Solidaris

Nutzen stiften – mit Freude für Menschen

ARBEITSHILFE

IT-Risiken managen: Anforderungen an das digitale Gesundheitswesen

IT-Sicherheit und Datenschutz
Ein Praxisleitfaden für Verantwortliche

Berlin
Erfurt
Freiburg
Hamburg
Köln
Mainz
München
Münster
Wien (A)
Würzburg

VORWORT

Digitalisierung im Gesundheitswesen bezeichnet im Wesentlichen die Anwendung elektronischer Geräte zur medizinischen Versorgung sowie die Speicherung, Vernetzung und automatisierte Verarbeitung von Informationen. Die fortschreitende Digitalisierung ermöglicht es, schnell und umfassend Informationen zu erhalten, zu strukturieren und zu analysieren und erleichtert den Austausch zwischen den Akteuren der Branche (z. B. Krankenkassen, niedergelassenen Ärzten, Versicherungen). Zusammengefasst wird dieser Zusammenhang oftmals in dem Begriff „E-Health".

Neben diesen Vorteilen bringt die Digitalisierung aber auch neuartige Risiken mit sich. Während die breite Öffentlichkeit erst mit dem massiven Anstieg von Schadsoftware-Angriffen in deutschen Krankenhäusern Anfang 2016 davon Notiz genommen hat, beschäftigt sich der Gesetzgeber schon seit einigen Jahren mit der Frage des Schutzes sogenannter Kritischer Infrastrukturen. Bereits im Juli 2015 ist das Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) in Kraft getreten. Es soll nach dem Willen der Bundesregierung einen Beitrag dazu leisten, die IT-Systeme und digitalen Infrastrukturen in Deutschland sicherer zu machen.

Die Anforderungen, die sich aus dem IT-Sicherheitsgesetz für die Krankenhausbranche ergeben, und konkrete Handlungsempfehlungen zur Umsetzung von geeigneten Maßnahmen zur Erfüllung der entsprechenden Anforderungen bilden einen zentralen Schwerpunkt der vorliegenden Arbeitshilfe.

Mit der Digitalisierung einher gehen auch gestiegene Risiken für die Erhebung, Verarbeitung und Speicherung von digitalen Informationen. Diesen neuen Herausforderungen trägt die ab Mai 2018 anzuwendende EU-Datenschutz-Grundverordnung (DSGVO) Rechnung. Unsere Arbeitshilfe gibt einen Überblick über die wichtigsten Normen und Veränderungen des künftigen Datenschutzes. Ein wesentlicher Schwerpunkt liegt dabei auf dem kirchlichen Datenschutz, denn vor dem Hintergrund der neuen gesetzlichen Vorschriften wird der Datenschutz in den Kirchen künftig wesentlich ernster zu nehmen sein als bislang. Der bisherige Sonderstatus der kirchlichen Körperschaften und Einrichtungen im Hinblick auf den Umgang mit dem Datenschutz wird weitgehend abgeschafft.

Abschließend wollen wir im Rahmen unserer Arbeitshilfe Wege aufzeigen, die es der Unternehmensführung ermöglichen, die gesetzlichen, unternehmensinternen und vertraglichen Regelungen im Bereich der IT-Landschaft umzusetzen. Unternehmen unterliegen zahlreichen rechtlichen Verpflichtungen, deren Nichteinhaltung hohe Geldstrafen und/oder Haftungsverpflichtungen nach sich ziehen kann. Mit dem vorgestellten IT-Compliance-Ansatz dieser Arbeitshilfe soll den Compliance-Anforderungen in der IT – Informationssicherheit, Verfügbarkeit, Datenaufbewahrung und Datenschutz – Rechnung getragen werden.

Die vorliegende Arbeitshilfe kann nur allgemeine Informationen über die vielfältigen Anforderungen und Neuerungen im Zusammenhang mit der Digitalisierung im Gesundheitswesen vermitteln. Daher empfehlen wir, sich je nach der jeweils individuellen Sachlage vertiefend mit bestimmten Sachverhalten zu befassen. Unser multiprofessionelles Team bestehend aus IT-Sicherheitsexperten, Fachjuristen, Revisionsexperten und Datenschützern steht Ihnen hierzu gerne zur Verfügung. Sprechen Sie uns an! Ergänzend informieren wir auf unserer Internetseite www.solidaris.de über aktuelle Entwicklungen zum Thema.

