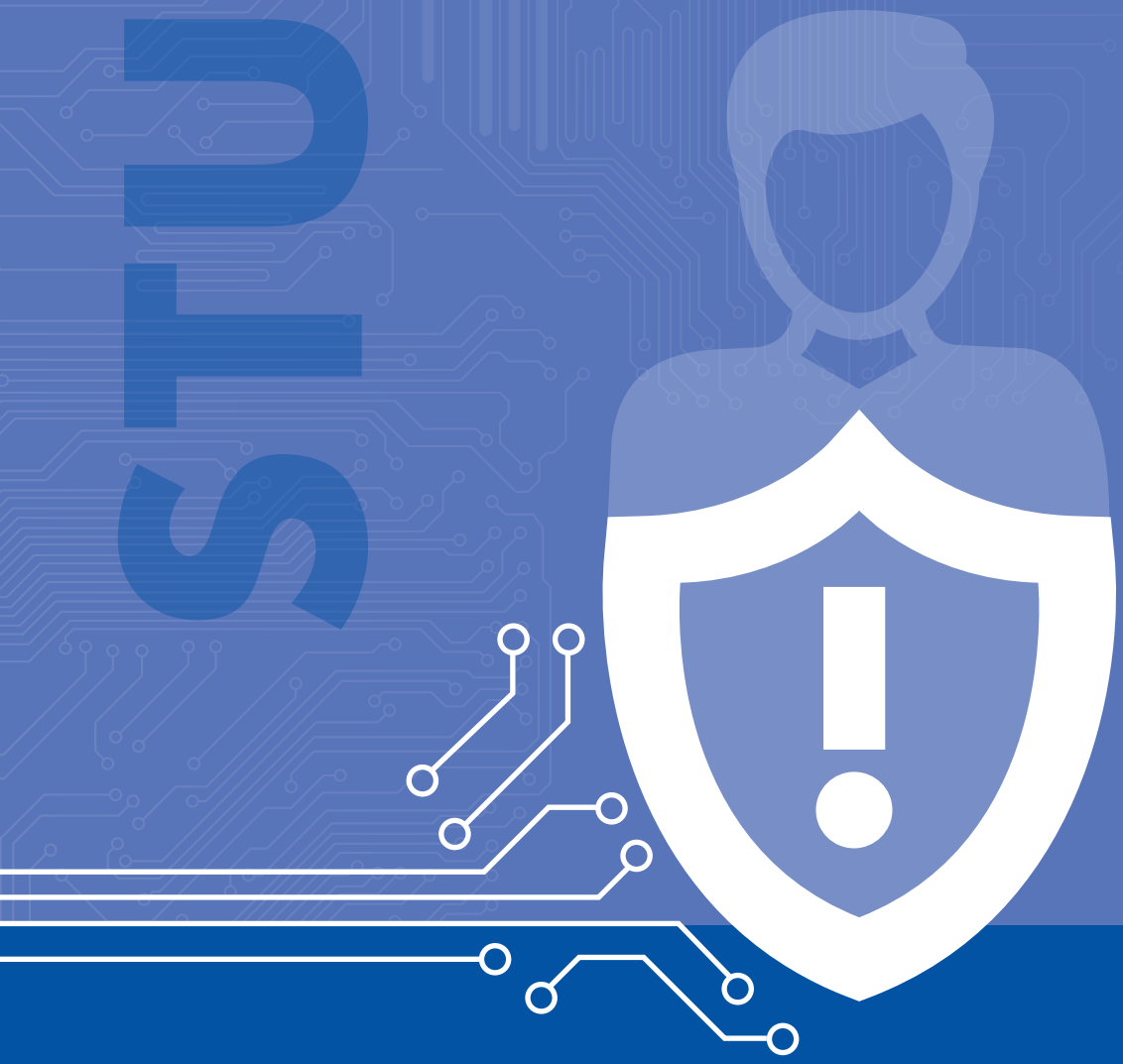
STUDIE

Datenschutz zwischen DSGVO und Digitalisierung

Wo stehen wir nach vier Jahren DSGVO?



CURACON

Inhalt

In Anlehnung an den Gesetzestext der Datenschutz-Grundverordnung und zugunsten einer leichteren Lesbarkeit beschränkt sich der Studientext auf das generische Maskulinum, wie beispielsweise „der Datenschutzbeauftragte". Natürlich beziehen sich die Angaben auch in dieser Form auf alle Geschlechter.

Vorwort

Liebe Leserin, lieber Leser,

gerade in der Gesundheits- und Sozialbranche, in der besonders schützenswerte Daten generiert und verarbeitet werden müssen, ist der Schutz der Daten von besonderer Bedeutung. Die formalen und administrativen Erfordernisse, die sich aus der DSGVO sowie den geltenden staatlichen und kirchlichen Datenschutzgesetzen ergeben, und die sich verändernden branchenspezifischen Rahmenbedingungen führen zu einer Komplexitätssteigerung sowie unvermeidlich zu einem steigenden Ressourceneinsatz. Besonders die Digitalisierungsdynamik, die auch nicht zuletzt durch die Pandemie beschleunigt wurde, birgt weitere Herausforderungen, die datenschutzrechtlich zu lösen sind.
Das Ziel der Studie ist es, die Komplexität beim Thema Datenschutz in den genannten Branchen abzubilden und sowohl den alten als auch neuen Herausforderungen Rechnung zu tragen. Hierbei wird in einzelnen Bereichen auf die Erkenntnisse der Studie von 2018 eingegangen und – sofern möglich – ein Vergleich gezogen.
Im ersten Teil beschäftigt sich die Studie mit der Rolle des Datenschutzbeauftragten, seinen zeitlichen Ressourcen sowie der Frage, wie häufig Datenschutzbeauftragte sich fort- und weiterbilden. Ferner wird betrachtet, wie Schulungen, insbesondere mit Blick auf die Pandemie, durchgeführt werden. Beleuchtet wird zudem die Art und Weise, wie Schulungen durchgeführt und welche Inhalte vermittelt werden. Schließlich widmet sich dieser erste Teil den Begehungen und dem Umgang mit den dort gewonnenen Erkenntnissen.
Im zweiten Teil der Studie wird die Umsetzung datenschutzrechtlicher Standards betrachtet. Hierbei wird insbesondere auf regelmäßige Risikoeinschätzungen sowie die zugehörigen technischen und organisatorischen Maßnahmen eingegangen. Die Studie gibt zudem Hinweise darauf, welche datenschutzrechtlichen Anforderungen im Alltag die größten Schwierigkeiten verursachen, für welche Maßnahmen Prozesse implementiert wurden, die die Umsetzung gewährleisten, und welche Begleitumstände die Umsetzung von Datenschutzmaßnahmen erschweren. Schließlich wird der Frage nachgegangen, ob die in der Curacon-Datenschutzstudie 2018 erwartete Verschärfung eingetreten ist und welche Gründe gegebenenfalls hierfür ausschlaggebend sind.
Mit Inkrafttreten der DSGVO beziehungsweise der konfessionellen Gesetze wurde der Meldung einer Verletzung der Rechte und Freiheiten natürlicher Personen eine stärkere Gewichtung zugewiesen. Ebenso wurde die Rolle der Aufsichtsbehörden gestärkt. Die Studie befasst sich daher im dritten Teil mit der Anzahl der gemeldeten beziehungsweise potenziellen Datenschutzverletzungen sowie den Reaktionen der Aufsichtsbehörden und den Erfahrungen der Einrichtungen mit diesen.
Der vierte und vorletzte Abschnitt der Studie befasst sich mit datenschutzrechtlichen Fragen, die im Kontext der Digitalisierung auftreten. Beleuchtet werden die Antreiber der Digitalisierung sowie die daraufhin entstehenden Hürden und Herausforderungen, die sich sowohl für die Unternehmen als auch für die Datenschutzbeauftragten ergeben.
Der letzte Abschnitt gibt einen Ausblick und diskutiert die Ergebnisse der Studie.

Wir bedanken uns herzlich bei allen Teilnehmer:innen der Studie. Ein ganz besonderer Dank gilt Leonie Michalak, die in unserem Research-Team maßgeblich zum Gelingen der Studie beigetragen hat.

Wir wünschen Ihnen eine erkenntnisreiche Lektüre!

Dr. Uwe Günther
Partner
Leiter Beratungsfelder Datenschutz und IT-Management
Geschäftsführer Sanovis GmbH

Johannes Mönter
Manager
Beratungsfeld Datenschutz

Stefan Strüwe
Partner
Leiter Beratungsfeld Datenschutz

DSGVO und Digitalisierung

Auf einen Blick

Datenschutzbeauftragte

98 % der Befragten gaben an, einen Datenschutzbeauftragten bei der zuständigen Aufsichtsbehörde gemeldet zu haben. Der Anteil interner bzw. externer Datenschutzbeauftragter ist ausgeglichen.

Lediglich 34 % der Datenschutzbeauftragten verfügen über ein definiertes Stundenkontingent zur Erfüllung ihrer Aufgaben als Datenschutzbeauftragter.

Zwei Drittel der Befragten erreichen über 60% der Beschäftigten ihres Unternehmens durch Schulungen. Die Schulungen beinhalten zumeist die gesetzlichen Grundlagen des Datenschutzes, die berufliche Schweigepflicht sowie die Besonderheiten des Datenschutzes im Tätigkeitsfeld der Beschäftigten etc.

Umsetzung datenschutzrechtlicher Standards

Herausforderungen in der alltäglichen Umsetzung der Standards: Datenschutz-Folgenabschätzung, Auskunft gegenüber Angehörigen und die datenschutzkonforme Übermittlung personenbezogener Daten an Kooperationspartner.

45 % der Teilnehmenden empfinden, dass seit 2018 eine Verschärfung des Datenschutzes eingetreten ist. Die umfangreichen Informationspflichten und erhöhten Rechenschaftspflichten, aber auch die Datenschutz-Folgenabschätzung sind hierfür ursächlich.

Datenschutzaufsichtsbehörden

55 % der teilnehmenden Einrichtungen registrieren intern lediglich 1–5 Datenschutz-Vorfälle.

Die zuständigen Datenschutzaufsichtsbehörden reagierten nicht auf knapp 48 % der durch die Einrichtungen erfolgten datenschutzrechtlichen Eingaben.

Die Hälfte der Befragten machten bisher positive Erfahrungen mit den Datenschutzaufsichtsbehörden.

Datenschutz und Digitalisierung

Die COVID-19-Pandemie trieb die Digitalisierung in der Gesundheits- und Sozialwirtschaft an. Neben den Geschäftsführungen der befragten Einrichtungen zeigten besonders die Beschäftigten und Klienten Interesse am digitalen Ausbau.

Eine wesentliche Hürde bei der Einführung neuer digitaler Verfahren stellt die zeit- und ressourcenintensive Datenschutz-Folgenabschätzung dar.

Digitalisierungsdynamik im Zusammenhang mit der COVID-19-Pandemie: Das Vertrauen in den Datenschutz sinkt bei 40 % der Befragten. Grund dafür ist die steigende Komplexität.

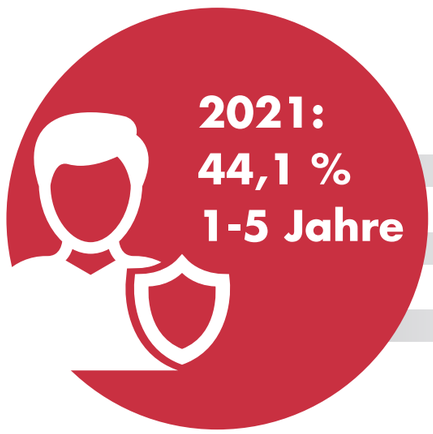
1. Datenschutzbeauftragte

Der erste Teil der Studie beleuchtet die Situation der betrieblichen Datenschutzbeauftragten. Dabei werden auch die Einflüsse der COVID-19-Pandemie sowie die Einflüsse der Digitalisierung auf die Arbeit der betrieblichen Datenschutzbeauftragten betrachtet.

