Gemeinsame Empfehlung hinsichtlich des Arbeitsaufwandes im Gesundheitsdatenschutz

Obwohl sich gerade in Deutschland durch die Einführung der Datenschutz-Grundverordnung (DS-GVO) bei den aus dem Datenschutz resultierenden Anforderungen im Vergleich zu vielen anderen europäischen Ländern wenig änderte, resultiert im Vergleich zur „Vor-DS-GVO-Zeit“ gerade aus den umfangreichen Nachweispflichten ein deutlicher Mehraufwand zur Erfüllung der datenschutzrechtlichen Pflichten. Auch zwei Jahre nach Geltungseintritt der DS-GVO herrscht hier noch eine Unsicherheit hinsichtlich des Bedarfs an Kräften im Bereich des Gesundheitsdatenschutzes vor. Daher entschlossen sich die nachfolgend genannten Verbände zu dieser gemeinsamen Empfehlung:

Berufsverband der Datenschutzbeauftragten Deutschlands e. V.

Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V.
Arbeitskreis „Datenschutz und IT-Sicherheit im Gesundheitswesen“

Gesellschaft für Datenschutz und Datensicherheit e. V.
Arbeitskreis „Datenschutz und Datensicherheit im Gesundheits- und Sozialwesen“

Autor(en)

Backer-Heuveldop, Andrea	ds² Unternehmensberatung GmbH & Co. KG
Mönikes, Klaus	privsec Klaus Mönikes Unternehmensberatung
Mönter, Johannes	CURACON GmbH
Rüdlin, Mark	Rechtsanwalt + Datenschutzbeauftragter
Schrenk, Nikolaus	Kliniken des Bezirks Oberbayern Kommunalunternehmen
Schütze, Dr. Bernd	Deutsche Telekom Healthcare and Security GmbH

Version 1.0

Stand der Bearbeitung: 01. Mai 2020

Copyright

Haftungsausschluss

Das vorliegende Werk ist nach bestem Wissen erstellt, der Inhalt wurde von den Autoren mit größter Sorgfalt zusammengestellt. Dennoch ist diese Ausarbeitung nur als Standpunkt der Autoren aufzufassen, eine Haftung für die Angaben übernehmen die Autoren nicht. Die in diesem Werk gegebenen Hinweise dürfen daher nicht direkt übernommen werden, sondern müssen vom Leser für die jeweilige Situation anhand der geltenden Vorschriften geprüft und angepasst werden.

Die Autoren sind bestrebt, in allen Publikationen die Urheberrechte der verwendeten Texte zu beachten, von ihnen selbst erstellte Texte zu nutzen oder auf lizenzfreie Texte zurückzugreifen.

Alle innerhalb dieses Dokumentes genannten und ggf. durch Dritte geschützten Marken- und Warenzeichen unterliegen uneingeschränkt den Bestimmungen des jeweils gültigen Kennzeichenrechts und den Besitzrechten der jeweiligen eingetragenen Eigentümer. Allein aufgrund der bloßen Nennung ist nicht der Schluss zu ziehen, dass Markenzeichen nicht durch Rechte Dritter geschützt sind!

Geschlechtergerechte Sprache

Hinweis bzgl. geschlechtsneutraler Formulierung im gesamten Text:

> Eine gleichstellungsgerechte Gesellschaft erfordert eine geschlechterneutrale Sprache. Geschlechterneutrale Sprache muss im deutschen Umfeld drei Geschlechtern gerecht werden: Divers, Frauen und Männern.
>
> Im folgenden Text wird, soweit möglich und sinnvoll, entsprechende Formulierungen genutzt (z. B. Paarformeln, Ableitungen). Personenbezeichnungen, bei denen es sich um juristische Fachbegriffe handelt, die sowohl natürliche als auch juristische Personen bezeichnen können, werden im folgenden Text nicht durch Paarformeln ersetzt. Dies gilt auch für technische Fachbegriffe, Definitionen und Zitate aus Normen (z. B. DIN EN ISO) und gesetzlichen Vorschriften. Entsprechende Begriffe sind im Sinne der Gleichbehandlung geschlechtsneutral zu interpretieren.
>
> Wo aus Gründen der leichteren Lesbarkeit bei personenbezogenen Substantiven und Pronomen nur ein Geschlecht dargestellt wurde, impliziert dies jedoch keine Benachteiligung der anderen beiden Geschlechter, sondern soll im Sinne der sprachlichen Vereinfachung als geschlechtsneutral verstanden werden.

Einführung ins Thema

Ob ein Datenschutzbeauftragter (DSB) benannt werden muss, regelt die DS- GVO und ggf. ergänzend das jeweilige nationale Recht – in Deutschland finden sich beispielsweise ergänzende Regelungen in § 5 Bundesdatenschutzgesetz (BDSG) für öffentliche Stellen bzw. § 38 BDSG für nichtöffentliche Stellen. Unabhängig von dieser Pflicht zur Benennung obliegt den für die Verarbeitung personenbezogener Daten Verantwortlichen (i. S. v. Art. 4 Ziff. 7 DS-GVO) die Pflicht, den datenschutzrechtlichen Vorgaben zu genügen. D.h. völlig unabhängig von der Pflicht zur Benennung einer oder eines Datenschutzbeauftragten existieren Pflichten aus dem Datenschutzrecht, denen Verantwortliche genügen müssen. Allerdings kann die freiwillige Benennung eines DSB dazu beitragen, diesen Aufwand weiter zu reduzieren, da diejenigen Beschäftigten, die mit der Erfüllung der datenschutzrechtlichen Pflichten betraut werden durch die Beratung des DSB für diese Tätigkeiten besser vorbereitet werden und in der Umsetzung Unterstützung finden.

Betrachtet wird grundsätzlich der vollständige Arbeitsaufwand für alle datenschutzrechtlichen Fragen. Es wird nicht der Arbeitsaufwand des Datenschutzbeauftragten dargestellt, sondern kumulativ der Aufwand aller Personen, die sich mit datenschutzrechtlichen Fragestellungen beschäftigen (z. B. IT-Mitarbeitende, die eine datenschutzrechtliche Dokumentation erstellen), betrachtet. Dabei wird eine professionelle Aufgabenerfüllung mit entsprechender Fachkenntnis vorausgesetzt. Evtl. notwendige Einarbeitungszeiten von nicht ausgebildeten Personen stehen nicht im Fokus dieser Arbeitshilfe und müssen gesondert betrachtet werden.