Wir hoffen, dass die vorliegende Arbeitshilfe Ihnen praktische Einsichten bieten wird, und freuen uns auf Ihre Hinweise und Anregungen (s. Kontaktdaten im Impressum, S. 66).

Köln, im Januar 2018

Dr. Rüdiger Fuchs
Sprecher der Geschäftsführung

Inhaltsverzeichnis

I

Konzeption der Arbeitshilfe

Diese Arbeitshilfe richtet sich an Unternehmensverantwortliche, die mit der Aufgabe der Implementierung, Steuerung und/oder Beurteilung von datenschutzrechtlichen bzw. IT-sicherheitstechnischen Themen betraut sind. Wir haben uns zur Erstellung dieser Arbeitshilfe aus mehreren Gründen entschlossen. Einerseits ergeben sich aufgrund der aktuellen Gesetzgebung eine Vielzahl von neuen Anforderungen für Unternehmen hinsichtlich des Datenschutzes (EU-Datenschutzgrundverordnung), der Vernetzung innerhalb des Gesundheitswesens (E-Health-Gesetz) und der IT-Sicherheit (IT-Sicherheitsgesetz). Andererseits stoßen wir bei der Durchführung von IT-Revisionen bzw. IT-Systemprüfungen im Rahmen von Jahresabschlussprüfungen regelmäßig auf inhaltliche Unsicherheiten, insbesondere in der Geschäftsführung sowie in Aufsichtsgremien kleinerer und mittelgroßer Unternehmen. Daraus leiten wir einen Informationsbedarf über die Entwicklungen und Anforderungen im Zusammenhang mit datenschutzrechtlichen und IT-sicherheitstechnischen Themen für diese Unternehmen ab.

Bei der Konzeption der Arbeitshilfe und bei der Auswahl der Inhalte sind wir davon ausgegangen, dass unsere Leserinnen und Leser über keine bis wenige Kenntnisse im Zusammenhang mit den künftigen Anforderungen im Zusammenhang mit den oben genannten Gesetzen verfügen.

Um die Bandbreite der bestehenden und der neuen gesetzlichen Anforderungen aufzuzeigen, stellen wir in Abschnitt II zunächst die einschlägigen rechtlichen Rahmenbedingungen in ihren Grundzügen dar. Dabei liegt der Schwerpunkt auf den neuen datenschutzrechtlichen Anforderungen aus der EU-Datenschutz-Grundverordnung (DSGVO), die ab Mai 2018 anzuwenden ist, sowie auf den Anforderungen und Auswirkungen des IT-Sicherheitsgesetzes auf die Krankenhausbranche. Abschließend werden in diesem Abschnitt die Entwicklungen im Zusammenhang mit der zunehmenden Vernetzung im Gesundheitswesen und dem E-Health-Gesetz dargestellt.

Abschnitt III verdeutlicht die Auswirkungen der Anforderungen des IT-Sicherheitsgesetzes auf die betroffenen Krankenhäuser anhand von Praxisbeispielen. In diesem Zusammenhang formulieren wir konkrete Handlungsempfehlungen hinsichtlich der Umsetzung einer IT-Sicherheitsorganisation innerhalb von Unternehmen und geben einen ersten Einblick in vorbereitende Maßnahmen hinsichtlich einer gesetzlich vorgeschriebenen externen Prüfung zur Umsetzung der Anforderungen des IT-Sicherheitsgesetzes.

Abschließend beschäftigt sich Abschnitt IV mit der Strukturierung, Steuerung und Überwachung der diversen Anforderungen an Unternehmen im Rahmen eines IT-Compliance-Managementsystems.

Im Anhang dieser Arbeitshilfe ist eine Checkliste zur Ermittlung des individuellen Handlungsbedarfs von Unternehmen vor dem Hintergrund der Anforderungen der EU-Datenschutz-Grundverordnung dargestellt. Außerdem finden sich dort eine Liste mit weiterführender Literatur und ein Abkürzungsverzeichnis.