Datenschutz erfolgreich verankert – 99 % verfügen über einen Datenschutzbeauftragten

Es hat sich mit Blick auf eine organisatorische Verankerung viel getan seit der Datenschutzgrundverordnung. Auf die Frage nach der Bestellung eines Datenschutzbeauftragten gaben 99 % der Befragten an, einen Datenschutzbeauftragten bei der zuständigen Aufsichtsbehörde gemeldet zu haben.
Der Anteil der Einrichtungen, die einen Datenschutzbeauftragten über eine interne bzw. externe Lösung bestellt haben, ist ausgeglichen. Eine interne Bestellung des Datenschutzbeauftragten liegt bei 56 % der Befragten vor; eine externe Bestellung bei 42 %. Zum Vergleich: Im Jahr 2018 lag der Prozentsatz der internen Bestellung bei bis zu 82%. Die externen Bestellungen lagen zwischen 18 % und 27 %. Daraus lässt sich schließen, dass externe Bestellungen aufgrund der wachsenden Komplexität zunehmen, um die erforderliche Expertise vorhalten zu können. Im Vergleich zur Studie 2018 lassen sich hier jedoch keine signifikanten Unterschiede hinsichtlich der Branchen oder Unternehmensgrößen erkennen.
Die verbleibenden ein Prozent der Befragten haben die Stelle weder besetzt noch soll die Stelle zukünftig durch eine interne oder externe Lösung besetzt werden. Ob in diesen Fällen der gesetzlichen Verpflichtung aufgrund von Ausnahmeregelungen nicht nachgekommen werden muss oder gegen die Verpflichtung zur Benennung eines Datenschutzbeauftragten verstoßen wird, lässt sich nicht mit Gewissheit sagen.

Seit wie vielen Jahren haben Sie einen Datenschutzbeauftragten in Ihrem Unternehmen? (in %)



Jahre	%
0	2,9
6 -10	26,5
11-15	10,3
16 -20	7,4
> 20	8,8

externe Bestellung
2021: 42 %
2018: ca. 20 %

interne Bestellung
2021: 56 %
2018: ca. 80 %

Im Rahmen der Frage, seit welchem Zeitpunkt ein Datenschutzbeauftragter in der Einrichtung bestellt wurde, ist hervorzuheben, dass lediglich 30 % der Einrichtungen bereits länger als 10 Jahre einen Datenschutzbeauftragten in der Einrichtung bestellt haben. Ca. 70 % der Befragten gaben an, erst in den letzten 10 Jahren einen Datenschutzbeauftragten bestellt zu haben. Die erhöhte Bestellungsquote von Datenschutzbeauftragten lässt annehmen, dass diese auf die strengeren Verpflichtungsvorschriften zur Bestellung von Datenschutzbeauftragten zurückzuführen ist. 44 % der Befragten gaben an, dass in den letzten ein bis fünf Jahren erstmalig ein Datenschutzbeauftragter in der Einrichtung bestellt wurde. Vermehrte Diskussionen im Rahmen der Datenschutzkonformität, beispielsweise hinsichtlich der Datenübermittlung in Drittstaaten, des Betreibens von Social-Media-Accounts oder der Nutzung von Messengern haben dazu beigetragen, ein verstärktes Verständnis für den Datenschutz in der Gesellschaft zu schaffen und zu etablieren.
Der Anteil der Einrichtungen, bei denen der Datenschutzbeauftragte das Amt als Vollzeit- (46 %) bzw. Teilzeitstelle (53 %) bekleidet, ist ausgeglichen. Hier lassen sich im Vergleich zur Studie von 2018 keine signifikanten Unterschiede hinsichtlich der Branche oder der Unternehmensgröße erkennen.

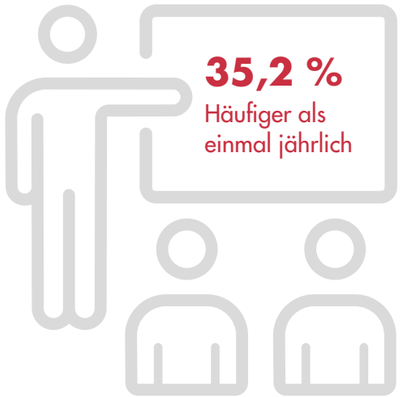
Allrounder – Datenschutzbeauftragte zumeist in mehreren Funktionen tätig

Bei der Abfrage der weiteren Tätigkeiten von Datenschutzbeauftragten fällt auf, dass diese neben der Tätigkeit im Datenschutz häufig weiteren Funktionen in den Einrichtungen nachkommen. Ausschließlich 22 % der Befragten führen die Tätigkeit des Datenschutzbeauftragten als Haupttätigkeit ohne Funktion in weiteren Abteilungen aus. Ein Großteil der Personen, die das Amt des Datenschutzbeauftragten bekleiden, ist zudem in den Abteilungen des Qualitätsmanagements (27 %) und in der Verwaltung (25 %) angesiedelt. Seltener bekleiden Personen aus der Stabsstelle Geschäftsführung/ Assistenz Geschäftsführung (14 %), Rechtsabteilung/Justiziar (8 %) und Rentner (3 %) das Amt des Datenschutzbeauftragten.
Bei Betrachtung der weiteren Funktionen, die Datenschutzbeauftragte in Einrichtungen ausführen, ist festzuhalten, dass ein Interessenkonflikt auf den ersten Blick weitestgehend ausgeschlossen werden kann. Insbesondere Personen aus Personal- oder IT-Abteilung wären aufgrund bestehender Interessenkonflikte ungeeignet. Interessenkonflikte entstehen dabei aufgrund von Zugriffsberechtigungen auf sensible Mitarbeiterdaten bzw. weitreichende Administratoren-Berechtigungen. Die Geschäftsführung selbst ist aufgrund von Interessenkonflikten ebenfalls ungeeignet für die Ausübung des Amtes.

50:50 – nur rund die Hälfte der Datenschutzbeauftragten wird regelmäßig geschult

Neben der Vermeidung eines Interessenkonflikts muss der/die Datenschutzbeauftragte die erforderliche Fachkunde vorweisen können, um das Amt nach den gesetzlichen Vorgaben ausführen zu können. Daher wurde im Rahmen der Studie bei den teilnehmenden Einrichtungen nachgefragt, in welcher Regelmäßigkeit die Datenschutzbeauftragten Zugang zu fachlichen Aus-, Fort- und Weiterbildungsmaßnahmen erhalten.
Annähernd die Hälfte der Befragten gibt an, dass sie mindestens einmal jährlich (14 %) oder häufiger als einmal jährlich (35 %) die Möglichkeit erhalten, an einer Fortbildungs- bzw. Weiterbildungsmaßnahme teilzunehmen, um die erforderliche fachliche Expertise auszuweiten. Bei 18 % der Befragten werden Weiterbildungsmaßnahmen unregelmäßig, je nach Bedarf angeordnet. Ausschließlich eine Ausbildungsmaßnahme zur Gewinnung der erforderlichen Fachkunde erhielten ca. 7 % der befragten Datenschutzbeauftragten.
4 % der Befragten gaben an, dass sie weder eine Ausbildungsmaßnahme bei Bestellung des Datenschutzbeauftragten noch eine Weiterbildungs- / Fortbildungsmaßnahme im weiteren Verlauf erhalten haben. In diesen Fällen ist davon auszugehen, dass die zuständigen Personen nicht über die erforderliche Fachkunde zur Erfüllung der Aufgaben des Datenschutzbeauftragten verfügen. Das Ausbleiben von regelmäßigen Fort- und Weiterbildungsmaßnahmen erhöht zudem das Risiko, dass Gesetzesänderungen, Rechtsprechungen und Stellungnahmen der Aufsichtsbehörden nicht wahrgenommen und umgesetzt werden. Das angesprochene Risiko gilt ebenfalls für die Datenschutzbeauftragten, die lediglich eine Ausbildungsmaßnahme erhalten, um die erforderliche Fachkenntnis zu erlangen.

An wie vielen Aus-/Fortbildungen und/oder Weiterbildungen hat der DSB zur Aufrechterhaltung/ Herstellung der erforderlichen Fachkunde teilgenommen? (in %)



7,0 %	Einmalig
14,1 %	Einmal jährlich
18,3 %	Unregelmäßig bzw. nach Bedarf
4,2 %	Bisher keine
21,1 %	k. A.

Rund ein Fünftel der Befragten (21 %) haben diese Frage nicht beantwortet.

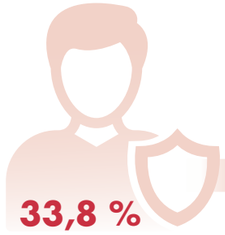
Zwei Drittel ohne Freistellung durch die Geschäftsführung

Die offizielle Freistellung ist aus arbeitsrechtlicher und steuerungstechnischer Sicht sinnvoll, um der Überlastung der betroffenen Personen effektiver entgegenwirken zu können. Insbesondere in Situationen, bei denen der Datenschutzbeauftragte eine weitere Funktion in einer anderen Abteilung innehat, besteht ein hohes Risiko für die Überlastung.
Lediglich 34 % der Befragten verfügen über ein definiertes Stundenkontingent zur Erfüllung der Aufgaben eines Datenschutzbeauftragten. Die Freigabe erfolgte dabei offiziell von der Geschäftsführung.
Jeweils 39 % der Datenschutzbeauftragten haben eine Freigabe für ein Stundenkontingent von 1–10 Stunden pro Woche bzw. 31–40 Stunden pro Woche. 21 % gaben an, dass dem Datenschutzbeauftragten ein Wochenkontingent von 11–20 Stunden zusteht.
Im Vergleich hierzu wurden im Rahmen der Studie die Datenschutzbeauftragten gefragt, wie viele Stunden tatsächlich durchschnittlich pro Woche aufgewendet werden, um den Aufgaben des Datenschutzbeauftragten nachzukommen. Im Vergleich zur Studie 2018 lassen sich hier keine signifikanten Unterschiede hinsichtlich der Branche oder der Unternehmensgröße erkennen.
29 % der befragten Datenschutzbeauftragten mit einer offiziellen Freistellung gaben an, dass pro Woche durchschnittlich 1–10 Stunden für den Bereich Datenschutz aufgewendet werden. 25 % dieser Befragten sagen, dass durchschnittlich 11–20 Stunden pro Woche für die Aufgaben des Datenschutzbeauftragten anfallen, 8 % wenden 21–30 Stunden pro Woche auf, knapp 30 % wenden 31–40 Stunden pro Woche auf und bei 8 % der Datenschutzbeauftragten entsteht ein Aufwand von durchschnittlich mehr als 40 Stunden pro Woche. Grob lässt sich damit festhalten, dass der Umfang der Freistellung und die tatsächlichen Aufwände im Einklang stehen.

66,2 % der DSB verfügen über keine offizielle Freistellung durch die Geschäftsführung

Seitens derer, die nicht über eine offizielle Freistellung verfügen, ergibt sich ein anderes Bild: Knapp 75 % und damit die deutliche Mehrheit der Datenschutzbeauftragten ohne Freistellung investieren wöchentlich 1-10 Stunden. 19 % wiederum investieren mehr als 11 Stunden – jedoch maximal 40 Stunden – in der Woche. 6 % gaben an, dass kein spürbarer Aufwand (entspricht 0 Stunden pro Woche) hinsichtlich der Aufgabenerfüllung als Datenschutzbeauftragte anfällt. In diesen Fällen kann davon ausgegangen werden, dass den gesetzlichen Verpflichtungen nicht ausreichend nachgekommen wird. Insbesondere Sensibilisierungsmaßnahmen, Begehungen, die Implementierung und Bewertung neuer Verarbeitungsprozesse, aber auch die Evaluierung bestehender Prozesse erfordern grundsätzlich die Aufmerksamkeit des Datenschutzbeauftragten.