Einfluss auf den jeweils in der individuellen Situation tatsächlich auftretenden Aufwand haben natürlich diverse Faktoren. Berücksichtigt werden sollten daher Aspekte wie unterschiedliche Arbeitsgeschwindigkeiten von Menschen, unterschiedliche Komplexitäten sowohl in Unternehmensstrukturen als auch in den zu behandelnden Fragestellungen sowie mögliche Synergieeffekte, z.B. durch gut vernetzte Datenschutzbeauftragte, welche Lösungen von anderen Datenschutzbeauftragten auf das eigene Unternehmen übertragen können oder auch durch den Einsatz externer Datenschutzbeauftragter, die für mehrere ähnlich ausgerichteter Unternehmen tätig sind Daher ist bzgl. der hier enthaltenen Aussagen zum Aufwand regelhaft eine Bedarfsanpassung erforderlich, Hinweise zur Bedarfsanpassung sind daher Bestandteil dieser Empfehlung.

Die hier aufgeschriebenen Empfehlungen sollen Verantwortlichen in der Gesundheitsversorgung helfen, diesen Aufwand resp. Arbeitsbedarf abzuschätzen, um so die benötigten personellen Ressourcen einplanen und bereitzustellen zu können. Daher werden die Empfehlungen in „Vollbeschäftigtenäquivalent“ (englisch „full time equivalent“ oder abgekürzt FTE) angegeben, wobei im Folgenden davon ausgegangen wird, dass eine FTE einer Arbeitszeit von 40 Stunden/pro Woche entspricht. Die Empfehlungen beruhen auf im Alltag erworbenen Erfahrungswerten; wissenschaftliche Untersuchungen zum aus dem Datenschutzrecht entstehenden Aufwand erfolgten bisher leider nicht, obwohl dies sicherlich ein spannendes Untersuchungsthema sein könnte.

Empfehlung

Jeder Verantwortliche verarbeitet neben seinen Kunden-/Patientendaten immer auch Beschäftigtendaten und selbstverständlich stellt auch die Verarbeitung von Beschäftigtendaten eine Verarbeitung personenbezogener Daten i. S. d. DS-GVO dar. Bzgl. der Verarbeitung der Daten von Beschäftigten wird empfohlen 0,1 FTE auf etwa 500 Beschäftigte einzuplanen. Aufgaben sind hier insbesondere die Bearbeitung von Betroffenennachfragen im Rahmen des

Beschäftigtendatenschutzes, als erster Ansprechpartner für potenzielle Datenschutzverstöße zur Verfügung zu stehen sowie Unterstützung bei (internen) Audits zu leisten.

Speziell bei den medizinischen Leistungserbringern wie Krankenhäuser und Großarztpraxen ist die Arbeitsweise in den dort betriebenen Organisationseinheiten (= Gynäkologie, Herzchirurgie, Verwaltung, IT-Abteilung, Medizintechnik, usw.) häufig so unterschiedlich, dass hier ein Ansprechpartner mit etwa 0,1 FTE pro Organisationseinheit zur Verfügung stehen sollte, so dass hier ggf. mehr Stellen eingeplant werden müssen, als sich allein von der Anzahl der Beschäftigten ergibt. Gleiches gilt für entsprechende eigenständige Organisationseinheiten in anderen Unternehmen wie beispielsweise Softwarehäuser; für die Beurteilung ist relevant, in welchem Maß eine eigenständige Arbeitsweise separate datenschutzrechtliche Betrachtungen erfordert.

Für Kunden- bzw. Patientendaten wird für deren Nachfragen ebenfalls 0,1 FTE empfohlen. Aufgaben sind hier insbesondere die Bearbeitung von Betroffenennachfragen (im Sinne von Anfragen der Kunden bzw. Patienten), ggf. bei Kunden- bzw. Patientengesprächen bei Fragen zum Umgang mit datenschutzrechtlichen Fragen zu unterstützen sowie als Ansprechpartner für potenzielle Datenschutzverstöße zu agieren.

Speziell bei Leistungserbringern mit hohen Patientenzahlen werden 0,1 FTE pro 1000 Patienten empfohlen, da die Anzahl von Anfragen von Patienten deutlich zunimmt und der Aufwand durch die Vorgaben zur Dokumentation durch die DS-GVO deutlich angestiegen ist.

Pro größerem IT-System wie KIS oder PACS sollten etwa 0,2 FTE eingeplant werden; bei Einführung des Systems wird jedoch mehr Zeit benötigt, es geht nur um den Betrieb. Aufgaben sind hier insbesondere Anpassung Berechtigungskonzept, Prüfung, ob eine Datenschutz-Folgenabschätzung (DSFA) erstellt bzw. überarbeitet werden muss sowie ggf. Unterstützung bei der Erstellung der DSFA[1], Kontrolle, ob die technisch-organisatorischen Maßnahmen (TOM) für die Verarbeitung der personenbezogenen Daten noch ein dem Risiko angemessenes Schutzniveau bieten, Unterstützung beim Abschluss von Verträgen zur Auftragsverarbeitung usw.

Hersteller von IT-Systemen ist zu empfehlen, etwa 0,1 FTE für Akquisegespräche bei Kunden sowie für die Unterstützung bei Ausschreibungen usw. einzuplanen. Aufgaben sind hier insbesondere die Unterstützung beim Abschluss von Verträgen zur Auftragsverarbeitung sowie Beratung bei der Gewährlistung der aus dem Auftragsverarbeitungsvertrag resultierenden Unterstützungsverpflichtungen. Im laufenden Kundengeschäft gehört dazu aber natürlich auch die Bearbeitung von aus der Verarbeitung personenbezogener Daten resultierenden Datenschutz-Anfragen des Kunden.

Für die Entwicklung sowohl von neuen Prozessabläufen bei den versorgenden Einrichtungen sollte 0,1 FTE für die Berücksichtigung der Anforderungen aus dem Datenschutz eingeplant werden. Fragen wie „Privacy by Design/Default“ oder „Erfordernis einer Datenschutz-Folgeabschätzung“ bedürfen einer fachlichen Unterstützung, ebenso entstehen bei der erforderlichen Dokumentation ggf. Fragen, für die eine bzgl. Fragen aus dem Datenschutzbereich kompetente Person benötigt wird.

[1] DSFA = Datenschutz-Folgenabschätzung; Weitere Informationen zur DSFA in der Ausarbeitung von bvitg, GMDS und GDD: Datenschutz-Folgenabschätzung gemäß Art. 35 DS-GVO. [Online] 2014 [Zitiert 2018-03-18] Verfügbar unter https://gesundheitsdatenschutz.org/html/dsfa.php

Gleiches gilt für Hersteller von IT-Systemen, denn bei der Entwicklung von IT-Systemen muss von Anfang an berücksichtigt werden, wie die gesetzlich geforderten Unterstützungsleistungen (Art. 32 DS-GVO Sicherheit bei der Verarbeitung, Kap. III DS-GVO Betroffenenrechte, Art. 35 DS-GVO Datenschutz-Folgenabschätzung, Artt. 33, 34 DS-GVO Meldungen von Datenpannen) sowie die in Art. 28 Abs. 3 S. 2 lit. h DS-GVO geforderten Nachweispflichten erfüllt werden. Daher sollten auch Hersteller von IT-Systemen 0,1 FTE für diese Aspekte einplanen.

