

# Bußgeldtabelle Gesundheitswesen International - DSGVO / Datenschutzrecht alt & neu - Jahre 2017 bis 2021 - unvollständig

© AID24 Rechtsanwaltskanzlei – Download & Nutzung mit diesem Vermerk für jedermann gestattet. Sie dürfen diese Fallübersicht auf Ihrer Internetseite kostenfrei Dritten verfügbar machen, wenn Sie [www.aid24.de](http://www.aid24.de) verlinken.

Datum	Behörde	Land	Bußgeld (€)	oder	(mutmaßlicher) Verstoß gegen	Verantwortlicher	Sachverhalt	Online-Fundstelle	Weitere	Fundstellen
07.12.20	Datinspektionen	Schweden	274.000,00 € – 2.964.000,00 €	2.500.000 – 30.000.000 SEK	Art. 32 DSGVO	Sieben von Acht geprüfte klinische Einrichtungen	Geprüft wurde die Einhaltung notwendiger Risikoanalysen zur Gewährleistung adäquater Zugangsberechtigungen für personenbezogene Daten in den elektronischen Gesundheitsakten. Sieben der Acht geprüften Einrichtungen konnten diese nicht vorweisen.	<a href="#">Link</a>		
2018	Autoriteit Persoonsgegevens	Niederlande	460.000,00 €		Art. 32	Haga Krankenhaus (Betreiber)	Die Autoriteit Persoonsgegevens verhängte ein Bußgeld in Höhe von 460.000 € gegen ein niederländisches Krankenhaus. Dort seien die technischen Sicherheitsvorkehrungen gegen einen Zugriff durch Unbefugte nicht ausreichend, weshalb es 2018 zu zahlreichen Zugriffen auf Krankendaten einer niederländischen Reality-TV-Persönlichkeit durch dazu nicht berechtigte Mitarbeiter gekommen sein soll. Sollte die Datensicherheit nicht bis zum 2.10.2019 verbessert werden, muss das Krankenhaus alle zwei Wochen 100.000 € zahlen, 300.000 € wären dabei jedoch das Maximum. Dies wurde am 16.07.2019 bekannt gegeben.	<a href="#">Link</a>	<a href="#">Link</a>	<a href="#">Link</a>
Feb.2021	Autoriteit Persoonsgegevens	Niederlande	440.000,00 €		Art. 32 DSGVO	Krankenhaus OLVG	Nach Ansicht der Behörde wurden keine ausreichenden technischen und organisatorischen Maßnahmen getroffen, um die Krankenakten vor dem Zugriff von unbefugtem Personal zu schützen. Die Krankenakten enthielten neben der Krankengeschichte des Patienten auch Sozialversicherungsnummern sowie Kontakt- und Adressdaten. Außerhalb des Krankenhauses konnten die Akten mittels einer 2-Faktor-Authentifizierung eingesehen werden. Im Krankenhaus reichte ein einfacher Login aus. Der Zugriff auf Patientenakte wurde dokumentiert aber nicht auf unautorisierte Zugriffe überprüft.	<a href="#">Link</a>	ZD-Aktuell 2021, 05095	
17.7.18	CNPD	Portugal	400.000,00 €		Art. 5 I f, 32 DS-GVO	Krankenhaus Barreiro Montijo	Das Berechtigungskonzept im Computersystem des Krankenhauses war mangelhaft: Es gab 985 Arztprofile bei tatsächlich nur 296 Ärzten. Zudem hatten alle „Ärzte“ Zugriff auf sämtliche Patientenakten, die jeweilige fachliche Spezialisierung wurde nicht berücksichtigt. Somit hatten zu viele Mitarbeiter auch über falsche Profile Zugang zu den Patientendaten.	<a href="#">Link</a>	<a href="#">Link</a>	<a href="#">Link</a>
	LFD Niedersachsen	Deutschland	294.000,00 €				Unnötig lange Aufbewahrung von Personalidaten und „übergeordnete“ Erhebung von Daten im Personalverfahren ( Abfrage von Gesundheitsdaten).	<a href="#">Link</a>		
	LFDI Rheinland-Pfalz	Deutschland	105.000,00 €			Mainzer Universitätsklinik	Falsche Rechnungsstellung durch Patientenverwechslung.; Patientendaten wurden öfter von dem falschen Empfänger erhalten.	<a href="#">Link</a>		
6.12.18	Datenschutzbehörde BW	Deutschland	80.000,00 €				Der Verantwortliche hatte im Rahmen einer digitalen Veröffentlichung wegen ungenügender interner Kontrollmechanismen versehentlich personenbezogene Gesundheitsdaten veröffentlicht. Dies wurde mit einer Geldstrafe in Höhe von 80.000 € + 4.000 € Verfahrensgebühr sanktioniert.	<a href="#">Link</a>	<a href="#">Link</a>	
01.07.20	Datatisynet	Norwegen	74.100,00 €	750.000 NOK	Art. 5, 32 DSGVO	Østfold HF Krankenhaus	Das Krankenhaus speicherte Patientendaten, die mitunter sensible Daten enthielten, außerhalb eines gesicherten Bereichs. Dadurch wurde der Zugriff auf die Daten weder kontrolliert, noch protokolliert. Darüber Hinaus wurden die Daten länger gespeichert, als sie erforderlich waren.	<a href="#">Link</a>	<a href="#">Link</a>	
04.11.20	DPC	Irland	65.000,00 €		Art. 32 DSGVO	Cork University Maternity Hospital	Das Klinikum entsorgte 78 Dokumente, die Patientendaten, mitunter sensiblen Daten beinhalteten, welche an einer öffentlichen Recyclinganlage aufgefunden wurden. Die technischen und organisatorischen Maßnahmen waren dem Risiko, welches mit den Daten verbunden ist, nicht angemessen, sodass die Entsorgung nicht ordnungsgemäß erfolgte und mit einem Bußgeld geahndet wurde.	<a href="#">Link (S. 51)</a>	<a href="#">Link</a>	
11.02.21	Garante per la protezione dei dati personali	Italien	45.000,00 €		Art. 32 DSGVO	Istituti ospedalieri bergamaschi	Das Unternehmen übermittelte medizinische Akten von sieben Betroffenen an den falschen Empfänger und meldete diesen Vorfall an die Aufsichtsbehörde. Diese stellte unzureichende technische und organisatorische Maßnahmen des Unternehmens als Ursache dafür fest.	<a href="#">Link</a>		
Feb.2021	UODO	Polen	20.000,00 €	85.000 PLN		Unternehmer, der eine wirtschaftliche Tätigkeit im Bereich des Gesundheitswesens ausübt	Das Amt für den Schutz personenbezogener Daten ordnete an, dass der Unternehmer seinen Patienten die Verletzung ihrer personenbezogenen Daten mitteilt und ihnen Empfehlungen gibt, wie sie die möglichen negativen Auswirkungen des Vorfalls minimieren können. Der für die Verarbeitung Verantwortliche hat dies nicht getan. Folglich wussten die Betroffenen nichts von der Verletzung.	<a href="#">Link</a>		
2018/19	Datenschutzbehörde NRW	Deutschland	36 Fälle zsm. ca. 15.000,00€			Krankenhaus	Unter den 36 Fällen war zumindest einer, in dem ein Krankenhaus Gesundheitsdaten an den falschen Patienten weitergab.	<a href="#">Link</a>		
2018/19	Datenschutzbehörde NRW	Deutschland	36 Fälle zsm. ca. 15.000,00€				Unter den 36 Fällen war zumindest einer, in dem wegen unzureichenden internen Kontrollmechanismen Gesundheitsdaten im Internet veröffentlicht wurden.	<a href="#">Link</a>		
	schwedische Aufsichtsbehörde	Schweden	11.363,10 €	200.000 SEK		forensische psychiatrische Klinik	Unerlaubte Veröffentlichung von Patientendaten ( besonders sensible Daten ) auf der Webseite.	<a href="#">Link</a>		
2019	Cyprian Data Protection Commissioner	Zypern	5.000,00 €		Art. 15 DS-GVO	Staatliches Krankenhaus	Eine Patientin beschwerte sich bei der Aufsichtsbehörde über die fehlende Möglichkeit zur Einsichtnahme in ihre medizinischen Unterlagen. Das Krankenhaus konnte diese nicht finden. Nach Untersuchung des Falls wurden 5.000 € als Geldstrafe verhängt.	<a href="#">Link</a>	<a href="#">Link</a>	<a href="#">Link</a>
	LDA Brandenburg	Deutschland	Bußgeld in viertelliger Höhe			Mediziner	Mediziner hat seinen Bekannten darüber gebeten sämtliche Daten der Praxis zu speichern. Dies hat der Bekannte innerhalb des Unternehmens seines Arbeitgebers getan. Dies war eine unbefugte Datenübermittlung.	<a href="#">Link (S. 31)</a>		
8.4.19	KZLD	Bulgarien	511,00 €		Art. 5 I a, 9 I, II, 6 I DS-GVO	Arztpraxis	Es ging um einen Wechsel des Hausarztes: Ein medizinisches Zentrum verwendete eine Software zur Erstellung eines Registrierungsformulars für den Hausarztwechsel der betroffenen Person, dort wurde der Patient dann nach dem Wechsel als „inaktiv“ geführt. Nachdem die Praxis aber von einem anderen Arzt übernommen wurde, der auch die Software mit ihren Daten übernahm, war der Betroffene wieder als „aktiver“ Patient geführt. Anschließend wurde dies an die Krankenversicherung übermittelt, obwohl der Betroffene nie bei dem neuen Inhaber der Praxis in Behandlung war.	<a href="#">Link</a>		