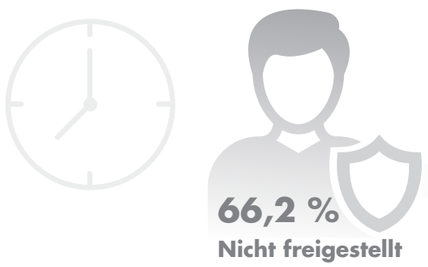
Besteht eine offizielle Freistellung für die Arbeit als Datenschutzbeauftragter mit definiertem Stundenkontingent durch die GF? Und wie viele Wochenstunden investiert der DSB durchschnittlich in die Arbeit als DSB? (in %)



33,8 %
Offiziell freigestellt

Offizielle Freistellung	
Stunden	%
1 - 10	34,8
11 - 20	21,7
21 - 30	0,0
31 - 40	43,5

Tatsächlicher Aufwand	
Stunden	%
1 - 10	29,2
11 - 20	25,0
21 - 30	8,3
31 - 40	29,2
> 40	8,3



66,2 %
Nicht freigestellt

Tatsächlicher Aufwand	
Stunden	%
0	6,4
1 - 10	74,5
11 - 20	8,5
21 - 30	2,1
31 - 40	8,5

6 % der nicht freigestellten DSB wenden überhaupt keine Zeit für ihre Rolle auf
74,5 % der nicht freigestellten DSB sind maximal 10 Stunden/Woche aktiv

E-Learning setzt sich immer mehr durch – unabhängig von der COVID-19-Pandemie

Zwar besteht keine explizite gesetzliche Pflicht zur Datenschutz-Schulung von Mitarbeitenden. Die Notwendigkeit zur Sensibilisierung und Schulung ergibt sich jedoch durch die Aufgabengebiete, die Mitarbeitende verantworten, wie beispielsweise die Pflichten zum datenschutzkonformen Umgang mit personenbezogenen Daten, Auskunftspflichten gegenüber Betroffenen oder Löschpflichten. Am Ende jedoch sind es die Unternehmen und Einrichtungen bzw. deren Verantwortliche, die zur Einhaltung der DSGVO beziehungsweise der konfessionellen Datenschutzgesetze einer Rechenschaftspflicht nachkommen müssen. Eine kontinuierliche Aufgabe der Datenschutzbeauftragten ist es, Mitarbeitende im Unternehmen in Belangen rund um den Datenschutz zu unterrichten, zu beraten und demnach in regelmäßigen Abständen zu schulen. Dabei ist die Art der Datenschutz-Schulung, die Mitarbeitende absolvieren sollten, nicht vorgeschrieben. Mögliche Mittel einer Sensibilisierung sind eine Präsenzschulung vor Ort, Zurverfügungstellung von Schulungsunterlagen oder E-Learnings online. Sicherlich haben die Auswirkungen der COVID-19-Pandemie einen Einfluss auf die Durchführung der Mitarbeiterschulungen im Zeitraum März 2020 bis zur Befragung dieser Studie. Trotz geltender Kontaktbeschränkungen und strenger Hygienekonzepte haben dennoch 33 % der Unternehmen und Einrichtungen ihre Mitarbeitenden in Präsenz geschult. 55 % nutzen E-Learning und 42 % führten ihre Schulungen virtuell via Online Meeting Tools (Videokonferenzen) durch. 30 % der Befragten gaben an, dass sie Mitarbeiterschulungen auf die Zeit nach der Pandemie verschoben haben. Im Zuge der COVID-19-Pandemie nahm die Nutzung von Videotelefonaten und -konferenzen deutlich zu. Bei einer im Januar 2021 durchgeführten Umfrage zum Nutzungsverhalten von Videokonferenzen gaben 19 % der Befragten an, fünf bis neun Stunden pro Woche Videogespräche geführt zu haben. Vor der Pandemie waren es im Vergleich nur 3 %.[1] Ähnlich wie bei der gestiegenen Nachfrage nach Videokonferenzsystemen soll diese Studie darlegen, ob Unternehmen und Einrichtungen E-Learning- Angebote zur Schulung ihrer Mitarbeitenden schon vor der Pandemie genutzt haben oder ob sie diese aufgrund der Pandemie eingeführt haben. Anders als der Trend zur bundesweit gestiegenen Nachfrage nach Videokonferenztools gaben 83 % der Befragten an, kein E-Learning aufgrund der Pandemie eingeführt zu haben. 85 % haben E-Learning bereits vor der COVID-19-Pandemie genutzt.

Zwei Drittel erreichen zwei Drittel ihrer Beschäftigten – eine Schulungslücke bleibt

Welcher Turnus zur Mitarbeiterschulung angemessen ist, wird gesetzlich nicht geregelt, sondern es gilt, die Häufigkeit von Datenschutz-Schulungen dem individuellen Unternehmen und den Einrichtungen anzupassen. In jedem Fall sollten Einrichtungen und Unternehmen davon ausgehen, dass eine einmalige Schulung von Mitarbeiter:innen nicht ausreichend ist, um langfristig und nachhaltig ein Bewusstsein für datenschutzrechtliche Belange zu schaffen. Vielmehr gilt es, Mitarbeitende in regelmäßigen Abständen auf den neuesten Stand der Themen rund um den Datenschutz zu bringen und gelernte Inhalte zu wiederholen. Nur so kann langfristig eine Unternehmenskultur entstehen, in der Datenschutz konsequent in die Arbeitsprozesse integriert wird. Dass Mitarbeiterschulungen in den Einrichtungen und Unternehmen größtenteils fest etabliert sind, zeigen die Angaben zur gewöhnlichen Schulungsquote. 40 % der Befragten gaben an, 61 bis 80 % der Beschäftigten des Unternehmens durch Schulungen zu erreichen. 28 % der Befragten erreichen 81 bis 100 % ihrer Beschäftigten. Trotz durchschnittlich hoher Schulungsquoten gaben 15 % der Befragten an, lediglich 0 bis 20 % ihrer Beschäftigten zu erreichen. Neben den regelmäßigen Schulungen ist insbesondere die Aktualität der Schulungsunterlagen wichtig. 76 % der Befragten gaben an, dass die Schulungsunterlagen regelmäßig an aktuelle Vorgaben und Gesetze angepasst werden. Sofern E-Learning genutzt wird, werden die Inhalte laut 61 % der Befragten ebenfalls in ausreichendem Umfang angepasst. Bei 32 % der Befragten erfolgt keine Anpassung der Inhalte von E-Learnings.

[1]Wie viele Stunden pro Woche nutzen Sie private Videotelefonate bzw. -konferenzen? Veröffentlicht von J. Bolkart, 26. April 2021 Abrufbar unter: https://de.statista.com/statistik/daten/studie/1225451/umfrage/umfrage-zur-nutzung-von-videotelefonie-vor-und-waehrend-der-corona-pandemie-in-deutschland/

Kritisch zu bewerten ist, dass interne Vorschriften oftmals nicht Inhalte der Schulung sind. Außerdem ist fast ein Drittel der Befragten der Auffassung, dass die Inhalte von Schulungen **nicht im ausreichenden Umfang regelmäßig auf die aktuellen Gesetze und Vorgaben angepasst** werden.

Zu welchen Themenfeldern des Datenschutzes werden die Mitarbeiter:innen geschult?
(Mehrfachauswahl möglich/in %)

90,1	Gesetzliche Grundlagen des Datenschutzes
88,7	Berufliche Schweigepflicht
80,3	Datenschutz in ihrem Tätigkeitsfeld
77,5	Umgang mit Datenpannen
76,0	Datenschutzrechtliche Praxisbeispiele aus dem Alltag

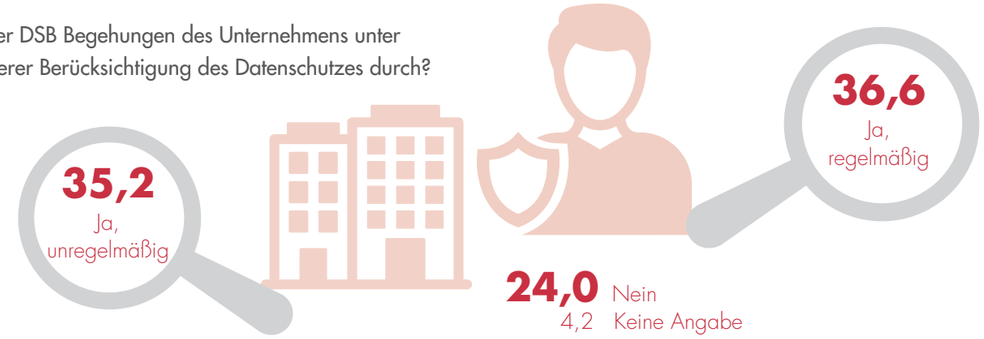
Schulungsdefizite mit Blick auf Digitalisierung

32,4	Herausforderungen, die durch die Digitalisierung entstehen
31,0	Herausforderungen durch „mobiles Arbeiten“
28,2	Vorstellung des internen Datenschutzkonzepts
19,7	Geschichte des Datenschutzes

Sonstiges: Datenschutz in Bezug auf Mitarbeitende und Bewerberdaten, Umgang mit sozialen Medien im Betrieb, Umgang mit Fotos, DSG-EKD

Häufigste Schulungsinhalte sind neben den gesetzlichen Grundlagen zum Datenschutz (90 %) die berufliche Schweigepflicht (88 %) und die Besonderheiten des Datenschutzes im Tätigkeitsfeld der Beschäftigten (80 %). Auch die Themenfelder zum Umgang mit Datenpannen (77 %) und datenschutzrechtliche Praxisbeispiele aus dem Alltag (76 %) spielen eine immer größere Rolle. Ähnlich den Ergebnissen der Datenschutzstudie aus dem Jahr 2018 finden die Vorstellung des internen Datenschutzkonzepts (28 %) sowie Herausforderungen, die durch die Digitalisierung entstehen, weniger Beachtung. Auch aktuelle Themen, die durch die COVID-19-Pandemie stärker von Relevanz geworden sind, wie die Herausforderungen des „mobilen Arbeitens“, werden nur begrenzt berücksichtigt (31 %). Durch die individuellen Angaben der Befragten wird zudem deutlich, dass vereinzelt Themen wie die Betroffenenrechte, Praxisbeispiele und Verhalten bei Datenschutzpannen keinerlei Berücksichtigung finden.
Festzuhalten bleibt, dass Schulungen zum Datenschutz von der Großzahl der Studienteilnehmer mit hohen Schulungsquoten durchgeführt werden. Kritisch zu bewerten ist, dass interne Vorschriften oftmals nicht Inhalte der Schulung sind sowie dass fast ein Drittel der Befragten der Auffassung sind, dass die Inhalte von Schulungen nicht im ausreichenden Umfang regelmäßig auf die aktuellen Gesetze und Vorgaben angepasst werden.

Führt der DSB Begehungen des Unternehmens unter besonderer Berücksichtigung des Datenschutzes durch?
(in %)



Begehungen zum Datenschutz weitgehend etabliert
Um den aktuellen Umsetzungsstand der datenschutzrechtlichen Vorgaben nachzuvollziehen, sind Begehungen in den Einrichtungen ein etabliertes und zielführendes Vorgehen. Dabei werden Schwachstellen und deren Nachbesserungsbedarf identifiziert, um potenzielle Maßnahmen zur Beseitigung des Problems zu finden. Rund drei Viertel der Befragten gaben an, dass Begehungen grundsätzlich durchgeführt werden. Rund 37 % der Befragten gaben an, dass Kontrollen durch den Datenschutzbeauftragten regelmäßig (mind. einmal jährlich) stattfinden. Bei rund 35 % der Befragten finden Begehungen unregelmäßig statt.
Unabhängig davon, ob in den Einrichtungen regelmäßige oder unregelmäßige Begehungen durchgeführt werden, erfolgt mehrheitlich eine Begehung pro Jahr (ca. 54 %).
Erwähnenswert ist ebenfalls, dass bei rund 15 % der Befragten mehr als zehn Begehungen pro Jahr stattfinden. Rund 6 % gaben an, dass mehr als 20 Begehungen pro Jahr durchgeführt werden.