Im Bereich der medizinischen Forschung erfolgt häufig eine grenzüberschreitende Zusammenarbeit, nicht selten auch in Kooperation mit Organisationen/Einrichtungen in einem Drittstaat. Empfohlen wird hier 0,1 FTE pro größeres Forschungsprojekt pro Monat. Aufgaben sind hier insbesondere Mitwirkung bei der Erstellung der Einwilligungsformulare, Mithilfe bei der Umsetzung der aus den aus Art. 25 DS-GVO resultierenden Anforderungen hinsichtlich Privacy by Design/Default, Unterstützung bei der DSFA sowie Beratung bei der datenschutzrechtlichen Vertragsgestaltung.

Bedarfsanpassung

Die basierend auf den obigen Empfehlungen ermittelte Anzahl FTE muss natürlich den real existierenden Bedürfnissen angepasst werden. Kriterien hier können sein:

- Abhängig vom Betroffenen
    - Wie hoch ist die datenschutzrechtliche Affinität der Betroffenenkreise, so dass hier mit mehr oder weniger Aufwand zu rechnen ist?
- Abhängig von der individuellen Bearbeitungssituation
    - Wie hoch ist die Sensitivität der verarbeiteten personenbezogenen Daten? Wie hoch ist die Anzahl der Verarbeitungen, in denen besondere Kategorien personenbezogener Daten verarbeitet werden?
    - Wie hoch ist der Umfang der eingesetzten Verarbeitungen personenbezogener Daten?
    - Wie komplex sind die jeweiligen Verarbeitungen ausgestaltet?
    - Besteht ein langfristig stabiler Bestand an Verarbeitungen oder werden regelhaft innovativ neue Verarbeitungen erprobt/ eingesetzt?
- Abhängig von der Unternehmensorganisation
    - In welchem Maß sind bei dem jeweiligen Verantwortlichen Gruppe Standards im Einsatz, die Anforderungen aus dem Datenschutz adressieren und die aus diesen Standards resultierenden Vorgaben durch die eingeplanten Stellen abgearbeitet werden müssen?
    - In welchem Maß entwickeln sich bei den für den Datenschutz eingesetzten Stellen innerhalb des Verantwortlichen Synergieeffekte, die eventuell den individuellen Aufwand senken?
    - Wie hoch ist der Grad an Digitalisierung im jeweiligen Unternehmen?
    - Mit welcher Intensität werden die ausgewiesenen Stellen zur Bearbeitung sich aus dem Datenschutz ergebender Fragen in datenschutzrechtliche Vorgänge auch tatsächlich einbezogen? (Z. B. bei Festlegungen in Betriebsvereinbarungen)
    - Können evtl. durch den Einsatz einer/eines (externen) Datenschutzbeauftragten und dessen Fachexpertise bzw. beruflichen Netzwerkes evtl. Lösungen anderer Unternehmen auf die eigene Situation übertragen und angepasst werden, sodass Aufwände reduziert werden können?

- Abhängig von der Unternehmensstruktur[2]
  - Wie viele Beschäftigte verarbeiten personenbezogene Daten?
  - Wie viele Standorte hat das Unternehmen?
  - In wie vielen Ländern werden Produkte oder Dienstleistungen erbracht/angeboten?
  - Wie viele Dienstleister (Auftragsverarbeiter) werden eingesetzt?
  - Wie hoch ist der Umfang an Kooperationen innerhalb und außerhalb der verbundenen Unternehmen? (Z.B. Forschung oder Tochterunternehmen)

Beispiele zur Bedarfsermittlung

1. Arztpraxis

Eine hausärztliche Praxis mit insgesamt 6 Beschäftigten (zwei ärztlichen und vier nicht-ärztliche Beschäftigte) mit etwa 1.600 Behandlungsfällen[3] pro Quartal und daraus resultierend etwa 2000 Patienten pro Jahr. Entsprechend obiger Empfehlung resultiert daraus:

	Anzahl	Anzahl FTE	FTE (gesamt)
Anzahl beschäftigter Personen	6	0,1	0,1
Anzahl Organisationseinheiten	1	0,1	
Anzahl Patienten/ Kunden pro Jahr	2.000	0,1	0,2
IT System	1	0,2	0,2
Forschung	0	0,0	0,0
		Gesamt:	0,5

Diese 0,5 FTE werden jetzt entsprechend dem Bedarf angepasst:

Kriterien	Bewertung
Betroffenenaufwand	Sehr gering
Individuelle Bearbeitungssituation	Sehr standardisiert
Unternehmensorganisation	Flache Hierarchie, festgelegte Arbeitsabläufe, Praxis ist ISO 9001 zertifiziert mit Verfahrens- und Arbeitsanweisungen

1.1 Arztpraxis ohne Datenschutzbeauftragten

Ein DSB, der ggf. einen Teil der Aufgaben übernehmen würde, ist nicht benannt. In der Bedarfsanpassung werden basierend auf der Erfahrung der Praxisinhaber die FTE für Betroffene (sowohl bzgl. beschäftigter Personen als auch von Patienten) auf 0,1 reduziert, desgleichen der Aufwand für das IT-System. Damit sieht die angepasste Aufwandabschätzung wie folgt aus:

[2] Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V.: Positionspapier zu Aufwandsabschätzungen des Datenschutzbeauftragten. [Online] 2020 [Zitiert 202020-04-07] Verfügbar unter https://www.bvdnet.de/wp-content/uploads/2020/04/Positionspapier_Aufwandsabsch%C3%A4tzungen_DSB.pdf

[3] „Ein Behandlungsfall ist die Behandlung desselben Versicherten durch dieselbe Arztpraxis in einem Kalendervierteljahr zulasten derselben Krankenkasse.“ Quelle: Kassenärztliche Bundesvereinigung, Gesundheitsdaten. Online, zitiert am 2020-03-10; Verfügbar unter https://gesundheitsdaten.kbv.de/cms/html/17023.php

	Anzahl	Anzahl FTE	FTE (gesamt)
Anzahl beschäftigter Personen	6	0,1	0,1
Anzahl Organisationseinheiten	1	0,1	
Anzahl Patienten/ Kunden pro Jahr	2.000	0,1	
IT System	1	0,2	0,1
Forschung	0	0,0	0,0
		Gesamt:	0,2

Damit resultiert für die Beispielpraxis ein Arbeitsaufwand zur Erfüllung der datenschutzrechtlichen Anforderungen von etwa 0,2 FTE.