V

Quick Wins

Rechtliche Rahmenbedingungen

Die Komplexität und die zunehmende Bedrohungslage, etwa durch Hackerangriffe auf das Gesundheitswesen, machen den Einsatz von Rahmenwerken und Standards wie die DIN ISO/IEC 27001 oder den BSI-Grundschutz dringend erforderlich. Dementsprechend weisen auch maßgebliche Akteure des Gesundheitswesens wie der Branchenarbeitskreis Gesundheitsversorgung im UP-KRITIS explizit auf den – unabhängig von der gesetzlichen Verpflichtung durch das IT-Sicherheitsgesetz – bestehenden Handlungsbedarf hin. Es empfiehlt sich, vor dem Hintergrund der Anforderungen des IT-Sicherheitsgesetzes und der damit verbundenen Verpflichtung zur Gewährleistung einer einheitlichen branchenspezifischen IT-Sicherheit nach dem Stand der Technik eine Bestimmung des IT-Sicherheitsniveaus innerhalb des eigenen Unternehmens durchzuführen (Gap-Analyse). Die Analyse der informationstechnischen Systeme, Komponenten und Prozesse sollte die unternehmensspezifischen Besonderheiten berücksichtigen, erheben und bewerten und somit einen detaillierten Überblick über den aktuellen Stand der IT-Sicherheit im Unternehmen verschaffen. Auf dieser Basis kann der potenzielle Handlungsbedarf optimal ermittelt werden.

Das Datenschutz-Management ist künftig insbesondere auf effiziente Dokumentations- und Nachweisprozesse auszulegen. Die Umsetzung sollte vom jeweiligen Datenschutzbeauftragten des Unternehmens angestoßen werden. Dabei kann sich die Umsetzung in weiten Teilen an der Datenschutzorganisation nach dem BDSG 2015 orientieren. Angesichts der Komplexität der Anforderungen dürfte bereits jetzt auszuschließen sein, dass der bisherige Aufwand für die Einhaltung des Datenschutzes auch den künftigen Anforderungen genügen wird. Die Rolle des Datenschutzbeauftragten wandelt sich durch die Datenschutz-Grundverordnung mehr zu einer Unterstützungs- und Beratungsinstanz, als dies noch nach dem BDSG der Fall war. Das in der Praxis noch häufig anzutreffende Modell, einen Mitarbeiter neben seinen eigentlichen Aufgaben mit den Datenschutz zu betrauen, ist nicht mehr zweckmäßig und gegebenenfalls sogar fahrlässig. Bisherige Mitarbeiter im Bereich des Datenschutzes werden künftig voraussichtlich die Rolle eines Datenschutzkoordinators übernehmen, wohingegen zum betrieblichen Datenschutzbeauftragten ein im Bereich des Datenschutzes zertifizierter Spezialist und Rechtsexperte bestellt werden wird.

Der Einzug des E-Health-Gesetzes in das Gesundheitswesen und die damit verbundene Digitalisierung sollen durch die Vernetzung der behandelnden Ärzte eine erhebliche Qualitäts- und Effizienzsteigerung erzielen sowie Zeit und Kosten einsparen. Nutzer aus unterschiedlichen Bereichen werden zukünftig an das Netz angeschlossen sein und hochsensible personenbezogene Daten austauschen. Mit Blick auf die verschiedenen Praxissoftwaresysteme und die unterschiedlichen Krankenhausinformationssysteme, die in Deutschland existieren, bringt die flächendeckende Vernetzung über die Telematikinfrastruktur sowohl dem Arzt als auch dem Patienten Vorteile: Die Ärzte haben Zugriff auf die medizinischen Daten und können auf Befunde, Röntgenbilder, verordnete Medikamente und Therapien zugreifen und mit- bzw. weiterbehandelnden Ärzten schnell zur Verfügung stellen. Patientendaten sind damit nicht mehr an ein Praxissoftware- oder ein Kliniksystem gebunden, sondern können mit dem standardisierten IT-System genutzt werden. Berechtigt sind grundsätzlich Ärzte in Praxen und Krankenhäusern, Psychotherapeuten und Apotheker, die über einen Heilberufsausweis verfügen. Zeitnah sollen alle Arzt- und Psychotherapeutenpraxen sowie Krankenhäuser an die Telematikinfrastruktur angeschlossen werden. Erst wenn die entsprechenden Hersteller nachweisen können, dass ihre Produkte die Anforderungen der Gematik erfüllen, dürfen diese in der Telematikinfrastruktur zum Einsatz kommen. Es sollten deshalb ausschließlich von der Gematik zertifizierte Komponenten verwendet werden, um den hohen Sicherheitsstandard insbesondere im Hinblick auf das Thema Datenschutz zu erfüllen.