Bei 24 % der Befragten führt der Datenschutzbeauftragte hingegen keine Begehungen in den Räumlichkeiten der Einrichtung durch. In diesen Fällen besteht das Risiko, dass Schwachstellen bzw. Handlungslücken langfristig unbemerkt bleiben.
Insofern Begehungen durchgeführt werden, stehen insbesondere

1. der Zugang zu Daten in Papierform (96 %),
2. der Zugang zu digitalen Daten (94 %),
3. der Zugang zu Diensträumen (90 %),
4. die Einhaltung allgemeiner Datenschutzgegenstände (88 %),
5. die Einhaltung der einrichtungsspezifischen Datenschutzgrundsätze (86 %) sowie
6. die datenschutzrechtlichen Risiken im Rahmen von Ereignissen höherer Gewalt, wie Brandschutz und die bauliche Ausgestaltung des Serverraums (51 %),

im Mittelpunkt der Betrachtung.

Wie wird mit erkannten datenschutzrechtlichen Risiken umgegangen?
(in % / Mehrauswahl möglich)

67,6	Report an die administrativen Bereiche bzw. GF
52,1	Dokumentiert; durch Handlungsempfehlungen ergänzt
49,3	Report an die Leitung
43,7	Im Datenschutz-Jahresbericht dokumentiert
38,0	Beratung in Abteilungs- bzw. Stantionsbesprechungen
35,2	In Schulungen behandelt

Aus Fehlern lernen! Gerade Aufbereitung und Dokumentation sind gering ausgeprägt – dabei lassen sich so künftige Risiken reduzieren.

Ferner werden auch die Aktualität von Aushängen, die Rechtmäßigkeit von Datenverarbeitungsvorgängen, die Erfüllung der Informationspflichten, das Videoüberwachungssystem sowie der Umgang mit Datenschutzverletzungen berücksichtigt und inspiziert.

Gefahr erkannt – Gefahr gebannt? Differenziertes Bild beim Umgang mit datenschutzrechtlichen Risiken

Um den Datenschutz in der Einrichtung nachhaltig zu verbessern und die datenschutzrechtlichen Risiken zu minimieren, bedarf es einer Nachverfolgung der identifizierten Schwachstellen. Nach Begehungen wird mehrheitlich (67 %) ein Report an die administrativen Bereiche bzw. Geschäftsführung der Einrichtung adressiert, um diese über bestehende Missstände und Handlungsbedarfe in Kenntnis zu setzen. Rund die Hälfte der Datenschutzbeauftragten (49 %) stellen der Leitung einen Reportbericht zum Begehungsergebnis bereit. Um das datenschutzrechtliche Risiko zu mindern, werden Feststellungen bei 38 % der Befragten in Stations- bzw. Abteilungsbesprechungen thematisiert und bei 35 % inhaltlich in Schulungen behandelt. 44 % der Befragten dokumentieren Risiken im Datenschutz-Jahresbericht und bei 52 % der befragten Einrichtungen wird die dokumentierte Feststellung durch Handlungsempfehlungen für die Betroffenen ergänzt. Ferner gaben die Befragten der Studie an, dass die Feststellung eines datenschutzrechtlichen Risikos zu einer Aktualisierung im Datenschutzhandbuch führt, Einzelgespräche sowie Teambesprechungen stattfinden und im Einzelfall eine Datenschutzfolgeabschätzung erstellt wird.

Wirksame Nachverfolgung lohnt sich: Zwei Drittel stellen Verbesserung fest

Ob datenschutzrechtliche Begehungen einen signifikanten Mehrwert für die Einrichtung haben und zur Verbesserung des Schutzes der personenbezogenen Daten beitragen, hängt in erster Linie von der Nachverfolgung der festgestellten datenschutzrechtlichen Risiken ab. Knapp zwei Drittel der Befragten (64 %) gaben an, dass Feststellungen aus Begehungen nachverfolgt wurden, sodass die Begehung zu einer wirksamen Verbesserung in Hinblick auf den Datenschutz beigetragen hat.

Die restlichen 13 % haben keine wirksame Verbesserung in Hinblick auf die identifizierten datenschutzrechtlichen Risiken im Rahmen der Begehung erfahren.
Rund ein Viertel der Befragten (24 %) konnten bzw. wollten keine Angaben hinsichtlich der wirksamen Verbesserung im Zusammenhang mit der Nachverfolgung machen. In diesen Fällen ist nicht nachzuvollziehen, ob die Nachverfolgung zur Verbesserung beigetragen hat oder überhaupt eine Nachverfolgung zur wirksamen Verbesserung des erkannten Risikos angestrebt wurde.

2. Umsetzung datenschutzrechtlicher Standards

Eine erfolgreiche Umsetzung von Datenschutz im Unternehmen und in den Einrichtungen ist maßgeblich abhängig von der Umsetzung auch ergänzender datenschutzrechtlicher Standards. Die wichtigsten Standards werden in diesem zweiten Teil unserer Studie beleuchtet.

Vereinbarungen zur Auftragsverarbeitung

Bedingt durch eine zunehmende Digitalisierung der Arbeitswelt sowie eine verstärkte Fokussierung auf Kernkompetenzen, nutzen immer mehr Einrichtungen Auftragsverarbeiter, die diese in ihrem Arbeitsalltag unterstützen. Exemplarisch seien hier Software zur Zeiterfassung bzw. Finanzbuchhaltung sowie der (technische) Support komplexer Medizingeräte mittels Fernzugriff genannt. Ungeachtet der konkreten Anwendung besteht seitens der Unternehmen, als Verantwortliche für diese Datenverarbeitung, die Notwendigkeit, mit diesen Anbietern eine Vereinbarung zur Auftragsverarbeitung gemäß DSGVO beziehungsweise entsprechend den konfessionellen Regelungen zu schließen.
61 % der befragten Einrichtungen geben an, dass in der Einrichtung eine Übersicht der geschlossenen Verträge zur Auftragsverarbeitung besteht. Zum Vergleich: In der Datenschutzstudie 2018 haben rund 76 % der befragten Einrichtungen angegeben, dass eine solche Übersicht vorhanden ist. 30 % geben an, dass diese teilweise vorhanden ist. 7 % der befragten Einrichtungen geben an, dass keine Übersicht vorhanden sei, 3 % haben keine Angaben gemacht.

Risikoeinschätzung und Wirksamkeitsprüfungen

37 % der befragten Einrichtungen geben an, dass sie regelmäßig Risikoeinschätzungen hinsichtlich des Datenschutzes durchführen. Diese Angaben sind vergleichbar mit der Aussage zur Überprüfung der technischen und organisatorischen Maßnahmen auf deren Wirksamkeit. Hier geben 34 % der befragten Einrichtungen an, dass erkannte potenzielle Datenschutzrisiken regelmäßig überprüft werden.
45 % der befragten Einrichtungen geben an, dass sie teilweise Risikoeinschätzungen durchführen.
Eine Aussage, die ebenfalls vergleichbar ist mit den Angaben zur Wirksamkeitsprüfung technischer und organisatorischer Maßnahmen (49 %).

Lediglich 14 % der befragten Einrichtungen geben an, dass weder regelmäßige Risikoeinschätzungen noch Wirksamkeitsprüfungen der technischen und organisatorischen Maßnahmen stattfinden. 4 % bzw. 3 % der Befragten haben keine Angaben gemacht.

Drei Baustellen in der alltäglichen Umsetzung

Hinsichtlich der Fragstellung, welche datenschutzrechtlichen Anforderungen im Alltag die größten Schwierigkeiten ergeben, lassen sich drei Antworten extrahieren, die nahezu in jeder Rückmeldung vorhanden sind.

1. Die Durchführung von **Datenschutz-Folgenabschätzungen** bereitet einer Mehrzahl der befragten Einrichtungen Schwierigkeiten. Als Ursache wird (selbstkritisch) angemerkt, dass den Datenschutzbeauftragten die notwendige Erfahrung fehlt, aber auch die fehlende Unterstützung der Unternehmensleitung. Letztere ist sicherlich erforderlich, um entsprechende Ressourcen zur Verfügung zu stellen.

2. Die **Auskunft** gegenüber Angehörigen sowie öffentlichen Stellen gilt als herausfordernd. Ursächlich hierfür ist zum einen die mangelnde Akzeptanz der Auskunftsersuchenden sowie zum anderen die Sensibilisierung der Beschäftigten.

3. Die **datenschutzkonforme Übermittlung** personenbezogener Daten an öffentliche Stellen und Kooperationspartner sowie weitere Leistungserbringer ist eine weitere Hürde. Als eine Ursache wird die fehlende einheitliche Verschlüsselung betrachtet.

Prozesse zur Gewährleistung der Umsetzung
78 % der befragten Einrichtungen geben an, dass sie einen Prozess implementiert haben, der die Erstellung des Verzeichnisses der Verarbeitungstätigkeiten gewährleistet. Im Vergleich zur Datenschutzstudie 2018 wird eine Steigerung von ca. 20 % deutlich. Daraus lässt sich ableiten, dass die befragten Einrichtungen mit den Prozessen vertraut sind und eine Bereitschaft zur Unterstützung des Datenschutzbeauftragten vorhanden ist.

Prozess zur Erstellung des Verzeichnisses der Verarbeitungstätigkeiten

2021: 78 %
2018: 58 %
+ 20 %

49 % der befragten Einrichtungen geben an, dass ein Prozess zu den Betroffenenrechten implementiert ist. Somit haben mehr als die Hälfte der befragten Einrichtungen keinen Prozess implementiert und laufen ggf. Gefahr, dass Betroffene in der Wahrnehmung ihrer Rechte entsprechend den datenschutzrechtlichen Vorgaben eingeschränkt werden.
82 % der befragten Einrichtungen haben einen Prozess zum Umgang mit Datenschutzverletzungen eingerichtet. Es ist anzunehmen, dass dies auf einen risikoorientierten Ansatz zurückzuführen ist, da eine ausbleibende Meldung einen schweren Verstoß gegen die DSGVO sowie die konfessionellen Datenschutzgesetze darstellt und somit ein erhöhtes Bußgeldrisiko auslöst.
70 % der befragten Einrichtungen geben an, dass hinsichtlich der Schulungs- und Sensibilisierungsmaßnahmen ein Prozess vorhanden ist. Im Vergleich zur Datenschutzstudie 2018 ergibt sich ein Rückgang um 17 %. Aller Wahrscheinlichkeit ist dies dadurch begründet, dass 30 % der befragten Einrichtungen angegeben haben, dass Schulungen auf die Zeit nach der Pandemie verschoben werden.
21 % geben an, dass ein Plan-Do-Check-Act-Zyklus (PDCA) hinsichtlich der Datenschutzthemen vorhanden ist. In Anbetracht der Tatsache, dass die DSGVO sowie die konfessionellen Datenschutzgesetze eine dem PDCA-Zyklus entsprechende Systematik erwarten, besteht hier Handlungsbedarf.

Erschwerende Begleitumstände bei der Umsetzung
62 % geben an, dass die Umsetzung der Datenschutzmaßnahmen durch nicht ausreichende Ressourcen erschwert wird. Nach Auffassung von 55 % der befragten Einrichtungen erschwert ein erhöhter Arbeitsaufwand durch Recherchen nach Gerichtsurteilen und Praxishilfen die Umsetzung.
Anhaltende Rechtsunsicherheit durch die Regelungen der DSGVO sowie der konfessionellen Datenschutzgesetze (38 %) sowie zu häufige Änderungen oder Anpassungen bei der Auslegung der Verordnung (37 %) würden zudem die Umsetzung erschweren.
In diesem Zusammenhang sind 21 % der Meinung, dass die uneinheitliche Auslegung der Regeln innerhalb der EU eine Umsetzung behindert.
Bei rund einem Drittel der Befragten hindern fehlende Umsetzungshilfen der Aufsichtsbehörden oder fehlendes Fachpersonal an der Umsetzung der Maßnahmen.
22 % der befragten Einrichtungen geben an, dass die Möglichkeit zum fachlichen Austausch nicht gegeben ist. Zusammengefasst lässt sich festhalten, dass insbesondere die unterschiedliche Auslegung der Regelungen sowie die wachsende Zahl gerichtlicher Entscheidungen zu datenschutzrelevanten Themen die Umsetzung von Maßnahmen erschweren.

