rechtschutz unter Beachtung der Vorgaben der DSGVO und des BDSG, des SGB X und der AO. Die Forderung nach effektivem Rechtschutz der DSGVO und GrCh wird im Lichte der Rechtsprechung des EuGH betrachtet. Hinzu kommen Sonderprobleme wie das One-Shop-Stop-Verfahren, die Bestimmung der zuständigen Aufsichtsbehörde und Rechtsschutzgewährung bei grenzüberstreitenden Verfahren. Nationalstaatlich ist die konkurrierende Rechtsprechung und gemeinsamer Senat der obersten Gerichtshöfe des Bundes im Lichte der EuGH-Rechtsprechung zu betrachten. Die Studierenden lernen dabei die Klaviatur des bereichsspezifischen Sozialdatenschutzechts und des mit dieser Materie unmittelbar verbundenen jeweiligen Rechtsschutzes in seinen spezifischen Ausprägungen.
4	**Lehr-/Lernformen und Lehrmaterialien:** Fernstudium im Blended-Learning Mix, bestehend aus schriftlichen Lehreinheiten, denen eine Lernzielbestimmung im Video-Format vorgeschaltet wird. Lehrbegleitend wird ein Online-Angebot auf der virtuellen Lernplattform *Moodle*, eingesetzt, dieses besteht u. a. aus hybriden Betreuungsveranstaltungen. Ebenso enthalten die verschiedenen Teile Hinweise zu weiterführenden wissenschaftlichen Beiträgen und ggf. einschlägiger Rechtsprechung, die im Selbststudium zu bearbeiten sind.
5	**Teilnahmevoraussetzungen:** Siehe § 5 der Prüfungsordnung für den weiterbildenden Masterstudiengang Datenschutzrecht (LL.M)
6	**Prüfungsformen:** (Kurz-)Hausarbeit
7	**Voraussetzungen für die Vergabe von Leistungspunkten:** Bearbeitung des Moduls und Bestehen der Modulabschlussprüfung
8	**Verwendung des Moduls** Weiterbildender Masterstudiengang Datenschutzrecht (LL.M.)
9	**Stellenwert der Note für die Endnote:** Siehe § 23 der Prüfungsordnung für den weiterbildenden Masterstudiengang Datenschutzrecht (LL.M.)
10	**Modulverantwortliche:** 1. Dr. Schulz-Große

	2. Dr. Schrader 3. Prof. Dr. Bieresborn
11	**Sonstige Informationen:**

IV. Masterarbeit

Masterarbeit					
Kennnummer	**Workload**	**ECTS**	**Studiensemester**	**Häufigkeit des Angebots**	**Dauer**
71108	600 h	20	2.-5. Semester (je nach Var.)	Jedes Semester	1 Semester

1	**Lehrveranstaltungen**	**Workload** 600 h	**Kreditpunkte** 20
2	**Lernergebnisse (learning outcomes)** In der Masterarbeit zeigt der Prüfling, dass er in der Lage ist, innerhalb einer vorgegebenen Frist ein komplexes Problem aus einem Fach selbständig nach wissenschaftlichen Methoden zu bearbeiten. Mit der Masterarbeit erlernen die Teilnehmenden die Erarbeitung einer der Tragweite des Problems angemessenen Lösung unter Berücksichtigung verschiedenster Lösungsansätze und des Einsatzes wissenschaftlicher Quellen.		
3	**Inhalte** Das Thema der Masterarbeit wird individuell bestimmt.		
4	**Lehr-/Lernformen** Die Teilnehmenden erstellen unter Betreuung der hauptamtlich Lehrenden eine schriftliche Arbeit. Der Umfang der Masterarbeit soll nicht mehr als 150.000 Zeichen (einschließlich Leerzeichen und Fußnoten) zuzüglich Deckblatt, Inhalts- und Literaturverzeichnis betragen. Im Anschluss an die Bewertung der Masterarbeit findet, so die Arbeit als bestanden bewertet wurde, eine mündliche Prüfung (Verteidigung) statt. Dort werden die Studierenden von einem Prüfer oder einer Prüferin sowie einer Beisitzerin bzw. einem Beisitzer geprüft und benotet. Der Termin der Disputation wird von den Prüfenden verbindlich festgelegt. Zu Beginn der Verteidigung referieren die Studierenden dann die wesentlichen Ergebnisse der Masterarbeit und führen im Anschluss daran mit den Prüfenden ein Prüfungsgespräch über die Masterarbeit. Das Gespräch kann sich auch auf andere Fragen des Faches und angrenzende Gebiete anderer Fächer beziehen, die mit dem Gegenstand der Masterarbeit zusammenhängen. Für die Verteidigung werden insgesamt etwa 30 Minuten angesetzt.		
5	**Teilnahmevoraussetzung** Siehe §§ 5, 16 der Prüfungsordnung für den Weiterbildenden Masterstudiengang Datenschutzrecht (LL.M.)		
6	**Prüfungsform** Schriftliche Arbeit sowie mündliche Verteidigung		
7	**Voraussetzungen für die Vergabe von Kreditpunkten** Die Masterprüfung muss mindestens mit der Note „ausreichend" (4,0) bewertet worden sein.		
8	**Verwendung des Moduls** Weiterbildender Masterstudiengang Datenschutzrecht (LL.M.)		
9	**Stellenwert der Note in der Endnote** Siehe § 23 der Prüfungsordnung für den Weiterbildenden Masterstudiengang Datenschutzrecht (LL.M.)		
10	**Modulverantwortliche** Siehe § 6 Abs. 5 der Prüfungsordnung für den Weiterbildenden Masterstudiengang Datenschutzrecht (LL.M.)		
11	**Sonstige Informationen** Die Bearbeitungszeit für die schriftliche Ausarbeitung beträgt gem. § 17 Abs. 5 der Prüfungsordnung für den Weiterbildenden Masterstudiengang Datenschutzrecht (LL.M.) 14 Wochen.		