1.2 Arztpraxis mit Datenschutzbeauftragten

Ein externer DSB wurde benannt. Der beauftragte DSB betreut mehrere Arztpraxen und kann seine in den verschiedenen Arztpraxen gewonnenen Erfahrungen in die jeweiligen Arztpraxen einbringen, insbesondere fallen einige Pflegeaufgabe wie z.B. Überwachung von Änderungen im Datenschutzrecht nur einmal für alle Arztpraxen an. Auch kann er Anfragen betroffener Personen schnell abarbeiten, da er basierend auf seinen Erfahrungen die Anfragen schnell zuordnen und rechtlich bewerten kann. Gleichermaßen kennt er die IT-Systeme entsprechend gut, so dass den Herstellern des in der jeweiligen Arztpraxis eingesetzten Praxisverwaltungssystems die datenschutzrechtlichen Erfordernisse klar vermittelt werden können.

In der Bedarfsanpassung werden basierend auf der Erfahrung des externen DSB die FTE für Betroffene (sowohl bzgl. beschäftigter Personen als auch von Patienten) auf 0,05 reduziert, der Aufwand für das IT-System ebenfalls auf 0,05 FTE. Damit sieht die angepasste Aufwandabschätzung wie folgt aus:

	Anzahl	Anzahl FTE	FTE (gesamt)
Anzahl beschäftigter Personen	6	0,1	0,05
Anzahl Organisationseinheiten	1	0,1	
Anzahl Patienten/ Kunden pro Jahr	2.000	0,1	
IT System	1	0,2	0,05
Forschung	0	0,0	0,0
		Gesamt:	0,1

Damit reduziert sich für die Beispielpraxis der Arbeitsaufwand zur Erfüllung der datenschutzrechtlichen Anforderungen durch den Einsatz eines externen Datenschutzbeauftragten um 0,05 FTE auf etwa 0,1 FTE.

2. Krankenhaus

Ein Schwerpunktkrankenhaus hat 600 Betten, davon insgesamt 32 Intensivbetten. Neben den Fachrichtungen Chirurgie und Innere Medizin umfasst das Versorgungsangebot auch die Fachrichtungen Gynäkologie und Geburtshilfe, Augenheilkunde und Orthopädie. An nicht bettenführenden Abteilungen werden Apotheke, Anästhesie, Laboratoriumsmedizin und Radiologie geführt. Jährlich werden im Krankenhaus etwa 22.000 Fälle versorgt. Im Krankenhaus arbeiten 1.395 Beschäftigte, davon 197 im ärztlichen Dienst, 1198 im nichtärztlichen Dienst. 21 Beschäftigte sind im technischen Dienst eingesetzt, 4 davon bilden die IT-Abteilung, welche die Betreuung der eingesetzten informations- und kommunikationstechnischen Systeme („IKT-Systeme“) gewährleisten.

Entsprechend obiger Empfehlung resultiert daraus:

	Anzahl	Anzahl FTE		FTE (gesamt)
Anzahl beschäftigter Personen	1.395	0,1	0,3	1,2
Anzahl Organisationseinheiten: 1. Verwaltung inkl. HR 2. IT-Abteilung 3. Medizintechnik 4. Chirurgie 5. Innere Medizin 6. Gynäkologie und Geburtshilfe 7. Augenheilkunde 8. Orthopädie 9. Apotheke 10. Anästhesie 11. Laboratoriumsmedizin 12. Radiologie	12	0,1	1,2	
Anzahl Patienten/ Kunden pro Jahr	22.000		0,1	2,2
Anpassung bestehender Workflows sowie Entwicklung neuer Arbeitsabläufe			0,1	0,1
IT System 1) SAP (Verwaltung inkl. HR und Einkauf) 2) KIS 3) PACS 4) LIS 5) Apotheke	5		0,2	1,0
Forschung	0		0,0	0,0
			Gesamt:	4,5

Diese 4,4 FTE werden jetzt entsprechend dem Bedarf angepasst:

Kriterien	Bewertung
Betroffenenaufwand	Gering, aber steigend
Individuelle Bearbeitungssituation	Überwiegend standardisiert, IT-Systeme erfordern immer wieder Anpassungen, da seitens medizinischer Abteilungen immer wieder Bedarf an individueller Dokumentation angemeldet wird
Unternehmensorganisation	Festgelegte Arbeitsabläufe, einzelne Abteilungen (Radiologie, Gynäkologie) sind ISO 9001 zertifiziert mit Verfahrens- und Arbeitsanweisungen

In der Bedarfsanpassung werden basierend auf den Erfahrungen des Krankenhausbetreibers die FTE für Betroffene von 2,2 auf 1,0 reduziert. Auf Grund der regelmäßig erforderlichen Nachfragen der IT-Abteilung hinsichtlich datenschutzrechtlicher Einschätzung bzgl. zu erstellender Auswertungen/ Statistiken für die medizinischen Fachabteilungen wie auch der Krankenhausverwaltung wurde der Bedarf innerhalb der IT-Abteilung auf 0,3 FTE erhöht.

Daraus resultiert für das Beispielkrankenhaus ein Arbeitsaufwand zur Erfüllung der datenschutzrechtlichen Anforderungen von etwa 3,4 FTE.

3. Universitätsklinikum

Das Universitätsklinikum betreut als Krankenhaus der Maximalversorgung alle medizinischen Fachrichtungen. Es hat 38 medizinische Kliniken, weiterhin 23 Institute (die 21 vorklinischen Institute

zählen rechtlich zur Universität und sind daher datenschutzrechtlich nicht zur Uniklinik gehörend zu betrachten) und 22 medizinische Zentren. In der Verwaltung existieren 5 Stabsstellen, die datenschutzrechtlich zu berücksichtigen sind, desgleichen 12 Geschäftsbereiche, zu denen auch die IT-Abteilung, Controlling und Medizintechnik gehören. Weiterhin gibt es 7 zentrale Bereiche wie beispielsweise Apotheke oder Zentrallabor.

Die 11.000 Beschäftigten des Universitätsklinikums versorgen pro Jahr etwa 60.000 stationäre Patienten sowie rund 500.000 ambulante Behandlungen; erfahrungsgemäß erfolgen durch ambulante Patienten so gut wie keine Betroffenenanfragen, so dass als Richtwert 80.000 Patienten für die Berechnung des Arbeitsaufwandes betrachtet werden. Im Universitätsklinikum wird eine Vielzahl von IT-Systemen eingesetzt, da viele medizinische Kliniken und Zentren ergänzend zum Krankenhaus-Informations-System (KIS) noch spezielle Software benötigen wie beispielsweise in den onkologischen Kliniken spezielle Dokumentationssoftware. Nahezu alle medizinischen Kliniken sind sehr aktiv in der medizinischen Forschung, so dass im Universitätsklinikum jährlich etwa 120 Forschungsprojekte durchgeführt werden, darunter mindestens 70 Projekte im Rahmen von Kooperationen mit externen Partnern.