2019	Landesdatenschutzbeauftragter RLP	Deutschland		eingeleitete Aufklärung		DRK-Trägergesellschaft Süd-West	Ein Virus hatte Server und Datenbanken in einem Krankenhaus-Netzwerk verschlüsselt, sodass Mitarbeiter nicht mehr darauf zugreifen konnten. Eif zur DRK-Trägergesellschaft Süd-West gehörende Krankenhäuser sowie vier Altenpflegeeinrichtungen waren betroffen. Bemerkte wurde dies am 14.07.2019. Es soll sich dabei um den bisher umfangreichsten Malware-Befall von Computern in Rheinland-Pfalz handeln. Wie es dazu kommen konnte, ist ebenso unklar wie die Frage, ob es sich um einen gezielten Angriff handelt. Die Verletzung des Schutzes personenbezogener Daten hat die Trägergesellschaft dem Landesdatenschutzbeauftragten gemäß Art. 33 DS-GVO gemeldet. Ein förmliches Verfahren zur Aufklärung ist im Gange. Bisher gebe es keine Hinweise darauf, dass Patientendaten erbeutet worden sein könnten.	<a href="#">Link</a>	<a href="#">Link</a>	<a href="#">Link</a>
30.7.19	LFDI Baden-Württemberg	Deutschland		Pressemitteilung		Arztpraxen	In Arztpraxen gibt es besorgniserregend viele Datenschutzverstöße. Insbesondere Verschlüsselungstrojaner stellen ein Problem dar ebenso wie die Übermittlung von Patientenberichten, Rezepten oder Röntgenbildern an den falschen Empfänger. Im Gesundheitswesen werden äußerst sensible und schützenswerte personenbezogene Daten verarbeitet. Mit diesen Daten ist besonders sorgfältig und korrekt umzugehen. Es sind technische Maßnahmen zur Datensicherung (z.B. Verschlüsselung) zu treffen sowie Mitarbeiter entsprechend zu schulen und sensibilisieren. Neben der Meldung an den LFDI sind bei Datenpannen oft auch Betroffene zu benachrichtigen (Art. 33 DS-GVO).	<a href="#">Link</a>		
2018	LFDI Bremen	Deutschland				mehrere unterschiedliche Verantwortliche	Meldungen der jeweils Verantwortlichen: falsch sortierte Unterlagen bei einer Krankenversicherung; fehlerhaft versandte Rechnungen eines Labors; Diebstahl von Festplatten sowie Laptops in einer Arztpraxis; geklaute Speicherkarte mit Bildmaterial von Patienten; Bett-Kennzeichnung im Krankenhaus mit den privaten Adressdaten der Patienten; Übermittlung von Blutalkoholwerten vom Krankenhaus an Polizei	<a href="#">Link (S. 24f)</a>		

2017/18	LDI NRW	Deutschland	abratender Hinweis	Art. 5 I f, 9 I IVm 4 Nr. 14, II DS-GVO	Apotheker als verantwortliche Stellen (Sv Art. 4 Nr. 7 DS-GVO)	Apotheken bieten ihren Kunden vermehrt an, Rezeptdaten über WhatsApp zu schicken. Besorgte Bürger sowie Apotheken fragten diesbezüglich bei der LDI NRW nach. Diese steht der WhatsApp-Nutzung zur Übermittlung von Gesundheitsdaten sehr kritisch gegenüber und rät Kunden und Apotheken davon ab.	<a href="#">Link (S.82)</a>
2017/18	LDI NRW	Deutschland			Ärzte	Häufig nutzen Ärzte externe Dienstleistungsunternehmen zur Abrechnung ihrer Leistungen. Dafür müssen bei den betroffenen Patienten zuvor aber wirksame Einverständniserklärungen eingeholt werden. Das Einverständnis wirkt allerdings nicht dauerhaft.	<a href="#">Link (S.81)</a>
2017/18	LDI NRW	Deutschland				Vor Gutachterkommissionen für Behandlungsfehler sind Verfahren ohne die Haftpflichtversicherer der Ärzte prinzipiell datenschutzrechtlich möglich.	<a href="#">Link (S.80)</a>
2018	LFDI Baden-Württemberg	Deutschland			Arztpraxen	Die ärztliche Schweigepflicht umfasst die Diskretion in den Praxen. Sie ist grundlegend für das Vertrauen zwischen Arzt und Patient. Im Warte- sowie Empfangsbereich sollte eine entsprechende Akustik regelmäßig überprüft werden. Über Diagnosen und Patientennamen ist nicht zu sprechen, sofern Dritte mithören könnten.	<a href="#">Link (S.107)</a>
2018	Berliner Beauftragte für Datenschutz und Informationsfreiheit	Deutschland	Beobachtung		Senatsverwaltung für Gesundheit, Pflege und Gleichstellung (Berlin)	Bei Anmeldung und Gesundheitsberatung werden personenbezogene Daten von Prostituierten verarbeitet. Dazu gehören Daten bezüglich Gesundheit und Sexualleben. Es handelt sich dabei um äußerst sensible personenbezogene Daten, die nach der DS-GVO besonders schützenswert sind, was in der Verfahrensumsetzung zu berücksichtigen ist. Daher wird die Umsetzung des Prostituiertenschutzgesetzes im Land Berlin vom LFDI beobachtet.	<a href="#">Link (S.96)</a>
2018	Berliner Beauftragte für Datenschutz und Informationsfreiheit	Deutschland	geplante Einwirkung auf Unternehmen			Als Konsequenz von Beschwerden beschäftigt sich der LFDI mit dem Angebot einer elektronischen Gesundheitsakte. Diese können Patienten zur Verwaltung ihrer medizinischen Unterlagen nutzen.	<a href="#">Link (S.98)</a>
2018	Berliner Beauftragte für Datenschutz und Informationsfreiheit	Deutschland	Datenschutzrechtliche Begleitung		Projekt „Babylotse“	Für das Projekt „Babylotse“ ist eine gewisse Vertraulichkeit erforderlich und die Einhaltung datenschutzrechtlicher Standards sicherzustellen. Der LFDI begleitet es daher datenschutzrechtlich.	<a href="#">Link (S.100)</a>
2018	Berliner Beauftragte für Datenschutz und Informationsfreiheit	Deutschland	Begleitung bei Behebung der festgestellten Mängel		Charité	Bereits vor der DS-GVO war die Charité verpflichtet, vorab die Verfahren zur Verarbeitung von Patienten-/Probandendaten datenschutzrechtlich zu kontrollieren. Dem ist die Charité bisher nicht (vollständig) gerecht geworden. Sie muss Risiken der betroffenen Personen im Rahmen ihrer Verfahren bewerten und die nach einer entsprechenden Analyse erforderlichen technischen und/oder organisatorischen Maßnahmen durchgehend umzusetzen. Dies hat in Form von systematisierten Sicherheits- und Datenschutzkonzepten zu erfolgen.	<a href="#">Link (S.101)</a>
2018	Berliner Beauftragte für Datenschutz und Informationsfreiheit	Deutschland	Aufforderung zur Besserung sowie Überprüfung		Berliner Unternehmen zur Vermittlung von medizinischen Dienstleistungen	Die Vermittlung von medizinischen Dienstleistungen verlagert sich zunehmend ins Internet. Der LFDI ist durch eine Beschwerde auf einen entsprechenden Dienstleister hingewiesen worden, der rechtswidrig Daten erhob. Erst nachdem dies unwiderlegbar nachgewiesen wurde, versprach das Unternehmen die Datenverarbeitung datenschutzrechtskonform umzugestalten. Der LFDI wird dies noch überprüfen. Übers Internet erfasste Gesundheitsdaten dürfen nicht ohne weiteres verarbeitet werden. Betroffene Personen müssen zunächst umfassend informiert werden und danach ausdrücklich einwilligen.	<a href="#">Link (S.103)</a>
2018	Berliner Beauftragte für Datenschutz und Informationsfreiheit	Deutschland	Aufforderung zur Besserung		Pflegedienst	Aufgrund eines Hinweises wurde ein Pflegeunternehmen geprüft. Notwendige medizinische Angaben zu den betreuten Personen wurden bei internationalen Unternehmen in der Cloud gespeichert. Deren Beschäftigte unterliegen jedoch keiner gesetzlichen Schweigepflicht mehr. Allerdings müssen Angehörige von Gesundheitsberufen sicherstellen, dass die Verarbeitung der Daten ihrer Kunden auch bei etwaigen genutzten Dienstleistern datenschutzrechtlich korrekt erfolgt.	<a href="#">Link (S.104)</a>
2018	Berliner Beauftragte für Datenschutz und Informationsfreiheit	Deutschland	bemängelnde Überprüfung		klinisches Krebsregister der Länder Brandenburg und Berlin	Von Amts wegen wurde die Datenschutzkonformität des gemeinsamen klinischen Krebsregisters der Länder Brandenburg und Berlin überprüft. Die äußerst sensitive und vollumfängliche Speicherung von Daten über Krebserkran-kungen unterliegt streng einzuhaltenen gesetzlichen Vorgaben. Eingriffe in die Rechte der Betroffenen sind zu minimieren. Dazu gehört auch die Vermeidung von überlanger Speicherung, Datenlecks oder deren Missbrauch.	<a href="#">Link (S.105)</a>