Verschärfung des Datenschutzes
Nach Auffassung von 45 % der befragten Einrichtungen ist die vermutete Verschärfung des Datenschutzes seit 2018 eingetreten. Zum Vergleich: In der Datenschutzstudie 2018 waren 41 % der Befragten der Auffassung, dass eine Verschärfung eintreten werde. 17 % der Befragten erkennen keine Verschärfung. Bei 24 % ist diese teilweise eingetreten. 14 % machen keine Angabe.
Die Befragten geben an, dass die Verschärfung im Wesentlichen durch umfangreichere Informationspflichten (84 %), Datenschutz-Folgenabschätzungen (78 %), erhöhte Rechenschaftspflichten (69 %) sowie Verträge zur Auftragsverarbeitung (67 %) und das Verzeichnis der Verarbeitungstätigkeiten (67 %) erfolgt ist.
Hinsichtlich der Meldepflicht von Datenschutzverletzungen sind 60 % der befragten Einrichtungen der Auffassung, dass diese zu einer Verschärfung geführt hat. 55 % geben an, dass Einwilligungen eine Verschärfung darstellen. Höhere Geldbußen (51 %) sowie berechtigte Anfragen von Betroffenen (49 %) führen nach Auffassung der befragten Einrichtungen zu einer Verschärfung des Datenschutzes.
41 % geben an, dass erweiterte Kontrollen zu einer Verschärfung führen – für ein Drittel sind es auch unberechtigte Anfragen von Betroffenen, die zu einer Verschärfung führen.

51 % ohne Prozess zur Wahrung der Betroffenenrechte!

79 % ohne PDCA-Zyklus – trotz klarer gesetzlicher Anforderung

Für welche der Datenschutzmaßnahmen wurde ein Prozess implementiert, der die Umsetzung gewährleistet?
(Mehrfachauswahl möglich/in %)

81,7 %
Umgang mit Datenschutzverletzungen

77,5	Verzeichnis der Verarbeitungstätigkeiten
70,4	Vereinbarungen zur Auftragsverarbeitung
70,4	Schulungen und Sensibilisierung der Mitarbeitenden
63,4	Zugriffs-/Berechtigungskonzept
62,0	Datenschutz-Folgenabschätzung
59,2	Einwilligungen angepasst
49,3	Prozess zu den Rechten der Betroffenen implementiert
45,1	Anpassung der IT
21,1	Einführung eines PDCA-Zyklus für Datenschutzthemen

Gut laufende Prozesse

Durch welche Begleitumstände wird die Umsetzung von Datenschutzmaßnahmen erschwert?
(Mehrfachauswahl möglich/in %)

62,0 %
Nicht ausreichende Ressourcen

55,0	Erhöhter Arbeitsaufwand durch Recherche nach Anpassung, Gerichtsurteilen oder Praxishilfen
38,0	Anhaltende Rechtsunsicherheit durch die Regeln der DSGVO etc.
36,6	Zu viele Änderungen oder Anpassungen bei der Auslegung der Verordnung
32,4	Fehlende Umsetzungshilfen durch Aufsichtsbehörden
28,2	Fehlendes Fachpersonal
22,6	Fehlende Möglichkeit zum fachlichen Austausch
21,1	Uneinheitliche Auslegung der Regeln innerhalb der EU

Erschwerte Prozesse

3. Datenschutzaufsichtsbehörden

Ungefähr die Hälfte der internen Meldungen erfüllt statistisch die Kriterien zur Weitergabe an übergeordnete Aufsichtsbehörden. Der dritte Teil unserer Studie widmet sich der Organisation der entsprechenden Behörden, vor allem aber auch dem Miteinander von Unternehmen bzw. Einrichtung und Aufsichtsbehörde.

Meldung Datenschutzvorfälle

Mit der DSGVO beziehungsweise den angepassten konfessionellen Regelungen hat das Thema um die Meldung von Datenschutzvorfällen eine eigene Dynamik entwickelt. Betrachtet man einmal selbstkritisch seine internen Prozesse, fallen doch relativ häufig Datenpannen auf. Diese sind von unterschiedlicher Schwere – von der verlegten Akte, dem Fehlversand schützenswerter Daten an den falschen Empfänger bis zur versehentlichen Freischaltung brisanter Daten im Internet.

55 % der teilnehmenden Einrichtungen registrieren über das Jahr lediglich 1–5 Vorfälle. Nur ein geringer Teil bekommt häufiger eine entsprechende Information. Dies lässt eine Diskrepanz zwischen Tatsächlichem und Gemeldetem erahnen. Die Erfahrung zeigt, dass nur mit stetiger Schulung und dem Aufbau eines internen Meldesystems die Fehler registriert und Schwachstellen optimiert werden können. Kann in der Schulung nicht ein vertraulicher Umgang mit den Daten vermittelt werden, lässt so mancher Mitarbeitende aus Sorge um arbeitsrechtliche Konsequenzen die Meldung in der Schublade verschwinden.

Ungefähr die Hälfte der internen Meldungen erfüllen die Kriterien zur Weitergabe an die Aufsicht – vorausgesetzt, die Bewertung erfolgte ordnungsgemäß. Dies zeigt ein Abwägungsverhalten der Einrichtungen und nicht ein automatisches Durchreichen, was den Pensenschlüssel[2] der Aufsichten unverhältnismäßig anwachsen ließe. Durch diese Selektion können die leichten Fälle hausintern optimiert werden. Unter Beteiligung der Aufsicht ist dann bei schwerwiegenden Fällen gewährleistet, dass zum einen eine Aufarbeitung nachvollziehbar dargestellt werden muss und zum anderen Wiederholungen, welche aufgrund einer fehlenden Aufarbeitung passieren, mit einem Bußgeld geahndet werden können.

Interessant bleibt die Frage, inwieweit die Aufsichten die Gesamtheit der Eingaben auswerten. Wünschenswert wäre ein anonymisierter Report, von dem alle profitieren und anhand dessen sie vorsorglich ihre Prozesse überprüfen können.

Rückmeldungen der Aufsicht

In knapp 48 % der Eingaben erfolgte keine Reaktion seitens der Aufsicht. Dies ist auch nicht erforderlich, erleichtert aber den Abschluss auf Seiten der meldenden Stelle. In den anderen Fällen verteilen sich eine zügige Rückmeldung und eine verzögerte Reaktion zu ungefähr vergleichbaren Teilen. Soweit eine entsprechende Reaktion überhaupt erfolgte, beschränkt sich der Großteil auf ein bis zwei Kontakte. Dies wird regelhaft die Aufforderung zur Stellungnahme und die abschließende Bescheidung sein. Langwierige Verfahren werden selten geführt.

Eine Auswertung der Freitexte lässt mehrheitlich eine kooperative und auch beratende Hilfestellung durch die Aufsichten erkennen. In einigen Fällen wird eine praxisferne und sehr bürokratische Zusammenarbeit beklagt. Zusammenfassend machen fast 47 % der teilnehmenden Einrichtungen eine positive Erfahrung mit den Aufsichten.

Hilfreich ist auch die Teilnahme der Aufsichten an Veranstaltungen der Einrichtungen zum Datenschutz. Erfa-Kreise zum Beispiel eröffnen den Blick für beide Positionen. So werden Vorurteile abgebaut.

Abschließend lässt sich das (noch) zurückhaltende Kontrollverhalten auf die seit 2018 aufzubauende Personalstruktur der Aufsichten zurückführen. Parallel wirken sich sicherlich gerade bei der spezifischen Struktur der Teilnehmer die behördlichen pandemiebedingten Betretungsverbote aus. Die herausfordernde Situation nicht noch durch datenschutzrechtliche Kontrollen zu verschärfen, zeigt ein umsichtiges Verhalten auch der Aufsichten.

[2] Gemäß Personalbedarfsberechnungssystem (PEBB§Y), nach welchem ein angemessener Personalbedarf festgelegt wird, um einen effektiven Rechtsschutz sicherstellen zu können.

Struktur der Datenschutz-Aufsichten in Deutschland

Während die konfessionelle Datenschutzaufsicht sich recht heterogen darstellt und nicht immer klassisch die Aufteilung gemäß den Landeskirchen bzw. Bistümern widerspiegelt, entspricht die behördliche Struktur des Bundes den bekannten föderalen Gegebenheiten.

Aufsichtsstruktur in Deutschland

Datenschutzaufsichtsbehörde des Bundes

Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Datenschutzaufsichtsbehörden der Länder

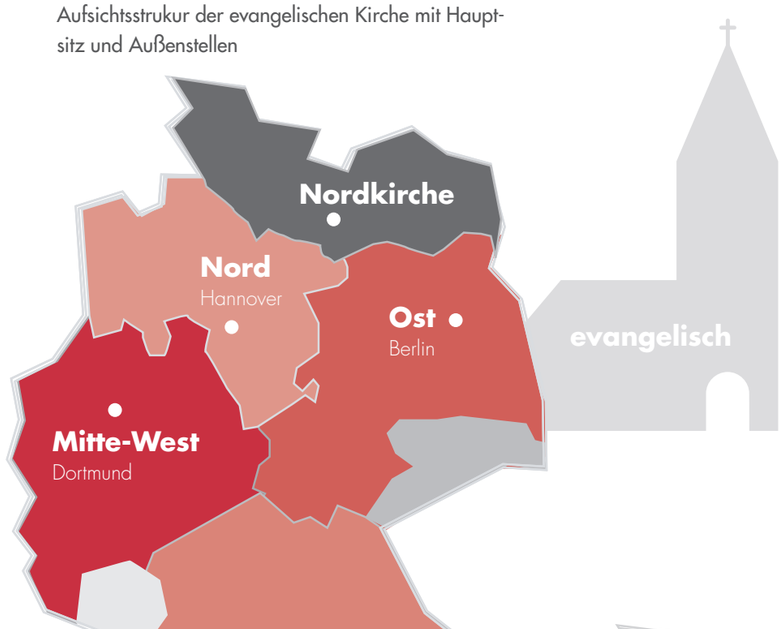
Jedes Bundesland verfügt über eine Datenschutzaufsichtsbehörde – nur Bayern differenziert nach öffentlichen und nicht öffentlichen Stellen (also für die Privatwirtschaft (Art. 18 BayDSG)).

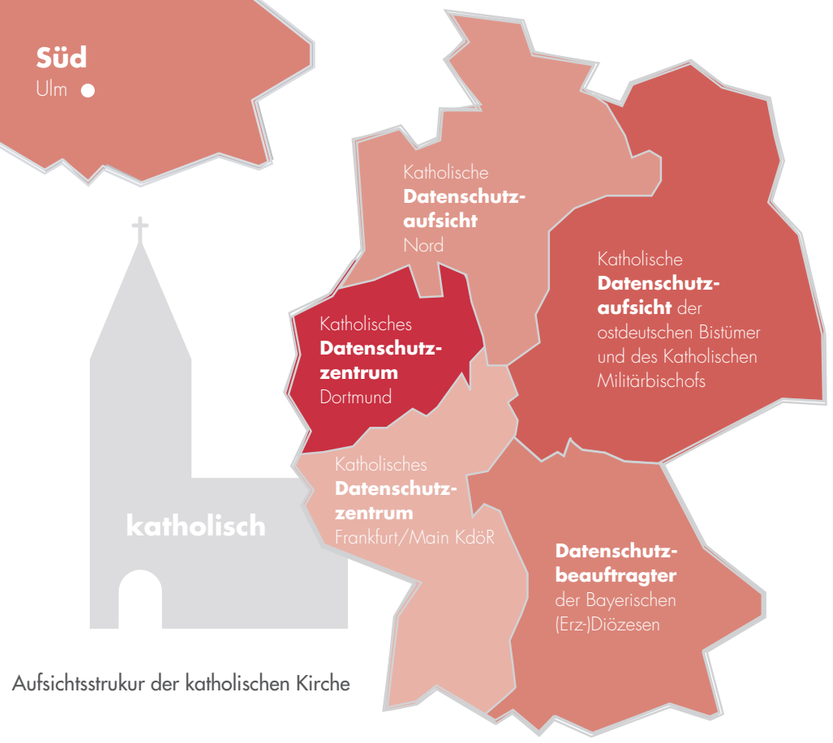
Datenschutzbeauftragte der Religionsgemeinschaften

- Diözesandatenschutzbeauftragte der katholischen Kirche in Deutschland
- Der Beauftragte für den Datenschutz der EKD
- Der Beauftragte für den Datenschutz im Evangelischen Werk für Diakonie und Entwicklung
- Datenschutzbeauftragte aus Kirche und Diakonie, die die Datenschutzaufsicht nicht auf die EKD übertragen haben

Die detaillierte Struktur des Datenschutzes in der evangelischen und katholischen Kirche findet sich auf der Folgeseite.