Entsprechend obiger Empfehlung resultiert daraus:

	Anzahl	Anzahl FTE		FTE (gesamt)
Anzahl beschäftigter Personen	11.000	0,1/500	2,2	10,7
Anzahl Organisationseinheiten: – 38 medizinische Kliniken – 23 Institute – 22 medizinische Zentren – 5 Stabsstellen – 12 Geschäftsbereiche – 7 zentrale Bereiche	107	0,1	10,7	
Anzahl Patienten/ Kunden pro Jahr	80.000		0,1/1.000	8,0
Anpassung bestehender Workflows sowie Entwicklung neuer Arbeitsabläufe			0,1	0,1
IT System – SAP (Verwaltung inkl. HR und Einkauf) – 2 x PACS – KIS – 5 x Laborsoftware – 5 techn. Systeme wie Telefonanlage – 2 x Diktatsoftware – 24 x Spezialsoftware für Kliniken – 1 x Apotheke – 1 x Anästhesie-Management-System – 1 x Kommunikationsserver – 1 x Patientendatenmanagementsystem – 6 x Ambulanzsoftware	50		0,2	10,0
Forschung (Weiterentwicklung PACS)	90		0,1	9,0
			Gesamt:	37,8

Diese 37,7 FTE werden jetzt entsprechend dem Bedarf angepasst:

Kriterien	Bewertung
Betroffenenaufwand	Mäßig, aber steigend
Individuelle Bearbeitungssituation	In der jeweiligen Klinik überwiegend standardisiert, aber von Klinik zu Klinik bzw. Zentrum nicht einheitlich; IT-Systeme erfordern immer wieder Anpassungen, da seitens medizinischer Abteilungen immer wieder Bedarf an individueller Dokumentation angemeldet wird
Unternehmensorganisation	Überwiegend festgelegte Arbeitsabläufe, einzelne Abteilungen sind ISO 9001 zertifiziert mit Verfahrens- und Arbeitsanweisungen Aber bei internen QM-Audits wird regelmäßig festgestellt, dass innerhalb der medizinischen Versorgung häufiger von den Vorgaben abgewichen wird.
Prozessentwicklung/-anpassung	Prozesse müssen in verschiedenen medizinischen Einrichtungen, u.a. bedingt durch die Entwicklung der medizinischen Versorgung, häufiger dem Stand der Wissenschaft angepasst werden. Daher ist hier eine größere Unterstützungsleistung erforderlich.

In der Bedarfsanpassung werden basierend auf den Erfahrungen des Krankenhausbetreibers die FTE für Betreuung der Beschäftigten und der Organisationseinheiten auf 5,2 FTE reduziert sowie hinsichtlich der Bearbeitung von Patientenanfragen auf 2,4 FTE. Die Erfahrungen innerhalb der IT-Abteilung ergibt, dass überwiegend keine Dokumentation hinsichtlich innerhalb der OH KIS geforderten Konzepte wie beispielsweise Lösch- oder Archivierungskonzept existierten. Für die Erstellung dieser Konzepte sollen externe Berater eingestellt werden, für die tägliche Routine glaubt man mit 4 FTE auszukommen. Hinsichtlich der Beratung bei Forschungsprojekten sollen 2 FTE eingesetzt werden und gerade bei Forschung mit externen Partnern finanzielle Mittel für die Hinzuziehung externer Datenschutzberater berücksichtigt werden. Auf Grund des höheren Bedarfs bei der Anpassung bestehender Workflows sowie Entwicklung neuer Arbeitsabläufe in den medizinischen Bereichen wird hier mit einem höheren Bedarf gerechnet, so dass 0,2 FTE eingeplant werden.

Daraus resultiert für das Universitätsklinikum ein Arbeitsaufwand zur Erfüllung der datenschutzrechtlichen Anforderungen von etwa 13,6 FTE, wie nachfolgender Tabelle entnommen werden kann:

	Anzahl	Anzahl FTE		FTE (gesamt)	Bedarfs-anpassung
Anzahl beschäftigter Personen	11.000	0,1/500	2,2	10,7	5,2
Anzahl Organisationseinheiten: – 38 medizinische Kliniken – 23 Institute – 22 medizinische Zentren – 5 Stabsstellen – 12 Geschäftsbereiche – 7 zentrale Bereiche	107	0,1	10,7		
Anzahl Patienten/ Kunden pro Jahr	80.000	0,1/1.000		8,0	2,4
Anpassung bestehender Workflows sowie				0,1	0,2

	Anzahl	Anzahl FTE	FTE (gesamt)	Bedarfs-anpassung
Entwicklung neuer Arbeitsabläufe				
IT System – SAP (Verwaltung inkl. HR und Einkauf) – 2 x PACS – KIS – 5 x Laborsoftware – 5 techn. Systeme wie Telefonanlage – 2 x Diktatsoftware – 24 x Spezialsoftware für Kliniken – 1 x Apotheke – 1 x Anästhesie-Management-System – 1 x Kommunikationsserver – 1 x PDMS – 6 x Ambulanzsoftware	50	0,2	10,0	4,0
Forschung (Weiterentwicklung PACS)	90	0,1	9,0	2,0
			Gesamt:	13,8

Die Reduzierung soll kritisch beobachtet und im Bedarfsfall im Verlauf der nächsten 2-3 Jahre eine personelle Anpassung entsprechend des festgestellten Bedarfs erfolgen.

4. PACS-Hersteller

Ein Hersteller eines Picture Archiving and Communication System (PACS) für radiologische Leistungserbringer sowohl im niedergelassenen wie auch im stationären Umfeld hat in Deutschland 145 niedergelassene (=radiologische Arztpraxen) sowie 285 stationäre Kunden (= Krankenhäuser) und beschäftigt 245 Personen.