2018	Berliner Beauftragte für Datenschutz und Informationsfreiheit	Deutschland	Anpassung erreicht		Kinderarzt	Ein Kinderarzt legte dem LFDI den Vordruck einer Bescheinigung für die Kita-Aufnahme vor. Darin mussten bereits erfolgte Schutzimpfungen eingetragen werden. Nach dem Infektionsschutzgesetz ist allerdings nur das Einholen einer Impfberatung zu bestätigen. Es gibt keine gesetzliche Pflicht. Angaben zu Schutzimpfungen können daher nur freiwillig sein.	<a href="#">Link (S.106)</a>
2018	Berliner Beauftragte für Datenschutz und Informationsfreiheit	Deutschland			Online-Bewertungs-Portale	Patienten können mittels anonymen Bewertungsportale ihre medizinische Behandlung bewerten. Unzufriedene Ärzte können eine Überprüfung durch den Portalbetreiber anregen und eine Gegendarstellung veröffentlichen. Der LFDI erhielt mehrere Beschwerden, es sollen dabei identifizierende Patientendaten an den Portalbetreiber gelangt sein. So etwas verletzt unzulässigerweise die ärztliche Schweigepflicht. Es kann nicht davon ausgegangen werden, dass dem Portalbetreiber die Identität des Patienten bekannt ist.	<a href="#">Link (S.107)</a>
2018	TLFDI (Thüringen)	Deutschland	Unterstützung		Arztpraxis	Der TLFDI erhielt eine Anfrage zum Verbleib einer Patientenakte aus einer geschlossenen Arztpraxis in Gera. Die Akte befand sich zu diesem Zeitpunkt sicher verwahrt bei einer Poliklinik, nachdem das behandelnde Krankenhaus 2017 geschlossen worden war, sodass nur Zugriff auf die alten Akten genommen wurde, wenn die Patienten diese bei einer Weiterbehandlung benötigten. Der Datenschutzbeauftragte erklärte dazu, dass ärztliche Aufzeichnungen nach Behandlungsabschluss grundsätzlich 10 Jahre aufbewahrt werden müssen (§ 630 f BGB, § 10 IV MBO-A). Eine Weitergabe erfordert prinzipiell die Einwilligung des Patienten. Der Patient hat nach § 13 BDSG a.F. bzw. § 57 n.F. grundsätzlich ein Auskunftsrecht hinsichtlich der gespeicherten ihn betreffenden (Gesundheits-) Daten.	<a href="#">Link (S.239)</a>
2018	TLFDI (Thüringen)	Deutschland			logopädische Praxen	Bei logopädischen Praxen bestand Unklarheit, wann gemäß Art. 37 DS-GVO ein eigener Datenschutzbeauftragter erforderlich ist. Nach § 38 BDSG muss bei weniger als zehn Angestellten, die ständig mit der automatisierten Verarbeitung personenbezogener Daten zu tun haben, noch kein Datenschutzbeauftragter bestellt werden. Erst ab zehn Personen gilt die Verarbeitung als umfangreich genug. Das gilt sowohl für eine gewöhnliche Arztpraxis als auch einer Praxis vergleichbare Heilberufe. Ein eigener Datenschutzbeauftragter ist ebenso erforderlich, wenn eine Datenschutz-Folgenabschätzung nach Art. 35 I DS-GVO nötig ist.	<a href="#">Link (S.230)</a>
2018	TLFDI (Thüringen)	Deutschland	Beantwortung einer Anfrage		Heilpraktiker	Für Heilpraktiker ist eine Einwilligung nach Art. 9 I DS-GVO zur Behandlung von Patienten erforderlich. Nur Ärzte können sich auf Art. 9 II h DS-GVO berufen. Der TLFDI wurde dazu durch den Verband der Osteopathen Deutschland befragt.	<a href="#">Link (S.231)</a>
2018	TLFDI (Thüringen)	Deutschland	Beantwortung einer Frage		Arztpraxen	Nach der DS-GVO sollten Patienten bei der Anmeldung in einer Arztpraxis gefragt werden, ob sie mit einem namentlichen Aufruf einverstanden sind und diesbezüglich einwilligen. Ansonsten wären sie von Praxismitarbeitern persönlich im Wartezimmer abzuholen. Diesbezüglich wandte sich ein Praxismitarbeiter im Mai 2018 an den TLFDI. Das Aufrufen der Patienten mit ihrem (Nach-) Namen ist datenschutzrechtlich problematisch. Dieser wird so dritten Patienten bisher meist ungefragt zugänglich gemacht.	<a href="#">Link (S.232)</a>
2018	TLFDI (Thüringen)	Deutschland	Auskunft		Arztpraxen	Das Faxen medizinischer Befunde an weiterbehandelnde Ärzte ist erlaubt. Ein Fax kann technisch nicht verschlüsselt werden, dies ist gemäß § 88 TKG auch nicht erforderlich. Der Geschäftsführer eines Arztpraxen beratenden Unternehmens wandte sich im Mai 2018 den TLFDI. Er wollte wissen, ob und unter welchen Voraussetzungen Praxen ärztliche Dokumente faxen dürfen.	<a href="#">Link (S.233)</a>

2018	TLFDI (Thüringen)	Deutschland	Auskunft		Arztpraxen	Bestandspatienten sollten die Informationen nach Art. 13, 14 DS-GVO innerhalb von zwei Jahren nach Inkrafttreten der DS-GVO erhalten (Erwägungsgrund 171 DS-GVO). Ärzte sind beim Abholen von Medikamenten durch dritte Personen gesetzlich nicht verpflichtet, die Vollmacht inklusive persönlicher Angaben des Abholers aufzubewahren. Nach Art. 6 I b DS-GVO wäre dies aber empfehlenswert. Im April 2018 erkundigte sich der Geschäftsführer eines Qualitätsmanagement-Unternehmens aus NRW diesbezüglich beim TLFDI.	<a href="#">Link (S.246)</a>
2018	TLFDI (Thüringen)	Deutschland	Überprüfung, eine Datenschutzverletzung konnte nicht festgestellt werden	Art. 19 DS-GVO	Medizinischer Dienst der Krankenversicherung Thüringen e. V.	Die sensiblen Gesundheitsdaten sind nach Art. 9 Abs. 1 DS-GVO besonders zu schützen. Unbeteiligte bzw. unbefugte Personen dürfen nicht bei medizinischen Team-Sitzungen zur Planung der Weiterbehandlung von Patienten anwesend sein. Die unerlaubte Offenlegung personenbezogener Daten gegenüber Dritten stellt einen Datenschutzverstoß dar (Art. 9 DS-GVO). So sind Beschäftigte des Medizinischen Dienstes der Krankenversicherung Thüringen e. V. nicht therapeutisch tätig und haben an medizinischen Team-Sitzungen eigentlich nicht teilzunehmen. Diesbezüglich erhielt der TLFDI im Juni 2018 eine anonyme Beschwerde. Im konkreten Fall konnte jedoch keine Datenschutzverletzung festgestellt werden.	<a href="#">Link (S.242)</a>
2018	TLFDI (Thüringen)	Deutschland	Übereinstimmung nach Überprüfung	Art. 5 II, 7 I DS-GVO		Nach Art. 5 II, 7 I DS-GVO muss der Verantwortliche nachweisen, dass die Datenerhebung und -verarbeitung rechtmäßig erfolgt (vorherige Einwilligungserklärung als Beispiel). Ärzte dürfen auf entsprechende behördliche Zusicherungen vertrauen. Wenn auf einer Kopie der Einwilligung auf ärztlicher Seite bestanden wird, kommt dem die zuständige Behörde in aller Regel nach. Im Juli 2018 bewerteten sich zwei Arztpraxen beim TLFDI. Es wurde sich darauf geeinigt, den bisherigen Zustand beizubehalten. Der TLFDI prüfte nur, ob dem die DS-GVO entgegenstehen könnte und verneinte dies.	<a href="#">Link (S.243)</a>
2018	TLFDI (Thüringen)	Deutschland	Überprüfung, eine Datenschutzverletzung konnte nicht festgestellt werden		privater medizinischer Pflegedienst	Kürzung von Pflegegeld bei Mängeln: Nach § 11 i des Rahmenvertrags nach § 75 SGB XI zur ambulanten pflegerischen Versorgung im Freistaat Thüringen zwischen den Landesverbänden der Pflegekassen und der Arbeitsgemeinschaft der kommunalen Spitzenverbände sowie den Vereinigungen der Träger der ambulanten Pflegeeinrichtungen soll der Pflegedienst der Pflegekasse mitteilen, wenn aus seiner Sicht Maßnahmen zur Prävention in Betracht kommen. Die DS-GVO erlaubt auch zukünftig spezialgesetzliche nationale Regelungen (auch solche des SGB) anzuwenden. Im Juli 2018 ging die Beschwerde eines Bürgers über einen privaten medizinischen Pflegedienst beim TLFDI ein.	<a href="#">Link (S.245)</a>