Aufsichtsstrukur der evangelischen Kirche mit Hauptsitz und Außenstellen





Aufsichtsstrukur der katholischen Kirche

4. Datenschutz und Digitalisierung

Das Gesundheits- und Sozialwesen hatte sich trotz verschiedener gesetzlicher Initiativen bisher als relativ zögerlich bei der Digitalisierung der Leistungsprozesse gezeigt. Als Triebfeder der Digitalisierung fungiert seit Beginn des Jahres 2020 schließlich die COVID-19-Pandemie. Die Entwicklung im Bereich der Digitalisierung sowie die damit verbundenen Anforderungen an den Datenschutz beleuchtet Teil 4 unserer Studie.

Die COVID-19-Pandemie als Treiber der Digitalisierung hat sich in vielen Bereichen niedergeschlagen. Der Trend erreichte, anders als zuvor, auch das Leistungsangebot: So gab es im Krankenhaus einen großen Bedarf, beispielsweise Vor- und Nachsorgegespräche über Videotools durchzuführen oder im Bereich der Sozialhilfe Online-Beratung anzubieten. Auch neue Lösungen des Instant-Messagings, der digitalen Kontaktnachverfolgung sowie der Besucherregistrierung wurden eingeführt, ebenso neue Kollaborationstools und Cloud-Dienste, die das Arbeiten im Homeoffice erleichtern sollten. Flankiert wurde dies durch neue Förderprogramme, die häufig für eine verbesserte technische Ausstattung verwendet wurden. Heute sind daher auch im Gesundheits- und Sozialwesen die überwiegende Anzahl der Arbeitsplätze mit Mikrofonen und Kameras ausgestattet. Treiber dieser Entwicklungen sind hierbei klar die Geschäftsführungen, die ein Interesse daran haben, dass die Leistungen auch in Zeiten von Lockdown und Kontaktbeschränkungen weiter erbracht werden können. Aber auch die Beschäftigten und Patienten bzw. Klienten selbst haben die Entwicklung forciert, indem sie neue Lösungen eingefordert haben, um entweder unnötige Risikokontakte zu vermeiden oder Kinder im Homeschooling betreuen zu können. Darüber hinaus zeigen die Studienergebnisse, dass zum einen auch das Marktumfeld mit einem Drittel als Grund für die Einführung neuer Lösungen genannt wurde – wenn die Klinik im Nachbarstadtteil virtuelle Rundgänge im Kreißsaal anbietet, möchte man selbst hier ja nicht hintenanstehen – und zum anderen auch die Kostenträger selbst die Digitalisierung vorantreiben. Bei Letzteren sind sicherlich die Möglichkeiten zur Refinanzierung entsprechender Online-Angebote eine wesentliche Motivation.

Wodurch wird die Digitalisierung in Ihrem Unternehmen vorangetrieben? (in %)
Durch die Digitalisierungswünsche...

70,4 % aus eigenem Anspruch der Geschäftsführung

57,8 % der Beschäftigten

32,4 % der Patienten und Klienten

31,0 % der Kooperationspartner und weitere Leistungsbringer

28,2 % der Kostenträger

14,1 % der Aufsichtsgremien

5,6 % keine Treiber / 8,5 % keine Angabe

Parallel zu diesen Faktoren sorgt auch der Gesetzgeber für eine zunehmende Digitalisierung des Gesundheits- und Sozialwesens. So wurde seit dem Jahr 2020 mit dem E-Health-Gesetz der Ausbau der Telematikinfrastruktur vorangetrieben und diese trotz der Schwierigkeiten bei der technischen Umsetzung und Engpässen bei der Lieferung der notwendigen Hardware auch von zunehmend mehr Krankenhäusern und Praxen eingesetzt. Bis zum Jahr 2024 soll die Telematik dann als Datenautobahn alle Leistungserbringer im Gesundheitswesen miteinander vernetzen und die Nutzung von elektronischer Patientenakte, E-Rezept und E-AU ermöglichen. Dieses Vorhaben hat die neue Ampelkoalition auch noch einmal in ihrem Koalitionsvertrag bekräftigt.
Daher ist anzunehmen, dass viele Leistungserbringer im Gesundheitswesen hier bislang eine abwartende Haltung bei der Einführung anderer (und sicherer) Kommunikationsmittel eingenommen haben, ansonsten lässt sich kaum die hohe Anzahl der Einrichtungen erklären, die das Fax weiterhin als Kommunikationsmedium einsetzen, trotz der expliziten Warnungen hinsichtlich der Datensicherheit, die von verschiedenen Landesdatenschutzbeauftragten in Bezug auf die Faxnutzung ausgesprochen worden sind. [3,4]

Nutzen Sie in Ihrer Einrichtung weiterhin das Fax als Kommunikationsmittel? (in %)

47,9 % Ja, Fax-over-IP

38,0 % Ja, analog

5,6 % Nein

8,5 % k. A.

Datenschutzgefahr 38 % nutzen trotz expliziter Warnung unverändert das analoge Fax

[3] Der Hessische Beauftragte für Datenschutz und Informationsfreiheit: „Zur Übermittlung personenbezogener Daten per Fax", 22. Februar 2022, abrufbar unter: https://datenschutz.hessen.de/datenschutz/it-und-datenschutz/zur-%C3%BCbermittlung-personenbezogener-daten-per-fax

[4] Der Landesbeauftragte für Datenschutze Freie Hansestadt Bremen: „Telefax ist nicht Datenschutz konform", Mai 2021, abrufbar unter: https://www.datenschutz.bremen.de/datenschutztipps/orientierungshilfen-und-handlungshilfen/telefax-ist-nicht-datenschutz-konform-16111

Datenschutz als Hemmschuh für Digitalisierung?
Der Vorwurf ist zu vernehmen, dass der Datenschutz ein Hemmschuh für die Umsetzung von Digitalisierungsmaßnahmen im Gesundheits- und Sozialwesen ist. Dabei ist noch einmal zu betonen, dass sich die Gesundheitswirtschaft bereits in der Vergangenheit immer wieder aufgrund der Vielzahl von Interessengruppen und der föderalen Struktur als besonders reformresistent gezeigt hat. Dies lässt vermuten, dass der Datenschutz hier zum einen gerne als „Schwarzer Peter" herangezogen wird, wenn die ambitionierten Ziele der Digitalisierung nicht im anvisierten Zeitrahmen erreicht werden konnten. Zum anderen sollte nie aus dem Blick geraten, dass gerade die in der Gesundheits- und Sozialwirtschaft verarbeiteten Daten höchst sensibel sind und bei einer Gefährdung schwerste Folgen für die betroffenen Personen möglich sind. Diese Sorgen werden wohl auch von einem Großteil der behandelten Patienten geteilt.
So gab nur ein Viertel der Teilnehmenden die Akzeptanz der Patienten für Vorgaben des Datenschutzes als Hürde für die Digitalisierung an.

Mehr als 40 % benennen dagegen den mit der Einführung neuer digitaler Verfahren verbundenen datenschutzrechtlichen bürokratischen Aufwand in Form der Datenschutz-Folgenabschätzung als wesentliche Hürde. Im Rahmen dieses Risiko-Assessments sind systematisch alle technischen, rechtlichen und prozessualen Risiken zu erfassen, die auf die betroffenen Personen(gruppen) einwirken können. Dies erfordert nicht nur ein ausgeklügeltes methodisches Vorgehen und multidisziplinäres Fachwissen, sondern ist in der Regel auch sehr zeit- und mitunter kostenintensiv. Das bestätigen auch die Erkenntnisse zu den verschärften Anforderungen zum Datenschutz aus dem Kapitel „Umsetzung datenschutzrechtlicher Standards", S. 13ff.

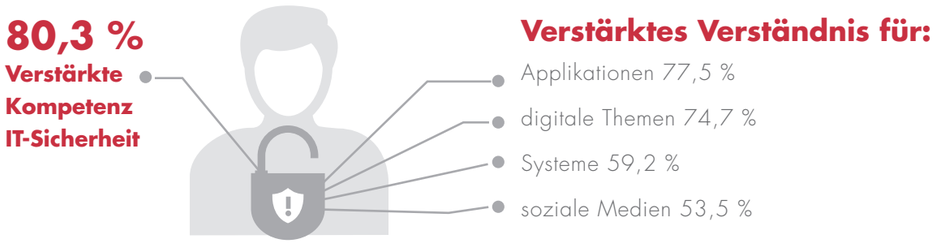
Welche Anforderungen der Digitalisierung stellen besonders große Hürden dar? (in %)

41,4 %
Einschätzung der erforderlichen Datenschutzfolgeabschätzung

34,3 % Akzeptanz unter Beschäftigten für Vorgaben der datenschutzrechtlichen Prüfung

24,3 % Akzeptanz der Patienten für Vorgaben der datenschutzrechtlichen Prüfung

Welche neuen Anforderungen stellt die Digitalisierung an den Datenschutzbeauftragten? (in %)



Digitalisierung treibt die Anforderungen an DSB

Mit den Maßnahmen zur Digitalisierung steigen zweifellos auch die Anforderungen an die Datenschutzbeauftragten. So nannten jeweils mehr als drei Viertel der Befragten, dass ein tiefergehendes Verständnis sowohl für digitale Themen als auch für Applikationen und Anwendungen gefordert wird. Mehr als 80 % der Befragten sehen neue Anforderungen bei der notwendigen Kompetenz im Bereich der IT-Sicherheit. Mehr als die Hälfte halten entsprechende Anforderungen auch in Bezug auf die IT-Systeme selbst und auf den Bereich der sozialen Medien für notwendig. In den zuvor genannten Bereichen zeigt sich seit vielen Jahren eine sehr dynamische technische Entwicklung, insofern ist in Frage zu stellen, ob Datenschutzbeauftragte durch einmalige Schulung oder unregelmäßige Fortbildungen diesen Anforderungen überhaupt noch gerecht werden können (vgl. Kapitel „Datenschutzbeauftragte, S. 5ff.). Neben Fort- und Weiterbildungsmaßnahmen werden von den Studienteilnehmern auch weitere Maßnahmen ergriffen, um das Know-how des Datenschutzbeauftragten sicherzustellen (vgl. Abb. „Wie wird sichergestellt, dass die/der DSB das erforderliche Know-how erhält/besitzt?"). Hier ist zuerst, von mehr als der Hälfte der Befragten, die verstärkte Zusammenarbeit zwischen IT und Beauftragtem zu nennen, was als interne Wissensweitergabe sehr zielführend sein dürfte. Aber auch die Unterstützung durch externe Berater wird von der Hälfte der Einrichtungen als Möglichkeit genutzt, ebenso werden die Nutzung entsprechender Fachliteratur und der Austausch in Expertentreffen für das Wissensmanagement herangezogen. Weit weniger verbreitet ist die Bestellung externer Datenschutzbeauftragter, was nur von ca. 30 % der teilnehmenden Einrichtungen genutzt wird.

Die Pandemie als Digitalisierungsbeschleuniger – kommt der Datenschutz hinterher?

Wie wirkt sich nun die Digitalisierungsdynamik im Zusammenhang mit der COVID-19-Pandemie auf das Vertrauen in den Datenschutz allgemein aus?