Entsprechend obiger Empfehlung resultiert daraus:

	Anzahl	Anzahl FTE		FTE (gesamt)
Anzahl beschäftigter Personen	200	0,1	0,1	0,4
Anzahl Organisationseinheiten: 1. Verwaltung inkl. HR 2. IT-Abteilung 3. Softwareentwicklung 4. Vertrieb	4	0,1	0,4	
Anzahl Patienten/ Kunden pro Jahr	530		0,1	0,1
Akquisegespräche			0,1	0,1
Berücksichtigung Datenschutzanforderung bei der Entwicklung von IT-Systemen			0,1	0,1
IT System 1) SAP (Verwaltung inkl. HR und Einkauf) 2) PACS (Testumgebung) 3) Entwicklungsumgebung 4) PACS (Hostingbetrieb) für Kunden	4		0,2	0,8
Forschung (Weiterentwicklung PACS)	1		0,1	0,1
			Gesamt:	1,6

Diese 4,4 FTE werden jetzt entsprechend dem Bedarf angepasst:

Kriterien	Bewertung
Betroffenenaufwand (=Nachfragen Kunden)	Gering, aber steigend
Individuelle Bearbeitungssituation	Überwiegend standardisiert, Firma ist nach ISO 9001 zertifiziert, Rechenzentrum zertifiziert nach ISO 27001; eigene Verarbeitung nur Beschäftigtendaten; Patientendaten von Kunden werden im Rahmen von Verträgen zur Auftragsverarbeitung verarbeitet
Unternehmensorganisation	Festgelegte Arbeitsabläufe, Entsprechend ISO 9001 existieren Verfahrens- und Arbeitsanweisungen

In der Bedarfsanpassung werden basierend auf den Erfahrungen des Herstellers die FTE für Betroffene bzw. Betreuung der Organisationseinheiten auf 0,3 reduziert, da Verwaltung und die eigene IT-Abteilung mit einem gemeinsamen Ansprechpartner agieren können. Gerade in den letzten zwei Jahren zeigte sich aber, dass Kunden verstärkt Diskussionsbedarf hinsichtlich des Datenschutzes haben, so dass bei Kundengesprächen ein Bedarf von 0,2 FTE festgelegt wurde. Die Personalverwaltung erfolgt durch einen externen Dienstleister, welcher auch entsprechende datenschutzrechtliche Fragen aus dem HR-Bereich im Rahmen seiner Dienstleistung erbringt. Die datenschutzrechtlichen Fragen im Bereich der IT-Abteilung, Softwareentwicklung und Vertrieb basieren i.d.R. darauf, wer auf welche firmeninternen Daten mit welchem IT-System zugreifen darf, d.h. einzig die IT-Abteilung benötigt hier Unterstützung bei Fragen aus dem Datenschutzumfeld, so dass die Anzahl FTE reduziert werden können. Allerdings wird gerade das Hostingangebot in Richtung Cloud-Services erweitert, was einen erhöhten Bedarf verursacht. Der Bedarf für diesen Bereich wird daher mit 0,4 festgelegt. Bei der Weiterentwicklung des PACS werden immer wieder Kundendaten (DICOM-Daten) benötigt, allerdings wird dies direkt bei den Kundengesprächen – idealerweise sogar schon in den Akquisegesprächen – besprochen, so dass aus dem Forschungsbereich kein Bedarf besteht.

Somit zeigt sich nach der Bedarfsanpassung das folgende Bild:

	Anzahl	Anzahl FTE		FTE (gesamt)	Bedarfs-anpassung
Anzahl beschäftigter Personen	200	0,1	0,1	0,4	0,3
Anzahl Organisationseinheiten: 1. Verwaltung inkl. HR 2. IT-Abteilung 3. Softwareentwicklung 4. Vertrieb	4	0,1	0,4		
Anzahl Patienten/ Kunden pro Jahr	530		0,1	0,1	0,2
Akquisegespräche			0,1	0,1	0,1
Berücksichtigung Datenschutzanforderung bei der Entwicklung von IT-Systemen				0,1	0,1
IT System 1) SAP (Verwaltung inkl. HR und Einkauf) 2) PACS (Testumgebung) 3) Entwicklungsumgebung 4) PACS (Hostingbetrieb) für Kunden	4		0,2	0,8	0,4
Forschung (Weiterentwicklung PACS)	1		0,1	0,1	0,0
				Gesamt:	1,1

Der Arbeitsaufwand zur Erfüllung der datenschutzrechtlichen Pflichten beträgt in diesem Beispiel somit 1,1 FTE.

5. Hersteller mehrerer IT-Systeme für das Gesundheitswesen

Ein Hersteller bietet verschiedene IT-Systeme für Leistungserbringer in der medizinischen Versorgung an: ein KIS, welches auch in MVZ Verwendung findet, ein Archivsystem sowie ein Webportal für die Patientenanbindung. Der Hersteller hat in Deutschland 585 Krankenhaus-Kunden sowie 85 Kunden aus der ambulanten Versorgung. 345 beschäftigte Personen arbeiten für ihn.

Entsprechend obiger Empfehlung resultiert daraus:

	Anzahl	Anzahl FTE		FTE (gesamt)
Anzahl beschäftigter Personen	345	0,1	0,1	0,6
Anzahl Organisationseinheiten: 1. Verwaltung inkl. HR 2. IT-Abteilung 3. Softwareentwicklung für 3 Produkte 4. Vertrieb	6	0,1	0,6	
Anzahl Patienten/ Kunden pro Jahr	670		0,1	0,1
Akquisegespräche			0,1	0,1
Berücksichtigung Datenschutzanforderung bei der Entwicklung von IT-Systemen			0,1	0,1
IT System 1) SAP (Verwaltung inkl. HR und Einkauf) 2) 6 x Testumgebungen 3) 3 x Entwicklungsumgebung 4) Hostingbetrieb für Kunden	11		0,2	2,2
Forschung (Weiterentwicklung IT-Systeme)	3		0,1	0,3
			Gesamt:	3,3

In der Bedarfsanpassung werden basierend auf den Erfahrungen des Herstellers die FTE für Beratung hinsichtlich Beschäftigter bzw. den internen Organisationseinheiten auf 0,3 reduziert. Gerade in den letzten zwei Jahren zeigte sich, dass Kunden verstärkt Diskussionsbedarf hinsichtlich des Datenschutzes bei den Produkten haben und auch in Ausschreibungen verstärkt auf Themen des Datenschutzes eingegangen wird. Daher wurde bzgl. Kundenkontakte ein Bedarf von 0,2 FTE festgelegt. Sowohl für die Entwicklungsumgebung wie auch bei den Testumgebungen wird nicht mit personenbezogenen Daten gearbeitet, so dass hier kein Bedarf gesehen wird. Datenschutzrechtliche Fragen beim Hostingbetrieb werden in der Regel während der Akquisegespräche geführt. Hinsichtlich der eingesetzten IT-Systeme wird daher nur ein Bedarf von etwa 0,3 FTE gesehen. Im Bereich der Weiterentwicklung werden zwar Kundendaten (= Patientendaten) genutzt, jedoch wird die Nutzung in der Regel bei den Akquisegesprächen vereinbart. Dennoch ergeben sich regelmäßig Nachfragen, ob Daten ggf. auch systemübergreifend, d.h. beispielsweise Daten von KIS-Kunden für die Weiterentwicklung des Archivsystems, genutzt werden können oder in wie weit Zweckanpassungen statthaft sind. Daher wird hier ein Bedarf an 0,1 FTE gesehen. Bedingt durch die drei angebotenen IT-Systeme, die z.T. sehr unterschiedliche Aspekte aus Datenschutzsicht (z.B. langfristige Speicherung im Archivsystem inkl. ggf. erforderliche Krypto-Konzepte für elektronische Signaturen vs. eher kurzfristige Speicherung in Dokumentationssystemen) wird mit einem höheren Beratungsbedarf bei der Weiterentwicklung der IT-Systeme gerechnet, daher werden hier 0,2 FTE vorgesehen.