2018	TLFDI (Thüringen)	Deutschland	Auskunft		Zahnärzte und Dentallabore	Bei dem mit einer Kooperation zwischen Zahnärzten und Dentallaboren verbundenen Austausch von Patientendaten liegt nicht immer eine Auftragsverarbeitung vor. Auch eine Weiterleitung nach Art. 9 II h DS-GVO kommt in Betracht. Es ist zwischen verschiedenen Konstellationen zu unterscheiden. Die Notwendigkeit eines Vertrags zur Auftragsverarbeitung nach Art. 28 II DS-GVO hängt vor allem von der Frage ab, ob ein Laborarzt oder Zahntechniker das Dentallabor leitet.	<a href="#">Link (S.246)</a>
2018	ULD (Schleswig-Holstein)	Deutschland		Art. 17 I a DS-GVO	Ärzte	Ärzte müssen ihre Patientenbehandlungen dokumentieren, vgl. Art. 9 II h DS-GVO, § 22 I Nr. 1 b BDSG, § 630f I BGB, § 10 der Berufsordnung der Ärztekammer Schleswig-Holstein. Aus Art. 17 I a DS-GVO lässt sich auch für Patienten das „Recht auf Vergessenwerden“ ableiten. Personenbezogene Daten müssen gelöscht werden, sobald sie für den mit ihnen verfolgten Zweck nicht mehr zwingend benötigt werden. Ausnahmsweise muss die Patientendokumentation aber weiterhin aufbewahrt werden, sofern eine rechtliche Verpflichtung dies erfordert (Art. 17 III b DSGVO) oder der Löschung Aufbewahrungsfristen aus Satzung oder Vertrag entgegenstehen (§ 35 III BDSG). Das ULD hält eine Aufbewahrungsfrist von zehn Jahren einerseits zwar regelhaft für geboten, andererseits aber auch für völlig ausreichend.	<a href="#">Link (S.77)</a>
2018	ULD (Schleswig-Holstein)	Deutschland			Heilberufler	Neuerdings ist eine Auftragsverarbeitung auch ohne Einwilligung der Patienten möglich. Art. 28 DSGVO regelt, welche Inhalte ein dafür erforderlicher Vertrag haben muss. Wenn dies für die Dienstleistung nötig ist, dürfen Heilberufler nun ihren Dienstleistern Daten ihrer Patienten offenlegen. Dabei muss der Heilberufler jedoch sicherstellen, dass die bei seinem Dienstleister tätigen Personen zur Geheimhaltung verpflichtet sind.	<a href="#">Link (S.78)</a>
2018	ULD (Schleswig-Holstein)	Deutschland			Gemeinde	Eine Kommune verlangte von einer Klinik ihr aufgrund der Kurabgabebesatzung die Patientennamen sowie deren jeweilige Aufenthaltsdauer mitzuteilen, um mit diesen Daten Kurabgabebescheide zu erlassen. Die Kliniken sollten sogar die Kurabgabe für die Kommune eintreiben. Die Klinik sah darin eine Verletzung der ärztlichen Schweigepflicht. Das ULD stellte dazu klar, dass die ärztliche Schweigepflicht einen starken Schutz bietet und grundsätzlich auch zur Kurabgabenerhebung nicht durchbrochen werden darf.	<a href="#">Link (S.79)</a>
2018	Bayerisches Landesamt für Datenschutzaufsicht	Deutschland			Arztpraxen	Das bayerische Landesamt für Datenschutzaufsicht stellte fest, dass Arztpraxen ziemlich oft von ihren Patienten unnötige Einwilligungen für Datenverarbeitungsvorgänge verlangen. Denn Art. 9 II h DS-GVO erlaube die erforderliche Verarbeitung von Gesundheitsdaten unter anderem im Rahmen der Gesundheitsvorsorge, Arbeitsmedizin, medizinischen Diagnostik, Versorgung oder Behandlung im Gesundheitsbereich sowie wenn die Datenverarbeitung aufgrund nationaler Vorschriften oder eines Behandlungsvertrages geschieht. Voraussetzung dabei ist allerdings, dass dies durch Personen bzw. unter deren Verantwortung erfolgt, die Berufsheimlichkeitspflicht sind oder an eine andere Geheimhaltungspflicht gebunden sind.	<a href="#">Link (S.91)</a>
2018	Bayerisches Landesamt für Datenschutzaufsicht	Deutschland	Aufforderungen		Arztpraxen	In vielen Arztpraxen bestehen bei der Anmeldung sowie im Sprechzimmer weiterhin Datenschutzlücken. Den Aufforderungen des bayerischen Landesamts für Datenschutzaufsicht an die jeweiligen Verantwortlichen zur Behebung der Missstände ist meist sehr gut nachgekommen worden.	<a href="#">Link (S.92)</a>
2018	Bayerisches Landesamt für Datenschutzaufsicht	Deutschland			Arztpraxen	Auch unter der DS-GVO soll die namentliche Ansprache von Patienten weiterhin zulässig sein. Anderweitige Informationen wertet das bayerische Landesamt für Datenschutzaufsicht als „Panikmache rund um die DS-GVO“. Bitten von Patienten um Diskretion sollten nach Möglichkeit aber beachtet werden.	<a href="#">Link (S.92)</a>
2018	Bayerisches Landesamt für Datenschutzaufsicht	Deutschland	Auskunft			Mehrere Ärzte wandten sich an das bayerische Landesamt für Datenschutzaufsicht, weil sie Patientendaten an ein Gericht weitergeben sollten, ohne die Schweigepflichtbindungserklärung des Patienten zumindest in Form einer Kopie als Beleg zu bekommen. Das Landesamt stellte diesbezüglich klar, dass Gerichtsentscheidungen über eine Schweigepflichtentbindung für Ärzte verbindlich sind. Auch unter der DS-GVO kann kein Beleg verlangt werden. Erforderlich ist (nur) die ausdrückliche Aussage des Gerichtes über die Schweigepflichtentbindung durch den Patienten. Zur Erfüllung der ärztlichen Rechenschaftspflicht wurde die Dokumentation einer solchen gerichtlichen Erklärung als ausreichend erachtet.	<a href="#">Link (S.93)</a>
2018	Bayerisches Landesamt für Datenschutzaufsicht	Deutschland			Arztpraxen	Für eine Offenlegung von Gesundheitsdaten an den Ehepartner durch Arztpraxen ist grundsätzlich eine Einwilligung sowie Schweigepflichtentbindungserklärung des Patienten erforderlich.	<a href="#">Link (S.93)</a>
2018	Bayerisches Landesamt für Datenschutzaufsicht	Deutschland			Heilpraktiker	Heilpraktiker bedürfen seit Wirksamwerden der DS-GVO als Rechtsgrundlage für Verarbeitungen von Gesundheitsdaten eine ausdrückliche Einwilligung der betroffenen Personen. Der gesetzliche Erlaubnistatbestand des Art. 9 II h DS-GVO greift nicht, weil Heilpraktiker keinem Berufsheimlichkeits- oder Geheimhaltungspflicht iSv Art. 9 III DS-GVO, § 22 I Nr. 1 b BDSG unterliegen.	<a href="#">Link (S.94)</a>
2018	Bayerisches Landesamt für Datenschutzaufsicht	Deutschland			Ärzte	Gemäß Art. 32 DS-GVO müssen Verantwortliche (Ärzte) technische sowie organisatorische Maßnahmen treffen, um ein risikogerechtes Schutzniveau zu gewährleisten. Ein wichtiger Grundsatz ist die Vertraulichkeit und Integrität der Daten. Demgegenüber können unverschlüsselte E-Mails diesen datenschutzrechtlichen Anforderungen nicht gerecht werden. Im Arzt-Patient-Verhältnis werden besonders schützenswerte Gesundheitsdaten verarbeitet, vgl. Art. 9 DS-GVO und auch § 203 StGB. Für die E-Mail-Kommunikation ist also eine Ende-zu-Ende-Verschlüsselung zu fordern. Patienten können darauf aber auf eigenen Wunsch verzichten.	<a href="#">Link (S.94)</a>

2018	Bayerisches Landesamt für Datenschutzaufsicht	Deutschland		Optiker und Sanitätshäuser	Verantwortliche aus dem Gesundheitshandwerk benötigen für die Verarbeitung von Gesundheitsdaten seit der DS-GVO eine ausdrückliche Einwilligung der betroffenen Personen. Der gesetzliche Erlaubnistatbestand des Art. 9 II h DS-GVO scheidet aus, weil sie an kein Berufsgeheimnis oder Geheimhaltungspflicht iSv Art. 9 III DS-GVO, § 22 I Nr. 1 b BDSG gebunden sind. Optiker können z.B. keine passende Lesebrille ohne Einwilligung in die Verarbeitung der Sehschärfe anfertigen. Weil diese Einwilligung für die Erfüllung eines solchen Vertrages erforderlich ist, bestehen keine Zweifel an ihrer Freiwilligkeit (Art. 7 Abs. 4 DS-GVO).	<a href="#">Link (S.95)</a>	
2018	Bayerisches Landesamt für Datenschutzaufsicht	Deutschland	Auskunft	Betreiber eines Seniorenheimes	In Seniorenheimen ist das Anbringen von Türschildern, individuellen Briefkästen sowie das Führen eines internen Telefonverzeichnisses auch nach der DS-GVO grundsätzlich zulässig. Die Betreiber eines Seniorenheimes fragten diesbezüglich nach. Art. 6 I f bzw. Art. 9 II a DS-GVO erlauben dies.	<a href="#">Link (S.95)</a>	