Hier zeigt die Studie ein eher gemischtes Bild (vergl. Abb. unten): Während knapp 40 % der Befragten konstatieren, dass durch die hohe Komplexität das Vertrauen in den Datenschutz sinkt, sieht ein Drittel keinen Einfluss auf den Datenschutz. 10 % hingegen nehmen ein gestiegenes Vertrauen in den Datenschutz wahr.
Zu den Gründen für diese Ergebnisse lässt sich an dieser Stelle nur spekulieren: Zum einen wird hier sicherlich die bereits angesprochene Suche nach dem „Sündenbock" eine Rolle spielen. Zum anderen sind Positionen von Lobby- und Berufsverbänden in Verbindung mit einer verzerrten medialen Berichterstattung als Gründe anzuführen. Wenn beispielsweise die Gesellschaft für Orthopädie und Unfallchirurgie beklagt, dass der Datenschutz im Rahmen von Notarzteinsätzen Menschenleben gefährdet und eine bekannte deutschlandweite Tageszeitung daraufhin titelt „Daten gerettet, Patient tot", prägt dies in der Bevölkerung nicht nur ein falsches Bild des Datenschutzes, sondern erschwert darüber hinaus auch die Arbeit der Datenschutzbeauftragten selbst.

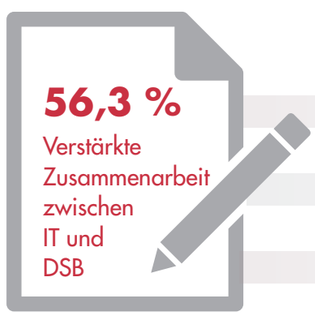
Weiter zunehmende Komplexität bei der Erfüllung aller Vorgaben

Nicht von der Hand zu weisen ist die hohe und noch weiter zunehmende Komplexität bei der Umsetzung der datenschutzrechtlichen Anforderungen. Neben den Informationen zur Datenverarbeitung, die den Betroffenen an vielen Stellen in geeigneter Weise zur Verfügung zu stellen sind, fordern auch das Verzeichnis der Verarbeitungstätigkeiten und allen voran die besagte Datenschutz-Folgenabschätzung einen hohen personellen und zeitlichen Einsatz. In Anbetracht der zum Teil sehr dürftigen Freistellung der Datenschutzbeauftragten (vgl. Kapitel „Datenschutzbeauftragte", S. 5ff), darf bezweifelt werden, dass die Unternehmen und Einrichtungen diesen Anforderungen wirklich gerecht werden. Daher sind die Geschäftsführungen aufgerufen, nicht nur in die Fort- und Weiterbildung zu investieren, sondern auch die erforderlichen Ressourcen für die Datenschutzbeauftragten bereitzustellen.

Expertentreffen – Erfahrungsaustausch, der sich lohnt

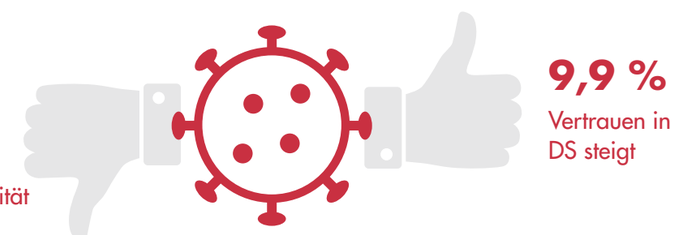
Nur 40 % der Befragten nutzen den Austausch in Expertentreffen als Möglichkeit zum Erhalt und Ausbau des Fachwissens. Mittlerweile werden viele Formate des Erfahrungsaustauschs sowohl auf regionaler als auch branchenspezifischer Ebene organisiert, an denen zum Teil auch die Datenschutz-Aufsichtsbehörden teilnehmen und zu aktuellen Themen referieren, Anforderungen konkretisieren und für Fragen zur Verfügung stehen. Insbesondere im Gesundheits- und Sozialwesen lassen sich in Bezug auf die Datenschutz-Folgenabschätzungen Potenziale nutzen, da zum einen die eingesetzten Anwendungen und Systeme in den Einrichtungen häufig die gleichen sind und zum anderen durch die Datenschutzregelungen vorgegeben wird, dass die Folgenabschätzungen thematisch größer angelegt werden können (vgl. Erwägungsgrund 92 der DSGVO) und sich von daher eine Zusammenarbeit als besonders fruchtbar herausstellen könnte.

Wie wird sichergestellt, dass der DSB das erforderliche Know-how erhält/besitzt?
(Mehrfachauswahl möglich/in %)



49,3	Unterstützung durch externe Beratung
43,7	Fachliteratur
39,4	Expertentreffen
35,2	Intensivierte Weiterbildung des DSB
29,6	Beauftragung externer DSB
11,3	k. A.

Wie wirkt sich das Pandemiegeschehen und die daraus resultierende Digitalisierungsdynamik auf den DS aus? (in %)



33,8	Pandemie hat keinen Einfluss auf Vertrauen in DS
16,9	k. A.

Ausblick

Neben der heute schon geforderten Branchen- beziehungsweise Unternehmenskenntnis und einem Verständnis für die rechtlichen Zusammenhänge wird es verstärkt darauf ankommen, dass Datenschutzbeauftragte ein besseres Verständnis für Applikationen und digitale Themen entwickeln. Letzteres wird u. a. durch den Koalitionsvertrag der aktuellen Ampel-Regierung deutlich, da dieser eine verstärkte Digitalisierung und Datennutzung im Gesundheitswesen vorsieht. Ebenso müssen Datenschutzbeauftragte ihre Kompetenzen im Bereich der IT-Sicherheit ausbauen. Diese Faktoren werden mittelfristig den Druck auf die Gesundheits- und Sozialwirtschaft erhöhen, da diese Qualifikationen und Kompetenzen am Arbeitsmarkt rar sind.
Unternehmen und Datenschutzbeauftragte sind daher gut beraten, sich mit diesen Themen zu beschäftigen und entsprechende Ressourcen zu schaffen.
Die Befragung zeigt, dass es Verbesserungspotenzial bei Sicherstellung und Erhalt des erforderlichen Know-hows der Datenschutzbeauftragten gibt.
Die DSGVO sowie die konfessionellen Datenschutzgesetze sind in den Unternehmen der Gesundheits- und Sozialwirtschaft angekommen. Die Bestellung eines Datenschutzbeauftragten ist in den befragten Unternehmen weitestgehend erfolgt. Dennoch verfügen zwei Drittel der Datenschutzbeauftragten über keine offizielle Freistellung für ihre Tätigkeit durch die Geschäftsführung. Hier klafft weiterhin eine Lücke zwischen freigestellter Zeit und dem erforderlichen Arbeitsaufwand für Datenschutzbelange.
Die Umsetzung der gestiegenen Anforderungen, insbesondere durch die Digitalisierung, ist in Teilen für die Datenschutzbeauftragten nur schwer umsetzbar, wobei die Sensibilisierung der Beschäftigten und Begehungen zum Datenschutz einen höheren Stellenwert einnehmen. Die Unternehmen konnten für gesetzlich geforderte Datenschutzmaßnahmen (z. B. Umgang mit Datenschutzverletzungen, Abschluss von Vereinbarungen zur Auftragsverarbeitung) Prozesse zu deren Umsetzung implementieren. Dennoch gestaltet es sich schwierig, dass eine Vielzahl von Sachverhalten schwammig formuliert sowie die Reichweite bestimmter Begriffe (exemplarisch sei auf die Rechtsprechung im Kontext von Auskunftsersuchen verwiesen) nach wie vor ungeklärt ist. Hinzu kommt, dass die Verantwortlichen gefordert sind, zahlreiche Gesetzesänderungen und -neuerungen (z. B. das TTDSG, das Seelsorge-PatDSG, Telematikinfrastruktur) in kürzester Zeit umzusetzen und sich dieser Trend verstetigen dürfte.
Diese Tatsache sorgt für Unsicherheiten, da sich Verantwortliche im anhaltenden Spagat zwischen gesetzeskonformer Umsetzung datenschutzrechtlicher Anforderungen auf der einen und der Notwendigkeit einer Effizienzsteigerung auf der anderen Seite befinden.
Die Befragung lässt eine Diskrepanz zwischen tatsächlichen und gemeldeten Datenschutzvorfällen erahnen. Die Erfahrung zeigt, dass nur mit stetiger Schulung und dem Aufbau eines internen Meldesystems Fehler registriert und Schwachstellen behoben werden können. Das (noch) zurückhaltende Kontrollverhalten ist sicherlich auf die seit 2018 aufzubauende Personalstruktur der Aufsichten zurückführen. Unter der Annahme, dass die Aufsichten ihre Stellen besetzen können, ist somit mit einer Zunahme aufsichtlicher Kontrollen zu rechnen, die wiederum Ressourcen erfordern.
Angesichts der technologischen Herausforderungen einer weltweit vernetzten Gesellschaft und neuer Gefährdungen durch Cyberkriminalität ist die Wahrung des Rechts auf informationelle Selbstbestimmung wichtiger und aktueller denn je. Heutige Diskussionen machen allerdings auch deutlich, dass immer wieder um eine Balance zwischen Freiheit und Sicherheit gerungen werden muss. Diese Balance müssen sowohl die Verantwortlichen als auch die Datenschutzbeauftragten in ihrer täglichen Arbeit finden, ebenso wie die Betroffenen.
Das Datenschutzrecht ist ein dynamischer, sich im permanenten Wandel befindlicher Prozess. Bestehende Normen müssen immer wieder aufgrund aktueller Entwicklungen und Erkenntnisse Anpassung finden. Sowohl die Gesetzgeber wie auch die Aufsichtsbehörden sind in der Pflicht, dem Recht auf informationelle Selbstbestimmung auch in der globalen Wissens- und Informationsgesellschaft Geltung zu verleihen.
Es bleibt also spannend.

Studiendesign

Die vorliegenden Studienergebnisse sind das Resultat einer Online-Befragung, die zwischen Anfang September und Mitte November 2021 durchgeführt wurde. Nachdem sich die vorherige Curacon-Datenschutzstudie 2018 auf datenschutzrechtliche Gesichtspunkte in deutschen Krankenhäusern fokussierte, wurde die Zielgruppe der Befragung für die aktuelle Studie auf die gesamte Gesundheits- und Sozialwirtschaft erweitert. Auf Datenschutzbeauftragte sowie Entscheidungsträger:innen (d. h. Geschäftsführungen oder Einrichtungsleitungen) beider Wirtschaftszweige zielte die Befragung zur Studie ab. Die Befragungsteilnehmer:innen wurden gebeten, über 40 Fragen zu den verschiedenen Themen der Datenschutzstudie 2022 zu beantworten. Das Ziel der Studie ist dabei, sowohl alte als auch neue datenschutzrechtliche Herausforderungen in der Gesundheits- und Sozialwirtschaft zu beleuchten und somit auch die Komplexität des Datenschutzes in beiden patienten- bzw. klientennahen Branchen abzubilden. Zu diesem Zweck verhilft die Studie u. a. zur Beantwortung der übergeordneten Fragen:

- Wie sind Einrichtungen datenschutzrechtlich organisiert?
- Haben die gestiegenen Anforderungen an den Datenschutz zu einer Veränderung der datenschutzrechtlichen Organisation geführt?
- Welche Aktivitäten führen Datenschutzbeauftragte (regelmäßig) durch?
- Wo entstehen die größten Herausforderungen bei der Umsetzung datenschutzrechtlicher Standards?
- Welche Erfahrungen wurden hinsichtlich der Datenschutzkontrollen im Falle von Datenschutzvorfällen gemacht?