Aus der Bedarfsanpassung resultiert somit:

	Anzahl	Anzahl FTE		FTE (gesamt)	Bedarfs-anpassung
Anzahl beschäftigter Personen	345	0,1	0,1	0,6	0,3
Anzahl Organisationseinheiten: 1. Verwaltung inkl. HR 2. IT-Abteilung 3. Softwareentwicklung für 3 Produkte 4. Vertrieb	6	0,1	0,6		
Anzahl Patienten/ Kunden pro Jahr	670		0,1	0,1	0,1
Akquisegespräche			0,1	0,1	0,2
Berücksichtigung Datenschutzanforderung bei der Entwicklung von IT-Systemen				0,1	0,2
IT System 1) SAP (Verwaltung inkl. HR und Einkauf) 2) 6 x Testumgebungen 3) 3 x Entwicklungsumgebung 4) Hostingbetrieb für Kunden	11		0,2	2,2	0,3
Forschung (Weiterentwicklung IT-Systeme)	3		0,1	0,3	0,1
				Gesamt:	1,2

Der Arbeitsaufwand zur Erfüllung der datenschutzrechtlichen Pflichten beträgt in diesem Beispiel somit 1,2 FTE.

Beispiele für Aufwand, der aus den datenschutzrechtlichen Anforderungen resultiert

Dokumentation der Verarbeitungstätigkeiten

Die DS-GVO beinhaltet dabei an den verschiedensten Stellen Dokumentationspflichten. So z. B.

- Nachweis der grundlegenden Anforderungen (Art. 5 DS-GVO), d.h. Nachweis und dementsprechend Dokumentation bzgl.
  - der Einhaltung von Rechtmäßigkeit, Transparenz (inkl. Drittland-Verarbeitung),
  - Wer ist der Verantwortlicher
  - Zweck(e) / Zweckbindung
  - Datenminimierung
  - Richtigkeit
  - Betroffene (Kategorien)
  - Daten (Kategorien)
  - Empfänger (Kategorien)
  - Löschfristen / Speicherbegrenzung
  - Integrität, Vertraulichkeit
- Einwilligung (Art. 7 DS-GVO): „[…] muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat“; dies beinhaltet den Nachweis
  - Freiwilligkeit
  - Für den bestimmten Fall (= Zweckbindung)
  - Informiertheit (insbesondere in Kenntnis der Sachlage, z. B. auch Berücksichtigung Artt. 12, 13,14 DS-GVO)
  - unmissverständlich abgegebene Willensbekundung (in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung)
  - Ausdrückliche Willenserklärung
- Informationspflichten (Artt. 13, 14 DS-GVO)
  Nachweis, dass der Verantwortliche seinen Dokumentationspflichten nachgekommen ist. D. h. Prozess dokumentieren, Prozess regelmäßig prüfen, Prüfung und Ergebnis Prüfung dokumentieren
- Sicherheit der Verarbeitung: Nachweis der Erfüllung der Anforderungen der Artt. 25,35 und 32 DS-GVO durch entsprechende Dokumentation; insbesondere gehören Audis und entsprechende Prüfberichte entsprechend Art. 32 Abs. 1 lit. d DS-GVO dazu.
- Auftragsverarbeitung (Art. 28 DS-GVO): Verantwortlicher muss nachweisen
  - Kriterien für die Auswahl des Auftragsverarbeiters
  - Einhaltung Vorgaben Art. 32 DS-GVO (Sicherheit Verarbeitung)
  - Gewährleistung der Rechte der betroffenen Person
  - Durchführung und das Ergebnis einer Vor-Ort-Prüfung (wenn durchgeführt)
  - Vertragsabschluss inkl. der Einhaltung der inhaltlichen Vorgaben aus Art. 28 Abs. 3 S. 2 lit. a-h DS-GVO
  - Einhaltung vertraglich vereinbarten Pflichten
- Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DS-GVO), wonach dokumentiert werden muss
  - Name/Kontaktdaten Verantwortlicher, wenn vorhanden auch Datenschutzbeauftragter
  - Zweck(e)
  - Betroffene (Kategorien)
  - Daten (Kategorien)
  - Empfänger (Kategorien)
  - Löschfristen

- Drittland-Verarbeitung
- Geplante und ergriffene technisch organisatorische Maßnahmen

- Verletzungen des Schutzes personenbezogener Daten („Datenpannen"); die Dokumentation der Datenpannen muss beinhalten
  - Verantwortlicher
  - Name/Kontaktdaten Datenschutzbeauftragter oder sonstige Anlaufstelle
  - Zweck(e)
  - Betroffene (Kategorien), ungefähre Anzahl betroffener Personen
  - Daten (Kategorien)
  - Beschreibung der Art der Verletzung des Schutzes
  - Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten (Risikobetrachtung)
  - Meldepflicht
  - Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen
- Dokumentation bei Drittlandverarbeitung
  - Art. 44 DS-GVO: „[…] ist nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter die in diesem Kapitel niedergelegten Bedingungen einhalten und auch die sonstigen Bestimmungen dieser Verordnung eingehalten werden; […]“
    → Insbesondere gilt auch die Nachweispflicht aus Art. 5 DS-GVO
  - Art. 44 DS-GVO: „Alle Bestimmungen dieses Kapitels sind anzuwenden, um sicherzustellen, dass das durch diese Verordnung gewährleistete Schutzniveau für natürliche Personen nicht untergraben wird.“
    → Es ist ein Nachweis erforderlich, wie das Schutzniveau erhalten bleibt

Etablierung eines Prozesses zur Gewährleistung von Betroffenenrechten

Es muss ein Prozess eingeführt und gelebt werden, welcher eine den datenschutzrechtlichen Anforderungen entsprechende Bearbeitung von Anfragen betroffener Personen gewährleistet. Dazu gehört:

1. **Annahme einer Anfrage.** Dies erfordert
   - Darstellung, wo Anfragen im Unternehmen eingehen können
   - Identifizierung der „Entry-Points“ wie Telefonzentrale, Kontaktformular Internet, E-Mail-Kommunikationsadressen des Unternehmens, z. B. Impressum, …
   - Schulung der die Anfragen entgegennehmenden Personen
   - Welche Informationen müssen erfragt werden?
   - An wen wird die Anfrage weitergeleitet?
2. **Umgang mit einer Anfrage**

   2.1 Eingangsprüfung
   - Überprüfung, ob es sich tatsächlich um eine datenschutzrechtliche Anfrage handelt
   - Erfassung der Anfrage in einem geeigneten Dokumentationssystem
   - Überprüfung, worum es sich handelt (Auskunftsersuchen, Korrekturanfrage, Löschungsersuchen, …)
   - Versendung einer Eingangsbestätigung an den Antragssteller
   - Prüfung der Identität des Antragsstellers
   - Prüfung, ob
     - unbegründete Antrag i.S.v. Art. 12 Abs. 5 DS-GVO
     - exzessiven Anträgen einer betroffenen Person vorliegen
   - Kann Antrag nicht sofort bearbeitet werden: Information betroffene Person ohne Verzögerung

   2.2 Inhaltliche Prüfung

- Prüfung, ob personenbezogene Daten der betroffenen Person verarbeitet werden/wurden
- Wenn keine Daten vorhanden sind: Negativmitteilung an den Betroffenen versenden !
- Wenn Daten vorhanden sind: Abarbeiten

2.3 Beantwortung

- Auskunftsersuchen:
  - Zusammenstellung
  - Unverzügliche Beantwortung
    a) Innerhalb eines Monats
    b) Wenn auf Grund Komplexität nicht innerhalb von einem Monat möglich
       - Innerhalb von 3 Monaten nach Antragstellung zwingend umzusetzen
       - Person muss innerhalb der ersten Monats über Verzögerung informiert werden
  - Beachten: Elektronische Antragstellung = Unterrichtung auch elektronisch, wenn betroffene Person nichts anderes verlangt
- Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit
  - Weiterleitung an entsprechende Stellen zwecks Umsetzung
  - Sobald Umsetzung erfolgt → Information betroffene Person (siehe Auskunftsersuchen)
  - Widerspruch Verarbeitung, Widerruf einer Einwilligung
  - Information der Stelle, welche
    a) die Verarbeitung (z. B. Forschung) durchführt
    b) die Einwilligung erhob
  - Verarbeitung einstellen
  - Prüfen, ob Daten gelöscht werden müssen (Art. 17 Abs. 1 lit. b, c DS-GVO)
  - Information betroffene Person über erfolgte Maßnahmen, ggf. auch über Löschung (siehe Auskunftsersuchen)

Dabei fallen natürlich bei jedem Bearbeitungsschritt diverse zu dokumentierende Elemente ein, z. B. getroffene Entscheidungen sowie ggf. deren Begründung.

Ein guter Nachweis besteht auch darin, für das jeweilige Unternehmen geltende Vorgaben in entsprechenden Konzepten festzuhalten, so dass einerseits Beschäftigte die Vorgaben kennen und bei Bedarf nachlesen können, andererseits gegenüber Datenschutz-Aufsichtsbehörden getroffene Vorgaben gegenüber nachgewiesen werden können. Zu den gängigen Konzepten, die im Umfeld von datenschutzrechtlichen Anforderungen seitens Aufsichtsbehörden immer wieder angefragt werden, gehören insbesondere

- Datenschutzkonzept und/oder Datenschutzrichtlinie
- Berechtigungskonzept (Rollen- und Rechtekonzept)
- Archivierungskonzept und/oder Archivordnung
- Protokollierungskonzept
- Löschkonzept
- IT-Sicherheitskonzept
- Notfall-Handbuch

Der Umfang der jeweiligen Konzepte ist dabei natürlich vom Unternehmen selbst abhängig. Eine Arztpraxis mit 4 Personen benötigt beispielsweise ein weniger umfangreiches Datenschutzkonzept wie in Krankenhaus mit 2000 Beschäftigten. Bei einem IT-Unternehmen, welches IT-Systeme für das Gesundheitswesen herstellt, stehen wiederum andere Aspekte im Vordergrund als bei Leistungserbringern.

Schulung/Unterweisung der Beschäftigten

Beschäftigte müssen bzgl. der Einhaltung der aus dem Datenschutzrecht resultierenden Anforderungen geschult werden. Zu den zu schulenden Themen gehören insbesondere

- Datenschutz
  - Sachlicher/Räumlicher Anwendungsbereich der verschiedenen Datenschutzgesetze
  - Rechtmäßigkeit der Verarbeitung
  - Betroffenenrechte
  - Datengeheimnis
  - Verzeichnis der Verarbeitungstätigkeiten
  - Sicherheit der Verarbeitung inkl. Meldepflichten
- IT-Sicherheit
  - Theoretische Wissensvermittlung bzgl. grundlegender Fragen der IT-Sicherheit, z.B. bzgl. Erstellung und Gestaltung von Passwörtern bzw. Passphrasen
  - Sicherheit beim Umgang mit Kommunikationsmitteln wie beispielsweise E-Mail, Messenger, Fax oder auch Post
  - IT-Sicherheit beim Umgang mit den medizinischen Informationssystemen
- Erkennen und melden von Vorkommnissen

Grundsätzlich gehört auch hierzu, dass ein entsprechender Nachweis zu erbringen ist. D.h. auch die Durchführung von Schulungen sowie die Teilnehmer inkl. Referent sind zu dokumentieren.

Abkürzungen

Abs.	Absatz
Art.	Artikel
Artt.	Artikel (Mehrzahl)
BDSG	Bundesdatenschutzgesetz
BvD	Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e. V.
bvitg	Bundesverband Gesundheits-IT e. V.
DSFA	Datenschutz-Folgenabschätzung
DS-GVO	Datenschutz-Grundverordnung
FTE	full time equivalent = Vollbeschäftigtenäquivalent
GDD	Gesellschaft für Datenschutz und Datensicherheit e. V.
GMDS	Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e. V.
i. S. d.	im Sinne des, im Senne der
i. V. m.	in Verbindung mit
ISO	International Organization for Standardization
IT	Informationstechnik, informationstechnisches…
Kap.	Kapitel
KIS	Krankenhaus-Informationssystem
MVZ	Medizinisches Versorgungszentrum
PACS	Picture Archiving and Communication System
PDMS	Patientendatenmanagementsystem
S.	Satz
TOM	technisch-organisatorische Maßnahmen