Kritische Infrastruktur (KRITIS) Krankenhaus

Für den Sektor Gesundheit liegt eine „Handlungsempfehlung zur Verbesserung der Informationssicherheit an Kliniken“ vor, die vom Branchenarbeitskreis Medizinische Versorgung (BAK MV) erstellt worden ist. Hervorzuheben ist in diesem Zusammenhang, dass der BAK MV die Umsetzung der empfohlenen Maßnahmen unabhängig von einer Einstufung als KRITIS durch Überschreiten des Schwellenwertes von 30.000 stationären Fällen im Krankenhaus empfiehlt. Mit den Empfehlungen gehen wichtige Hinweise zur Umsetzung der entsprechenden Maßnahmen einher. In Anbetracht der Komplexität der in Angriff zu nehmenden Veränderungen sowie des aktuellen Umsetzungsstands in der Krankenhausbranche ist der zeitliche Rahmen äußerst knapp bemessen.

Bislang liegt noch kein branchenspezifischer Sicherheitsstandard (B3S) für den Sektor Gesundheit vor. Allerdings ist zu bedenken, dass es keine gesetzliche Verpflichtung gibt, einen entsprechenden Standard zu entwickeln bzw. diesen anzuwenden. Sollte es bis zum Ablauf der Umsetzungsfrist am 30. Juni 2019 keinen branchenspezifischen Sicherheitsstandard für Krankenhäuser geben, muss aller Voraussicht nach auf die vom Bundesamt für Sicherheit in der Informationstechnik zur Verfügung gestellte Orientierungshilfe OH B3S zurückgegriffen werden.

IT-Compliance

Ob eine Organisation ausreichende Vorkehrungen zur Sicherstellung von IT-Compliance ergriffen hat, sollte in einem ersten Schritt zunächst von der Unternehmensleitung analysiert und beantwortet werden. Ein frühzeitiges Einbinden von entsprechenden Spezialisten, zum Beispiel IT-Leitung und – sofern vorhanden – Rechtsabteilung, sind dabei unerlässlich. Zielsetzung sollte die Implementierung eines Gesamtprozesses der IT-Compliance sein. Insbesondere zu Anfang ist eine Einbindung der Unternehmensleitung, vor allem bei der Anforderungsanalyse und der Definition und Festlegung der IT-Strategie, unabdingbar. Hier wird das Fundament für den späteren IT-Compliance-Prozess gelegt und eine entsprechende Festlegung der Rollen und Verantwortlichkeiten vorgenommen. Im Anschluss an die erste Phase zieht sich die Unternehmensleitung wieder aus den operativen Fragestellungen zurück und ist abschließend Adressat einer regelmäßigen Berichterstattung zur IT-Compliance. Im Ergebnis kann, zugeschnitten auf die organisatorischen Erfordernisse, ein angemessenes und wirksames IT-Compliance-Management-System eingerichtet werden, das der Führung und Überwachung von Unternehmensleitung und Aufsichtsgremium unterliegt.

Checkliste: Feststellung des Handlungsbedarfs bei der Umsetzung von DSGVO, KDG und EKD-DSG 2018