Die Studie fällt auch in die Zeit der omnipräsenten Pandemie, die beide Wirtschaftszweige in besonderem Maße in Atem hält und vor weitere Herausforderungen stellt. Teile der Befragung wurden daher ebenfalls im Lichte der COVID-19-Pandemie und ihrer Auswirkungen durchgeführt.
Insgesamt nahmen 71 Einrichtungen an der Befragung teil. Krankenhäuser als Repräsentanten der Gesundheitswirtschaft und ehemaliger Fokus der Curacon-Datenschutzstudie machen über 50 % der teilnehmenden Institutionen aus. Die weitere Hälfte des Teilnehmer:innenkreises setzt sich aus Einrichtungen der Altenhilfe, der Eingliederungshilfe, Kinder- und Jugendhilfe sowie einem großen Anteil großer Komplexträger zusammen. Weitere in der Sozialwirtschaft ansässige Unternehmen (z. B. Spitzenverbände oder ambulante soziale Dienste) beteiligten sich ebenfalls an der Befragung.
Bezüglich der Trägerschaft wird im Kreis der Teilnehmenden eine starke Akzentuierung im freigemeinnützigen Bereich deutlich. Öffentliche und private Träger bleiben in der Studie unterrepräsentiert, was bei der Interpretation der Befragungsergebnisse berücksichtigt wurde. Aufgrund des katholisch-freigemeinnützigen Schwerpunktes liegt es nahe, dass der überwiegende Teil der Befragten hauptsächlich das Kirchliche Datenschutzgesetz (KDG) nutzt. Das Datenschutzgesetz der Evangelischen Kirche in Deutschland (DSG-EKD) ist mit knapp 20 % jedoch ebenfalls stark vertreten. Die Datenschutz-Grundverordnung (DSGVO) wird überwiegend in 35 % der befragten Institutionen genutzt.

Einrichtungsarten (überwiegend/Rest: Sonstige)

52,9 % Gesundheitswirtschaft

37,1 % Sozialwirtschaft

An der Studie teilnehmende Trägerschaften

67,6 % Freigemeinnützig

davon: 64,6 % Katholisch / 25,0 % Evangelisch / 10,4 % Sonstige

15,5 % Öffentlich / **12,7 %** Privat / 4,2 % Sonstiges

Anzahl Mitarbeiter:innen

54,3 % > 600

18,6 % 200 - 599

27,1 % bis 199 Vollzeitkräfte

Autoren der Studie

Dr. Uwe Günther ist Partner bei Curacon und Geschäftsführer der Sanovis GmbH. Als Diplom-Informatiker, Diplom-Wirtschaftsingenieur und Gesundheitswissenschaftler blickt er auf eine über zwanzigjährige Erfahrung im Consulting bei weltweit führenden Technologie- und Unternehmensberatungen zurück. Mit dieser umfangreichen Branchenerfahrung ist er heute Leiter der Geschäftsfelder IT-Management und Datenschutz sowie Dozent an der EBS Universität für Wirtschaft und Recht.

Johannes Mönter ist Betriebswirt im Gesundheitswesen sowie Fachkraft für Datenschutz (DEKRA). Seine Beratungsschwerpunkte liegen in den Bereichen des konfessionellen Datenschutzes, Datenschutz gemäß Bundesdatenschutzgesetz sowie beim Datenschutz in ambulanten Pflegeeinrichtungen. Seine umfangreiche Erfahrung bringt er u. a. ein beim Aufbau einrichtungsinterner Datenschutzstrukturen inkl. Ausbildung und Coaching der Mitarbeiter sowie als externer Datenschutzbeauftragter.

Stefan Strüwe ist Partner bei Curacon und als Rechtsanwalt (Syndikusrechtsanwalt) externer Betriebsbeauftragter für Datenschutz, Experte für Datenschutz und Risikomanagement sowie Lehrbeauftragter der Mathias Hochschule Rheine und Mitglied im KGNW-Ausschuss IT (Datenschutz). Mehr als zehn Jahre Erfahrung als Rechtsanwalt im Gesundheitswesen machen ihn zum idealen Ansprechpartner, wenn es um Datenschutz- sowie Arzthaftungs- und Betreuungsrecht geht. Neben dem Aufbau einrichtungsinterner Datenschutzstrukturen inkl. Ausbildung und Coaching interner Betriebsbeauftragter bietet er Konzernberatung zur Umsetzung (konfessionellen) Datenschutzes an.

Dr. Uwe Günther
Partner
Leiter Beratungsfeld IT Management
Geschäftsführer Sanovis GmbH
uwe.guenther@curacon.de

Johannes Mönter
Manager
Beratungsfeld Datenschutz
johannes.moenter@curacon.de

Stefan Strüwe
Partner
Leiter Beratungsfeld Datenschutz
stefan.struewe@curacon.de

Co-Autor:innen:

Marco Eck hat einen Abschluss als Master of Arts mit der Vertiefung im Bereich des Gesundheits- und Sozialmanagements. Zudem ist er Datenschutzbeauftragter/ -auditor und Qualitätsmanagementbeauftragter (TÜV Rheinland). Schwerpunkte: Aufbau von DSMS und Datenschutzbegleitung.

Sarah Gindera ist Betriebswirtin im Gesundheitswesen mit Masterabschluss in Medizinmanagement für Wirtschaftswissenschaftler und Fachkraft für Datenschutz (DEKRA). Schwerpunkte: externe Betriebsbeauftragte für Datenschutz, Analyse datenschutzrelevanter Strukturen, DSMS und die datenschutzkonforme Gestaltung von Websites und Social Media.

David Große Dütting ist Manager, hat einen Abschluss als Master of Sciences Public Health (MPH), ist examinierter Gesundheits- und Krankenpfleger sowie Qualitätsmanagementbeauftragter (TÜV Süd) und Fachkraft für Datenschutz (DEKRA). Schwerpunkte: DSMS, spezielle Fragestellungen bei der Nutzung von Websites, Social Media, Instant-Messaging-Diensten und E-Health-Applikationen.

Simon Heitmeier ist Wirtschaftsjurist mit Schwerpunkt auf Compliance, Digitalisierung und Datenschutzrecht sowie Datenschutzbeauftragter (TÜV Nord). Schwerpunkte: DSMS, spezielle Fragestellungen zu datenschutzrechtlichen Anforderungen hinsichtlich Websites und Social Media.

Laura Mosen ist approbierte Tierärztin und zertifizierte Datenschutzauditorin und -beauftragte (TÜV Nord) mit ausstehendem Abschluss in Betriebswirtschaftslehre (B.A.). Schwerpunkte ihrer mehrjährigen Tätigkeit als externe Datenschutzbeauftragte: datenschutzkonforme Einbindung von Dienstleistern, Ausgestaltung von Rollen und Berechtigungen und den Aufbau von DSMS.

Über Curacon

Wir sind eine bundesweit tätige Wirtschaftsprüfungs- und Beratungsgesellschaft mit Spezialisierung im Non-Profit-Bereich. Im Verbund mit der Curacon Rechtsanwaltsgesellschaft mbH, der Krankenhausberatung Jüngerkes & Schlüter GmbH und der Sanovis GmbH betreuen mehr als 450 Mitarbeiter:innen an 14 Standorten über 2.000 Mandanten.

Die Curacon Unternehmensgruppe führt Prüfungs- und Beratungsaufgaben im Gesundheits- und Sozialwesen durch und gehört zu den 20 größten Wirtschaftsprüfungsgesellschaften in Deutschland mit den Schwerpunkten Wirtschaftsprüfung, Steuerberatung, Rechtsberatung und Unternehmensberatung. Mit Blick auf datenschutzrechtliche Themen profitieren unsere Mandanten von unserer umfassenden Expertise gerade mit Blick auf die folgenden Leistungen:

- Erhebung des Datenschutzbedarfs in Audits und Begehungen,
- Aufbau effizienter und praxistauglicher Datenschutzmanagement-Systeme, die sich in bestehende Systeme des Qualitäts- und Risikomanagements einfügen,
- Gestellung externer Datenschutzbeauftragter zur internen Entlastung und zugleich Wahrung der notwendigen und stets aktuellen Fachkunde,
- Schulung und Sensibilisierung zum Datenschutz, ein zentrales Element zur Senkung des unternehmerischen Risikos durch fehlendes Wissen und Fehlverhalten,
- Websiteprüfung, Websitemonitoring und Consent-Management – mit diesem Dreiklang lässt sich ein datenschutzkonformer Webauftritt sicherstellen,
- enge Vernetzung zu allen Fragen der IT-Sicherheit, der Cyber-Security etc. durch unsere Spezialist:innen für IT-Management und IT-Sicherheit, die Sanovis GmbH,
- Expertise zu speziellen Datenschutz-Fragestellungen mit klaren Antworten, schriftlichen Stellungnahmen und damit rechtlicher Sicherheit.

Unsere Spezialisierung auf die Gesundheits- und Sozialwirtschaft, den öffentlichen Sektor sowie die Kirchen mit ihren vielfältigen Besonderheiten zahlt sich gerade hier mit Blick auf den Schutz sensibler Daten besonders aus. Neben umfangreicher Erfahrung sind motivierte, flexible und eigenverantwortlich handelnde Mitarbeiter:innen unsere Stärke und der Schlüssel zum Erfolg. Wir fördern die Weiterentwicklung der fachlichen und sozialen Kompetenz unserer Mitarbeiter:innen durch spezifische Personalentwicklungskonzepte sowie regelmäßige fachbezogene Schulungen. Gegenseitige Wertschätzung, Loyalität und Partnerschaft sowie ein kooperativer Führungsstil in einer durch christliche Werte geprägten Unternehmenskultur sind die Grundlagen unserer Arbeit.

Wir verfügen über ein umfassendes Qualitätsmanagement, das im Rahmen der externen Qualitätskontrolle von unabhängigen Wirtschaftsprüfern geprüft und von der Wirtschaftsprüferkammer kontinuierlich überwacht wird. Die Qualität unserer Leistungen stellen wir somit dauerhaft und nachhaltig für unsere Mandanten sicher.

Nähere Informationen sowie aktuelle Themen und Trends aus der Branche finden Sie unter **www.curacon.de**.

Bestellung

Bei Bedarf leiten wir die Studie gerne auch an andere interessierte Personen weiter. Lassen Sie uns hierzu einfach die Adresse an studien@curacon.de zukommen.

Kontakt

Benötigen Sie zusätzliche Informationen, interessieren Sie sich für eine unserer Studien oder haben Sie weitere Fragen? Dann senden Sie uns gerne eine E-Mail an:
studien@curacon.de

CURACON-Studien im Überblick

Datenschutz zwischen DSGVO und Digitalisierung – Wo stehen wir nach vier Jahren DSGVO?
Eingliederungshilfe und das BTHG – Organisatorische und strategische Umsetzung des Bundesteilhabegesetzes
Controlling in der Sozialwirtschaft – Fokusthemen: Organisation, Personalausstattung, Wirkungscontrolling
Altenhilfebarometer – Besser durch die Pandemie gekommen als befürchtet, aber große Sorge um die Zukunft
Digitalisierung in den Kirchen – Studie zum Status quo und den Treibern der Digitalisierung
Controlling im deutschen Krankenhaussektor – Fokusthemen: Liquiditätssteuerung/Controlling in der Pflege
TCMS-Studie – Mit Tax-Compliance-Management-Systemen sicher landen – in unsicheren Zeiten
Komplexträger-Studie – Personalmanagement, das Schlüsselelement des Wachstums?
BTHG-Studie: Zeit zu handeln!
Öffentlich-Öffentliche Partnerschaften – Experiment oder Erfolgsgarant: gemeinsam auf den Weg in die Zukunft?
BTHG-Studie: Wohnsettings – Stimmungen und Herausforderungen
Studie Führung und Aufsicht: Corporate Governance – die Herausforderung der richtigen Flughöhe
Datenschutzstudie: Krankenhäuser im Spannungsfeld Datenschutz
Krankenhausstudie: Im Verbund erfolgreicher?
Komplexträgerstudie: Scheitern Strategien in der Organisation?

CURACON

Curacon GmbH
Wirtschaftsprüfungsgesellschaft
www.curacon.de

Berlin • Darmstadt • Freiburg • Hamburg • Hannover • Köln • Leipzig • München • Münster • Nürnberg • Ratingen • Rendsburg • Saarbrücken • Stuttgart