2018	LFD Sachsen-Anhalt	Deutschland	Klarstellung	(Zahn-) Ärzte	Zahlreiche Kontaktaufnahmen zeigten, dass viele (Zahn-) Ärzte wegen der DS-GVO für Datenverarbeitungen in ihren Praxen generell eine Patienteneinwilligung einholen. Dies ist aber gar nicht nötig, sofern die Datenverarbeitung zur Erfüllung eines Behandlungsvertrags erforderlich ist, vgl. Art. 6 I 1 b iVm Art. 9 II h DS-GVO. Auch gesetzliche Spezialnormen können Ärzte zur Datenverarbeitung befugt oder verpflichtet, z. B. § 295 SGB V. Die Verantwortlichen müssen aber stets ihre Informationspflichten (Art. 13, 14 DS-GVO) beachten. Ein entsprechender Nachweis (Art. 5 II DS-GVO) kann mittels freiwilliger Unterschrift des Patienten, alternativ durch einen Aushändigungsvermerk oder auch mit Dokumentation eines festgelegten Verfahrens zur Umsetzung der Informationspflicht erfolgen. Patienten darf keinesfalls ein Behandlungsabbruch bei Verweigerung der Unterschrift angedroht werden, dies wäre mit der DS-GVO nicht vereinbar.	<a href="#">Link (S.29)</a>	
2018	LFD Sachsen-Anhalt	Deutschland	Positionierung	Art. 9 II a	Heilpraktiker	Heilpraktiker wie z.B. Osteopathen oder Chiropraktiker üben zwar einerseits einen Gesundheitsberuf aus, unterliegen andererseits aber keiner gesetzlichen Geheimhaltungspflicht, die mit § 203 StGB vergleichbar ist. Teilweise mag es zwar vertraglich vereinbarte Geheimhaltungspflichten geben und manche haben sich auch freiwillig einer Geheimhaltungspflicht eines Berufsverbandes unterworfen. Weil es sich dabei aber nicht um gesetzlich geregelte Geheimhaltungspflichten handelt, lässt der LFD solche Vereinbarungen nicht genügen. Eine Datenverarbeitung ist für Heilpraktiker nur bei vorheriger Einwilligung zulässig (Art. 9 II a DS-GVO). Der LFD Sachsen-Anhalt hat sich diesbezüglich mit den weiteren Datenschutzaufsichtsbehörden in Deutschland abgestimmt, daraus resultierte eine gemeinsame Positionierung gegenüber einem Berufsverband.	<a href="#">Link (S.30)</a>
2018	LFD Sachsen-Anhalt	Deutschland	anlaufende Überprüfung			Im Rahmen der Schuleingangsuntersuchung werden in Sachsen-Anhalt über einen Elternfragebogen Daten der einzuschulenden Kinder auf Einwilligungsbasis abgefragt. Nun soll dies auf § 37 Abs. 2 SchulG LSA gestützt verpflichtend geschehen. Es sollen Daten zum Sozialstatus, Migrationshintergrund, Rauchverhalten im Haushalt und zu Geschwistern des Kindes erhoben werden. Die Erforderlichkeit dieser umfangreichen Datenverarbeitung erscheint jedoch fraglich. Der Öffentliche Gesundheitsdienst stützt sich auf Erkenntnisse aus diversen Studien und argumentiert nur so eine optimale Beratung bieten zu können. Der LFD überprüft nun die Erforderlichkeit unter Berücksichtigung der Handhabung in anderen Bundesländern.	<a href="#">Link (S.30)</a>
2018	Unabhängiges Datenschutzzentrum Saarland	Deutschland	Auskunft	Arztpraxen	Fraglich war, ob Patienten im Wartezimmer weiterhin mit ihrem Namen aufgerufen werden dürfen. Das Datenschutzzentrum bejahte dies, eine anderweitige Auslegung der DS-GVO gehe in der Regel zu weit. Datenschutzrechtlich unzulässig ist jedoch ohne Zweifel die Erläuterung von Diagnosen im Beisein Dritter. Die Informationspflicht aus Art. 13 DS-GVO soll Patienten nur die Möglichkeit geben Informationen direkt und einfach zu erhalten. Eine Kenntnisnahme ist kein Muss. Ein Aushändigungsvermerk oder die Dokumentation eines festgelegten Verfahrens zur Umsetzung der Informationspflicht, das sicherstellt, dass Patienten im Regelfall die Informationen erhalten, genügt hinsichtlich der Nachweispflichten gegenüber der Aufsichtsbehörde.	<a href="#">Link (S.94)</a>	
2017/18	Unabhängiges Datenschutzzentrum Saarland	Deutschland	Kooperation	gesetzliche Krankenkassen	Ein Versicherter beschwerte sich über seine gesetzliche Krankenkasse hinsichtlich der Krankengeldzahlung. Seiner Meinung nach wurde die Aufgabentrennung zwischen Krankenkasse und Medizinischem Dienst der Krankenversicherungen bei der Datenerhebung nicht hinreichend beachtet. So forderte die Krankenkasse Unterlagen an, die aus Sicht des Versicherten nur für den MDK bestimmt seien. In Kooperation mit der Krankenkasse konnte beim Krankengeldfallmanagement eine bessere Umsetzung der datenschutzrechtlichen Bestimmungen erreicht werden.	<a href="#">Link (S.96)</a>	
2018	Unabhängiges Datenschutzzentrum Saarland	Deutschland	Stellungnahme			Im September 2018 wurde in einer Anhörung im saarländischen Landtag die gegenwärtige Lage der Telemedizin thematisiert. Dabei werden sehr sensible, besonders schutzwürdige Patientendaten übermittelt. Dabei ist der Datenschutz enorm wichtig. Folglich war auch der Landesbeauftragte für Datenschutz und Informationsfreiheit eingeladen. Sowohl die rechtlichen als auch technischen Voraussetzungen für die Einführung eines solchen Verfahrens waren erfüllt. Der LFD hatte keine Bedenken mehr. Der Echtbetrieb begann 2018.	<a href="#">Link (S.98)</a>
2017/18	Unabhängiges Datenschutzzentrum Saarland	Deutschland	Überprüfung	privater Pflegedienst	Das Unabhängige Datenschutzzentrum Saarland wurde anonym darauf hingewiesen, dass ein privater Pflegedienst sensible Dokumente mit Informationen über Mitarbeiter und Patienten über die „blaue Tonne“ entsorge. Ein unberechtigter Zugriff durch Dritte sei nicht ausgeschlossen. Es gehört zu den Grundsätzen der Verarbeitung personenbezogener Daten dagegen geeignete technische sowie organisatorische Maßnahmen zu ergreifen. Dies trifft insbesondere die Entsorgung solcher Unterlagen. Der Pflegedienst konnte allerdings nachweisen, dass er einen spezialisierten sowie TÜV-zertifizierten Dienstleister nutzt. Folglich handelt es nicht um eine unsachgemäße Entsorgung der Akten.	<a href="#">Link (S.100)</a>	
2017/18	Unabhängiges Datenschutzzentrum Saarland	Deutschland	Hinweis	Seniorenheim	Bei der Veröffentlichung von Daten und Fotos der Bewohner eines Seniorenheims durch Aushang handelt es sich datenschutzrechtlich um eine Datenübermittlung an Dritte. Hierfür ist eine rechtliche Grundlage, die es in diesem Fall aber nicht gibt, oder eine entsprechende Einwilligung erforderlich. Ein Seniorenheim wurde daher darüber informiert, dass es das Einverständnis der Betroffenen bzw. deren gesetzlicher Vertreter benötigt.	<a href="#">Link (S.101)</a>	
2017/18	LFD Niedersachsen	Deutschland	Begleitung	Klinisches Krebsregister Niedersachsen	Bei der mehrjährigen Begleitung des Gesetzgebungsverfahrens zum klinischen Krebsregister Niedersachsen wurden viele datenschutzrechtliche Forderungen des LFD umgesetzt, das umfassende Widerspruchsrecht der Betroffenen wurde jedoch noch nicht hinreichend geregelt.	<a href="#">Link (S.111)</a>	
2018/19	LFD Niedersachsen	Deutschland	anlassunabhängige Prüfung	Krankenhäuser	Anlassunabhängige Prüfung von drei Krankenhäusern hinsichtlich der DS-GVO: Haben die Datenschutzbeauftragten genügend Zeit? Sind die Zugriffsberechtigungen auf das Krankenhaus-informationssystem datenschutzkonform? Umsetzung des Auskunftsrechts nach Art. 15 DS-GVO sowie der Informationspflichten? Ergebnisse folgen im nächsten Tätigkeitsbericht.	<a href="#">Link (S.117)</a>	
2018	LFDI Mecklenburg-Vorpommern	Deutschland			Nach Art. 9 I iVm Art. 4 Nr. 15 DS-GVO gehören Gesundheitsdaten zu den äußerst sensiblen und deswegen besonders schutzwürdigen personenbezogenen Daten. Der LFDI geht davon aus, dass nach einer Übergangszeit für die Übermittlung solcher besonders sensibler Daten eine Ende-zu-Ende-Verschlüsselung einzufordern sein wird. In der Praxis wird zunächst keine Möglichkeit zur vollständigen Durchsetzung einer Ende-zu-Ende-Verschlüsselung bestehen. Daher soll bei Datenübermittlungen, die nicht unter Art. 9 DS-GVO fallen, auch eine Transportverschlüsselung akzeptiert werden. Für die Verarbeitung besonderer Kategorien von Daten (z.B. Gesundheitsdaten und genetische Daten) ist nach Art. 9 II a DS-GVO eine ausdrückliche Einwilligung nötig. Konkretes Handeln genügt nicht.	<a href="#">Link (S.33)</a>	