	Umgesetzt?	
	Ja	Nein
Informationssicherheitsmanagement-System		
Ein Konzept zur Informations- bzw. IT-Sicherheit gemäß Art. 32 DSGVO / § 26 KDG / § 27 EKD-DSG 2018 existiert.		
Ein Konzept zur Überwachung der Wirksamkeit sämtlicher Maßnahmen der Informationssicherheit existiert.		
Die Prozesse zur Aktualisierung des Konzepts zur Informationssicherheit und der Wirksamkeitsprüfungen sind dokumentiert und wirksam.		
Die Prüfergebnisse der Wirksamkeitsprüfungen sind vollständig dokumentiert.		
Ein Prozess zur Dokumentation aller Sicherheitsvorfälle gemäß Art. 33, 34 DSGVO / §§ 32, 34 KDG / §§ 32, 33 EKD-DSG 2018 ist vorhanden und wirksam.		
Ein Prozess zur Meldung von Sicherheitsvorfällen an die Datenschutzaufsichtsbehörde gemäß Art. 33 DSGVO / § 32 KDG / § 32 EKD-DSG 2018 ist dokumentiert und wirksam.		
Ein Prozess zur Meldung von Sicherheitsvorfällen an die betroffenen Personen gemäß Art. 34 DSGVO / § 33 KDG / § 32 EKD-DSG 2018 ist dokumentiert und wirksam.		
Ein Prozess zur Prüfung von Hardware, Software sowie Services auf Konformität mit der DSGVO / KDG / EKD-DSG 2018 beim Einkauf ist dokumentiert und wirksam.		
Datenschutzmanagementsystem		
Es ist festgelegt und dokumentiert, welche Positionen im Unternehmen für die Überprüfung der Befolgung der Datenschutzvorschriften in jeder Abteilung verantwortlich sind.		
Es ist festgelegt und dokumentiert, für welche Aktivitäten eine datenschutzrechtliche Prüfung erforderlich ist.		
Es ist festgelegt und dokumentiert, für welche Beauftragungen von externen Unternehmen / Dritten eine datenschutzrechtliche Prüfung zu erfolgen hat.		
Ein Datenschutzbeauftragter ist – sofern durch DSGVO / BDSG 2018 / KDG / EKD-DSG 2018 vorgeschrieben – bestellt und verfügt über die notwendige Fachkunde. Er ist frei von Interessenkonflikten.		
Der bestellte Datenschutzbeauftragte ist der Aufsichtsbehörde gemeldet und seine Kontaktdaten sind veröffentlicht worden.		
Ein Prozess zur Bearbeitung von Anfragen betroffener Personen hinsichtlich Auskunft, Berichtigung, Sperrung, Löschung, Datenmitnahme sowie Widerspruch ist dokumentiert und wirksam. Der Prozess erfüllt die Vorgaben von DSGVO/ KDG / EKD-DSG 2018.		
Ein Konzept zur Löschung von nicht mehr benötigten gespeicherten Daten ist vorhanden und wird umgesetzt.		
Für jeden Dienstleister (Auftragsdatenverarbeiter)		
Alle alten und neuen Verträge zur Auftragsdatenverarbeitung erfüllen die Vorgaben von Art. 28 DSGVO / § 29 KDG / § 30 EKD-DSG.		
Es liegen ausreichende Garantien nach Art. 28 DSGVO / § 29 KDG / § 30 EKD-DSG 2018 für jeden Auftragsdatenverarbeiter vor.		
Für jede Betriebsvereinbarung		
Alle geltenden Betriebsvereinbarungen sind konform mit DSGVO / BDSG 2018 / KDG / EKD-DSG 2018.		

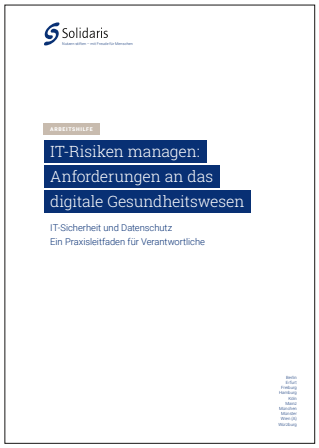
	Umgesetzt?	
	Ja	Nein
Für jede Software und jeden Prozess		
Für jede Programmfunktion und jeden Prozessschritt liegt eine gesetzliche Erlaubnis vor und dies ist dokumentiert.		
In allen Programmen und Prozessen werden ausschließlich für den jeweiligen Zweck erforderliche Datenfelder und Datensätze verarbeitet. Die Erforderlichkeit ist dokumentiert.		
Alle vergebenen Zugriffsrechte sind für die Tätigkeit der Nutzer erforderlich. Die Erforderlichkeit ist dokumentiert.		
Ein Prozess zur Beantragung oder Gewährung von Zugriffsrechten ist dokumentiert und wirksam.		
Ein Prozess zur regelmäßigen Prüfung der Notwendigkeit von vergebenen Zugriffsrechten ist dokumentiert und wirksam.		
Die Ergebnisse der Notwendigkeitsprüfung werden vollständig dokumentiert.		
Prüfungsmechanismen zur Erkennung unberechtigter Zugriffe sind dokumentiert und wirksam.		
In allen Softwareprogrammen (auch von Fremdherstellern) werden ausschließlich Komponenten (z. B. Codebibliotheken) eingesetzt, die nachgewiesenermaßen dem Stand der Technik entsprechen.		
Alle Softwareprogramme und IT-Geräte sind – sofern einschlägig – gemäß den Vorgaben der BSI-Grundschutz-Kataloge oder vergleichbarer Normen konfiguriert.		
Aus allen Softwareprogrammen können die gespeicherten Daten zu einer Person vollständig und in verständlicher Darstellung ausgedruckt werden.		
Aus allen Softwareprogrammen können die gespeicherten Daten zu einer Person vollständig in maschinenlesbarer Form exportiert werden.		
In allen Softwareprogrammen lassen sich Datensätze und Datenfelder einzeln sperren, so dass sie nicht mehr verarbeitet werden können.		
In allen Softwareprogrammen lassen sich Datensätze und Datenfelder sowohl manuell als auch durch automatische Regeln löschen.		
Ein Prozess zur fristgerechten Information des Betroffenen bei der direkten oder indirekten Datenerhebung entsprechend Art. 12 – 14 DSGVO / §§ 14 – 16 KDG / §§ 16 – 18 EKD-DSG 2018 ist dokumentiert und wirksam.		
Für jedes Datenfeld ist als Speicherfrist definiert, wann der letzte Zweck entfallen und eine eventuell bestehende gesetzliche Aufbewahrungsfrist abgelaufen ist.		
In allen Softwareprogrammen, abgelegten Dateien und E-Mails werden personenbezogene Daten unmittelbar nach Ablauf der Speicherfrist gelöscht.		
Nachweisfähigkeit		
Die Tätigkeiten mit Bezug zu personenbezogenen Daten sind festgelegt und dokumentiert. Dazu zählen Prozessbeschreibungen, Richtlinien und Arbeitsanweisungen.		
Ein Prozess zur Aktualisierung der Tätigkeitsfestlegungen ist dokumentiert und wirksam.		
Ein Dokumentationssystem ist etabliert, das erlaubt, die Einhaltung aller Vorschriften von DSGVO / KDG / EKD-DSG 2018 jederzeit nachweisen zu können.		
Alle Zwecke, für die personenbezogene Daten im Unternehmen verarbeitet werden (inkl. Ad-hoc-Auswertungen mit Excel), sind dokumentiert.		
Alle Datenfelder für personenbezogene Daten im Unternehmen sind dokumentiert.		
Alle von einer Datenverarbeitung betroffenen Personengruppen sind dokumentiert.		