2018	Hessischer Beauftragter für Datenschutz und Informationsfreiheit	Deutschland		Prüfung und Beratung		Informationen nach Art. 13 DS-GVO müssen insbesondere transparent sowie bestimmt sein. Im Gesundheitswesen sind Betroffene prinzipiell in Papierform zu informieren, damit die Informationen zur weiteren Lektüre mitgenommen werden können. Einwilligungen sind strikt von den Informationen nach Art. 13 DS-GVO zu trennen. Dem LFDI wurden zahlreiche Dokumente zur Erfüllung der Informationspflicht zur Überprüfung vorgelegt.	<a href="#">Link (S.123)</a>	
2018	Hessischer Beauftragter für Datenschutz und Informationsfreiheit	Deutschland		Hinweis	Art. 13 DS-GVO	Angehörige von Gesundheitsberufen	Angehörige von Gesundheitsberufen dürfen, wenn Patienten sich weigern Informationen (Art. 13 DS-GVO) zu unterschreiben, keinesfalls mit einem Behandlungsabbruch oder ähnlichem drohen. Diverse derartige Fälle wurden dem LFDI gemeldet.	<a href="#">Link (S.125)</a>
2018	Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit	Deutschland		Beratung und Datenschutz-Kommunikation	Art. 13, 14 DS-GVO	Arztpraxen	Verantwortliche aus dem Gesundheitswesen haben ihren Patienten die in Art. 13, 14 DSGVO genannten Informationen über die Verarbeitung ihrer Daten bereitzustellen. Die Informationspflicht kann durch gut sichtbare und lesbare Aushänge an geeigneten Orten in der Praxis umgesetzt werden. Zudem sollten die Informationen auch als Handzettel ausgelegt werden. Bei der Aufnahme eines neuen Patienten ist auf die Informationen und deren Mitnahmemöglichkeit aufmerksam zu machen. Datenschutzinformationen müssen nicht unterschrieben werden. Allerdings sollte die Information dann auf eine andere, belastbare Weise dokumentiert werden.	<a href="#">Link (S.118)</a>
2018	Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit	Deutschland		Beratung und Datenschutz-Kommunikation			Die Erhebung, Speicherung und Nutzung von Gesundheitsdaten durch einen Verantwortlichen im medizinischen Bereich ist im nach dem Behandlungsvertrag erforderlichen Umfang auch ohne Einwilligungserklärung der Patienten zulässig, vgl. Art. 9 II h letzte Alternative DS-GVO. Für zusätzliche Dienste (z.B. Newsletter und Recall-Service) ist die damit verbundene Verarbeitung von Patientendaten nicht durch den Behandlungsvertrag gedeckt. Die Einwilligung des Patienten ist daher erforderlich.	<a href="#">Link (S.118)</a>
2018	Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit	Deutschland		Beratung und Datenschutz-Kommunikation			Eine wegen Nichtunterschreibens der Datenschutzinformationen oder Ablehnung einer Einwilligungserklärung erfolgende Behandlungsverweigerung kann weder auf Art. 13, 5 II DS-GVO, noch auf Art. 9 I DS-GVO gestützt werden.	<a href="#">Link (S.120)</a>
2018	Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit	Deutschland		Beratung und Datenschutz-Kommunikation			Sicherheitsaspekte bei der Verarbeitung von Gesundheitsdaten begründen bei der elektronischen Speicherung sowie Übermittlung von Gesundheitsdaten grundsätzlich eine Verschlüsselungspflicht.	<a href="#">Link (S.120)</a>
2018	Landesbeauftragter für Datenschutz und Akteneinsicht Brandenburg	Deutschland		Auskunft			Der Landesbeauftragte für Datenschutz und Akteneinsicht Brandenburg wies regelmäßig darauf hin, dass die Erfüllung der datenschutzrechtlichen Informationspflicht ein aktives Angebot des Verantwortlichen gegenüber den betroffenen Personen erfordert. Es besteht keine Verpflichtung auf das Informationsangebot einzugehen, etwas zu unterschreiben oder ähnliches. Der Landesbeauftragte ermutigt Praxen mit den namentlichen Aufrufen fortzufahren. Nur mit Personen, die um Discretion bitten, sollten Alternativen abgesprochen werden. Darüber hinaus seien die Aufbewahrungsfristen für ärztliche Dokumentationen als Ausnahmen von der Löschungspflicht zu berücksichtigen.	<a href="#">Link (S.17)</a>
2018	Landesbeauftragter für Datenschutz und Akteneinsicht Brandenburg	Deutschland		Prüfung und Begleitung		Klinisches Krebsregister der Länder Brandenburg und Berlin	Der Landesbeauftragte für Datenschutz und Akteneinsicht Brandenburg prüfte zusammen mit dem Berliner LFDI das gemeinsame Klinische Krebsregister der beiden Länder. Ein besonderes Augenmerk galt der physischen Sicherheit der Registerstelle, Revisionsicherheit und dem Vorhandensein von Berechtigungskonzepten - also technischen sowie organisatorischen Maßnahmen, um ein adäquates Sicherheitsniveau sicherzustellen. Die Registerstelle Berlin besitzt jedoch weiterhin kein umfassendes Löschkonzept. Es wurde zugesichert, dass ein solches bis Mitte 2019 erstellt und umgesetzt wird. Zwar gibt es ein Revisionskonzept, in den Protokolldateien wurden allerdings auch medizinische Daten gespeichert. Daher wurde auf eine inhaltliche Anpassung der Protokolldateien gedrängt. Auch die Einführung einer smartcardbasierten Zwei-Faktor-Authentifizierung der Nutzer soll datenschutzrechtlich begleitet werden.	<a href="#">Link (S.59)</a>
2018	Landesbeauftragter für Datenschutz und Akteneinsicht Brandenburg	Deutschland		nach Zusage keine weiteren Maßnahmen		Physiotherapeut	Die Nutzung von digitalen Sprachassistenten in Behandlungsräumen greift potentiell in die Rechte und Freiheiten der Betroffenen ein. In einer solchen Umgebung werden in Gesprächen auch vertrauliche Daten ausgetauscht. Nachdem die Geschäftsleitung einer Physiotherapie-Praxis mit einem solchen KI-Assistenten glaubhaft mitteilte, diesen nicht mehr einzusetzen, sah der Landesbeauftragte für Datenschutz und Akteneinsicht Brandenburg von einem weiteren Tätigwerden ab.	<a href="#">Link (S.69)</a>
2018	Landesbeauftragter für Datenschutz und Akteneinsicht Brandenburg	Deutschland		dringende Empfehlung		Hebamme	Eine Beratungsdienstleistungen über Skype anbietende Hebamme wollte ihr Angebot nach der DS-GVO datenschutzkonform ausgestalten. Auf Nachfrage wurde der Hebamme vom Landesbeauftragten für Datenschutz und Akteneinsicht Brandenburg auf Nachfrage dringend empfohlen die Skype-Nutzung bleiben zu lassen.	<a href="#">Link (S.70)</a>
2018	Landesbeauftragter für Datenschutz und Akteneinsicht Brandenburg	Deutschland		Beratung		Medizinische Hochschule Brandenburg	Registerforschungen sollten nur mit pseudonymisierten Daten vorgenommen werden. Auch das Fehlen einer unabhängigen Vertrauensstelle, die eine Pseudonymisierung gewährleisten könnte, wurde bemängelt. Der Landesbeauftragte für Datenschutz und Akteneinsicht Brandenburg wies auch darauf hin, dass aufgrund der Art und Menge der Angaben eine personelle Zuordnung der Daten nicht ausgeschlossen werden könne. Das Herzinfarktregister sowie alle Auftragsverarbeiter sollten zur Sicherheit der Datenverarbeitung technische sowie organisatorische Maßnahmen treffen. Ein dem Risiko angemessenes Schutzniveau ist zu gewährleisten. Gefordert wurde eine Risikoanalyse sowie ein IT-Sicherheitskonzept für das Registerzentrum, die Erhebungszentren und die beteiligten Auftragsverarbeiter. Außerdem wird eine Datenschutz-Folgenabschätzung notwendig sein.	<a href="#">Link (S.96)</a>
10.07.1905	Bayerischer Landesbeauftragter für den Datenschutz	Deutschland				Krankenhäuser	Die Öffnungsklauseln der DS-GVO und die Möglichkeit zur Konkretisierung ihrer allgemeinen Vorschriften ermöglichen auch im Krankenhausbereich meist die Beibehaltung der bisherigen datenschutzrechtlichen Spezialvorschriften.	<a href="#">Link (S.114)</a>
2017/18	Bayerischer Landesbeauftragter für den Datenschutz	Deutschland				Krankenhäuser	Beim Austausch zwischen Krankenhäusern und Ermittlungsbehörden stellt sich regelmäßig die Frage, ob und inwieweit personenbezogene Daten von Beschäftigten oder Patienten an die Polizei weitergegeben werden dürfen. Anschließend werden im Tätigkeitsbericht (Link) die häufigsten Fallgestaltungen besprochen.	<a href="#">Link (S.115)</a>
2017/18	Bayerischer Landesbeauftragter für den Datenschutz	Deutschland		förmliche Beanstandung		Universitätsklinikum	Ein Universitätsklinikum übermittelte wiederholt personenbezogene Daten eines Patienten ohne dessen Einverständnis an externe Abrechnungsfirmen. Die Datenschutzverstöße waren dem Klinikum auch zuzurechnen. Die zunächst ergriffenen Maßnahmen behoben den Mangel nicht. Der wiederholte Datenschutzverstoß legte einen systematischen Fehler nahe. Dies hatte eine förmliche Beanstandung zur Konsequenz.	<a href="#">Link (S.116)</a>
2017/18	Bayerischer Landesbeauftragter für den Datenschutz	Deutschland		förmliche Beanstandung		Universitätsklinikum	Ein Universitätsklinikum informierte das Jugendamt ohne Befugnis und damit datenschutzwidrig über den genetischen Befund eines Patienten. Des Weiteren gab der behandelnde Arzt die medizinischen Daten ohne Erlaubnis an neun Therapeuten aus der Klinik weiter. Dies führte zu einer förmlichen Beanstandung.	<a href="#">Link (S.117)</a>
2017/18	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI)	Deutschland					Der Gesetzgeber hat den Schutz von Gesundheitsdaten und genetischen Daten auch im Rahmen der Forschung mit diesen Daten zu gewährleisten.	<a href="#">Link (S.56)</a>
2017/18	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI)	Deutschland					Um den datenschutzrechtlichen Standards zu genügen, sind für die Nutzung von elektronischen Patienten- und Gesundheitsakten weitere gesetzliche Grundlagen und Rahmenbedingungen zu schaffen. Insbesondere muss die Datenhoheit eindeutig bei dem Versicherten liegen. Von besonderer Bedeutung ist zudem die Freiwilligkeit der Nutzung einer solchen „Gesundheitsdatensammlung“.	<a href="#">Link (S.57)</a>
2018	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI)	Deutschland					Die Frage, wer Verantwortlicher für die Telematik-Infrastruktur ist und damit eine Datenschutz-Folgenabschätzung vorzulegen hat, konnte noch nicht endgültig geklärt werden.	<a href="#">Link (S.58)</a>

2017/18	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI)	Deutschland	beratendes Gespräch			Die datenschutzkonforme Umsetzung des Krankengeldfallmanagements durch die Krankenkassen lässt trotz bereits länger vorhandener gesetzlicher Grundlage (§ 44 IV SGB V) immer noch auf sich warten.	<a href="#">Link (S.60)</a>
2018	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI)	Deutschland	Hinweis	Art. 9 I DS-GVO	Sozialversicherungsträger	Im Kontakt mit Sozialversicherungsträgern sind sehr häufig gesundheitsbezogene Daten betroffen, die zu den besonderen Kategorien personenbezogener Daten gehören (Art. 9 I DS-GVO). Damit geht ein besonders hohes Schutzniveau einher. Der BfDI hat die Sozialversicherungsträger daher darauf hingewiesen, dass aufgrund fehlender Datenschutzkonformität viele Messenger-Dienste (insbesondere WhatsApp) kein geeignetes Kommunikationsmedium darstellen.	<a href="#">Link (S.61)</a>
2018	Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI)	Deutschland				Bei künftigen Registern im Gesundheitsbereich ist eine von der eigentlichen Registerstelle getrennte Vertrauensstelle zu schaffen. Beide müssen ein angemessenes Datenschutzniveau besitzen, insbesondere bei Pseudonymisierungsverfahren. Das Datenschutzkonzept sollte auch die Gewährleistung des Auskunftsrechts regeln.	<a href="#">Link (S.61)</a>
9.7.19	Belgian Data Protection Authority (DPA)	Belgien	Rüge (reprimand)		FPS Public Health	FPS Public Health wurde gerügt, weil es nicht auf die Ausübung des Auskunftsrechts eines Bürgers reagierte.	<a href="#">Link</a> <a href="#">Link</a>
20.12.18	Italian Garante	Italien	Beschluss (decision)		Agenzia delle Entrate	Für Gesundheitsdienstleistungen müssen keine elektronischen Rechnungen an die italienische Steuerbehörde herausgegeben werden.	<a href="#">Link</a>
27.3.19	Europarat		Empfehlung			Empfehlung des Ministerkomitees an die Mitgliedstaaten zum Schutz gesundheitsbezogener Daten	<a href="#">Link</a> <a href="#">Link</a>
1.5.18	Autoriteit Persoonsgegevens	Niederlande	supervisory framework			Bei Gesundheitseinrichtungen ist der Autoriteit Persoonsgegevens besonders wichtig, wie die personenbezogenen Daten geschützt werden und ob die Verarbeitungsvorgänge auf einer legitimen Rechtsgrundlage beruhen, insbesondere beim Austausch von Daten. Die Autoriteit Persoonsgegevens überwacht, ob die Datenverarbeitungsvorgänge hinreichend dokumentiert werden, ein Datenschutzbeauftragter ernannt wird und wie dieser positioniert ist. Der Datenschutzbeauftragte muss in der Lage sein die ihm übertragenen Aufgaben und Pflichten zu erfüllen (DS-GVO). Dies gab die Autoriteit Persoonsgegevens in ihrem „supervisory framework“ bekannt.	<a href="#">Link</a>
24.6.19	Autoriteit Persoonsgegevens	Niederlande	Nachricht			Datenschutzbeauftragte in Krankenhäusern funktionieren grundsätzlich gut. Insbesondere kleinere Krankenhäuser können sich jedoch noch verbessern, indem sie mehr schriftliche Garantien (schriftelijke waarborgen) einführen.	<a href="#">Link</a>
20.6.18	CNIL	Frankreich	praktischer Leitfaden			Der Nationalrat der Ärztekammer und die CNIL veröffentlichten einen praktischen Leitfaden für Ärzte zur DS-GVO.	<a href="#">Link</a>
22.2.19	UODO	Polen				Die Veröffentlichung von Patientenlisten mit deren persönlichen Daten und Behandlungszeiten in Kliniken ist unzulässig. Türschilder mit den Namen der behandelnden Ärzte verstoßen jedoch nicht gegen die DS-GVO.	<a href="#">Link</a>
13.8.18	UODO	Polen	gestartete Überprüfung			Das Erstellen einer "schwarzen Liste" unzuverlässiger Patienten ruft Bedenken der Datenschutzbehörde hervor. Sie prüft von Amts wegen, ob dies mit der DS-GVO vereinbar ist.	<a href="#">Link</a>
31.7.19	UODO	Polen				Es ging um die Frage, wie Bewohner eines Pflegeheims im Zusammenhang mit der Verabreichung von Medikamenten datenschutzkonform identifiziert werden können.	<a href="#">Link</a>
7.1.19	UODO	Polen				Wann soll ein Datenschutzbeauftragter bestellt werden?	<a href="#">Link</a>
19.10.18	CNPD	Luxemburg	Stellungnahme			Stellungnahme der CNPD zum Entwurf einer Großherzoglichen Verordnung über den minimalen Inhalt des individuellen Dossiers von Krankenhauspatienten	<a href="#">Link</a> <a href="#">Link</a>
15.1.19	dsb	Österreich	Beschaid, Beschwerde	Art. 12 IV, 17 DS-GVO	Arztsuch-/Bewertungsportal	Der Beschwerdeführer ist Arzt, die Beschwerdegegnerin betreibt ein Arztsuch-/Bewertungsportal im Internet. Dort wurden Berufsadresse, Telefonnummer, Öffnungszeiten, Diplome, Zertifikate und Name des Beschwerdeführers als Arztprofil publiziert. Patienten können auf dem Portal Arztbesuche bewerten und ihre Erfahrungen schildern. Die Datenschutzbehörde kam zu dem Ergebnis, schlussendlich eine Verletzung des Rechts auf Geheimhaltung zu verneinen ist. Die berechtigten Interessen der das Portal nutzenden Patienten überwiegen die des Arztes. Daher ist Art. 17 I d DS-GVO nicht erfüllt, die Verarbeitung der personenbezogenen Daten ist rechtmäßig. Darüber hinaus ist sie nach Art. 17 III a DS-GVO zur Ausübung des Rechts auf freie Meinungsäußerung und Information erforderlich. Das Portal hat das Arztprofil zurecht nicht gelöscht.	<a href="#">Link</a>
16.11.18	dsb	Österreich	Beschaid, amtswegiges Prüfverfahren	Art. 6, 7 IV, 9, 12, 13, 14, 35, 37 DS-GVO	Allergie-Tagesklinik D*** GmbH	Die Verantwortliche ist eine GmbH mit Sitz in D***. Ihr Geschäftszweck ist die Diagnostik und Therapie von allergischen Erkrankungen mit Fokus auf Kinder und Familien. Angestellt waren drei Mitarbeiter im Management, 17 Ärzte, zwölf Büro-/Labormitarbeiter und zwei Ernährungsberater. Gesundheitsdaten als eine besondere Kategorie von Daten (vgl. Art. 9 DS-GVO) wurden regelmäßig und umfassend verarbeitet. Die Datenschutzbehörde stellt einen Verstoß gegen die Pflicht zur Bestellung eines Datenschutzbeauftragten fest, bemängelte die Verpflichtung von Patienten zu unklaren, gesetzwidrigen Einwilligungen und rügte die Nichteinhaltung der Informationspflichten. Zudem wurde unzutreffenderweise davon ausgegangen, dass eine Datenschutz-Folgenabschätzung entbehrlich sei. Der Verantwortlichen wurde aufgetragen, innerhalb einer Frist von acht Wochen bei sonstiger Exekution die Mängel zu beheben (bzw. damit zu beginnen).	<a href="#">Link</a>
8.8.18	dsb	Österreich	Beschaid, amtswegiges Prüfverfahren	Art. 33, 34 DS-GVO	N*** Hilfs- und Rettungsverband, Landesverband ****	Am 12.11.2018 wurde eine Sicherheitsverletzung nach Art. 33 DS-GVO gemeldet, weil am 10.11.2018 ein Suchtgiftbuch verloren ging. Die Datenschutzbehörde trug dem Verantwortlichen auf, innerhalb von vier Wochen alle Personen, deren Gesundheitsdaten betroffen sind, zu informieren und dies nachzuweisen.	<a href="#">Link</a>
6.6.18	dsb	Österreich	Beschaid, Beschwerde	Art. 15 DS-GVO	Magistrat der Stadt Wien – MA 63 (Krankenhaus **** Wien)	Die Datenschutzbehörde entschied über die Datenschutzbeschwerde von Frau Nora A*** gegen den Magistrat der Stadt Wien – MA 63 (Krankenhaus **** Wien) wegen einer Verletzung im Recht auf Auskunft (unvollständig erteilter Auskunft). Der Beschwerde wurde stattgegeben, weil nicht darüber informiert wurde, wer konkret auf die Krankenakte zugegriffen hat. Der Beschwerdegegner wurde angewiesen, innerhalb von zwei Wochen die entsprechende Auskunft zu erteilen.	<a href="#">Link</a>
4.6.18	dsb	Österreich	Beschaid, Beschwerde		Magistrat der Stadt Wien – MA 63	Die Datenschutzbehörde entschied über die Datenschutzbeschwerde von Frau Nora A*** gegen den Magistrat der Stadt Wien – MA 63 wegen einer Verletzung im Recht auf Geheimhaltung. Der Beschwerde wurde stattgegeben. Es konnten mehrere unerlaubte Zugriffe auf die elektronischen Gesundheitsakten (elektronische Krankengeschichte) der Beschwerdeführerin festgestellt werden.	<a href="#">Link</a>
16.07.19	BfDI	Deutschland	Anweisung		Sozialversicherungsträger (Kranken- und Pflegekassen, Berufsgenossenschaften, Deutsche Rentenversicherung)	Der BfDI hat die Sozialversicherungsträger angewiesen, mit Versicherten nur noch auf datenschutzrechtlich unbedenkliche, sichere Weise zu kommunizieren. Dazu gehören die schriftliche Briefpost und verschlüsselte E-Mails. Unverschlüsselte E-Mails seien jedoch vom Schutzniveau auf die besonders sensiblen Gesundheitsdaten unangemessen. Ob durch ausdrückliche Einwilligung der Betroffenen auf ein der DSGVO entsprechendes Schutzniveau wirksam verzichtet werden könne, sei noch gerichtlich zu klären.	<a href="#">Link</a>
Dez 18	Berliner Beauftragte für Datenschutz und Informationsfreiheit	Deutschland	Hinweis		Ärzte	Die Berliner Datenschutzbeauftragte überprüft derzeit die datenschutzrechtlichen Implikationen einer elektronischen Gesundheitsakte und hat bereits Mängel festgestellt. Dem Betreiber wurde Zeit eingeräumt, die Mängel zu beheben, teils sei dies bereits geschehen. In einer Pressemitteilung wies die Datenschutzbeauftragte nun darauf hin, dass die Vorteile einer zentral gespeicherten und verwaltbaren Gesundheitsakte nicht zu Lasten des Datenschutzes gehen dürfen. Ärzte seien nicht verpflichtet, Daten in eine elektronische Gesundheitsakte eintragen zu lassen. Die Übermittlung von Daten an die Betreiber elektronischer Gesundheitsakten dürfe daher nur (verschlüsselt) erfolgen, wenn die Anforderung klar von dem Betroffenen ausgehe.	<a href="#">Link</a>

2019	LFDI Mecklenburg-Vorpommern	Deutschland	Warnung	angebliche Microsoft-Mitarbeiter	Der LFDI warnt Ärzte und Kliniken davor, dass in Thüringen wiederholt angebliche Mitarbeiter von Microsoft telefonisch versucht haben, Zugriff auf sensible Daten in Arztpraxen zu erhalten. Nach Vortäuschung eines Virenbefalls würden die Angerufenen aufgefordert, über TeamViewer Zugang zu den Computern zu verschaffen. Der Landesdatenschutzbeauftragte geht allerdings davon aus, dass nicht die besonders sensiblen Gesundheitsdaten der Patienten Ziel der Angriffe seien, sondern eher Abrechnungs- und Kontoinformationen.	<a href="#">Link</a>
2019	LFDI Rheinland-Pfalz	Deutschland	laufendes Verfahren	große medizinische Einrichtung	Sensible Patientendaten wurden nicht ausreichend gegen fehlerhafte Verarbeitung geschützt. Weitere Informationen über das noch laufende Verfahren sind bisher nicht bekannt.	<a href="#">Link</a>
BayLDA						
2019		Bayern	laufende Untersuchung	Bayerisches Rotes Kreuz	Offenbar hat der Blutspendedienst des BRK aufgrund fehlerhafter Konfiguration seiner Webseite sensible Daten von Blutspendern automatisch an Facebook gesendet, darunter zum Beispiel Informationen über HIV-Erkrankungen oder Schwangerschaften. Die Untersuchung des Vorfalls ist noch nicht abgeschlossen.	<a href="#">Link</a>
	LFDI Bremen	Deutschland	Klinikum bestätigte lediglich den Namen und die Patientennummer in der Zukunft zu verwenden	Klinikum Bremen-Ost	Umfangreiche Beschriftung der Infusionsflaschen im Krankenhaus ( Name, Geburtsdatum, Adresse, Telefonnummer, Krankenkasse und Krankenversicherungsnummer)	Jahresbericht 2019, S. 36)
	LFDI Bremen	Deutschland	AV-Vertrag wurde abgeschlossen, Mängel hinsichtlich der Einwilligungserklärung wurden noch nicht behoben.	Ambulanter Pflegedienst	Der Pflegedienst besteht aus einem Kinderkrankenpflegedienst und einem Hauspflegedienst. Zwischen beiden Teilen wurden personenbezogene Daten ( in den Bereichen der Personalverwaltung, der Buchhaltung, der Qualitätssicherung und der Telefonzentrale) ohne Rechtsgrundlage übermittelt.	Jahresbericht 2019, S. 37)
	LFDI Bremen	Deutschland	Sensibilisierung und Verwarnung	Arztpraxen	Unrechtmäßige Übermittlung von Patientendaten an Abrechnungsunternehmen. ( Bei Privatpatienten ist dies nur mit Einwilligung möglich. Das geschah nicht immer).	Jahresbericht 2019, S. 37)
	LFDI Bremen	Deutschland	Hinweis, dass aufgrund von Transparenzgründen zukünftig weitere Informationen zu den gesetzlichen Grundlagen vorliegen müssen.	Zentrale Stelle des Mammographie-Screenings des Gesundheitsamts	Einladungsschreiben zu Mammographie-Screenings ( Verwendung von Adress- und Geburtsdaten ohne Nennung der Rechtsgrundlage).	Jahresbericht 2019, S. 37)
	LFDI Bremen	Deutschland	Die Versandapotheke verwendet nun eine zwei Faktor Authentisierung, um die Daten besser zu schützen.	Versandapotheke	Mangelhafte Auskunftersuchen bzw. Löschersuchen und falsch versendete Abrechnungen.	Jahresbericht 2019, S. 38)
	ULD (Schleswig-Holstein)	Deutschland	Warnung	Klinik	Die Informationen über eine frühere Behandlung in derselben Klinik in welcher die Betroffene eine Ausbildung tätigt wurde nicht davon getrennt, dass die Betroffene dort eine Ausbildung ausübt.	<a href="#">Link ( S. 70)</a>
	ULD (Schleswig-Holstein)	Deutschland	Warnung	Arztpraxis	Beauftragung einer Arztpraxis zur Entsorgung von Röntgenbilder durch eine Fake-Firma. Ferner wurde kein AV-Vertrag abgeschlossen.	<a href="#">Link ( S. 62)</a>