Abkürzungsverzeichnis

B3S	Branchenspezifische Sicherheitsstandards
BAK MV	Branchenarbeitskreis Medizinische Versorgung
bDSB	betrieblicher Datenschutzbeauftragter
BDSG	Bundesdatenschutzgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSI-KritisV	Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz
BSIG	Gesetz über das Bundesamt für Sicherheit in der Informationstechnik
COBIT	Control Objectives for Information and Related Technology
DCGK	Deutscher Corporate Governance Kodex
DGK	Diakonischer Corporate Governance Kodex
DIN	Deutsches Institut für Normung
DKG	Deutsche Krankenhausgesellschaft
DSFA	Datenschutz-Folgenabschätzung
DSGVO	Datenschutz-Grundverordnung
DSG-EKD	Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland
DSMS	Datenschutz-Management-System
GKV	Gesetzliche Krankenversicherung
GÜAS	Gemeinsame übergeordnete Ansprechstelle
eGK	elektronische Gesundheitskarte
eHBA	elektronischer Heilberufeausweis
IEC	International Electrotechnical Commission
IoT	Internet of Things
IS	Informationssicherheit
ISACA	Informations Systems Audit and Control Association
ISB	IT-Sicherheitsbeauftragter
ISMS	IT-Sicherheitsmanagement-System
ISO	International Organization for Standardization
IT	Informationstechnik
ITSG	IT-Sicherheitsgesetz
KBV	Kassenärztliche Bundesvereinigung
KDG	Gesetz über den Kirchlichen Datenschutz
KDO	Anordnung über den Kirchlichen Datenschutz
kDL	kritische Dienstleistungen
KRITIS	Kritische Infrastrukturen
KZBV	Kassenzahnärztliche Bundesvereinigung
PIN	Personal Identification Number
PVS	Praxisverwaltungssystem
RMS	Risikomanagementsystem
TI	Telematikinfrastruktur
TKG	Telekommunikationsgesetz
TMG	Telemediengesetz
TOM	technische und organisatorische Maßnahmen
UP-KRITIS	Öffentlich-Private Partnerschaft zum Schutz Kritischer Infrastrukturen in Deutschland
VDD	Verband der Diözesen Deutschlands
VPN	Virtual Private Network
VSDM	Versichertenstammdatenmanagement
VVT	Verzeichnis der Verarbeitungstätigkeiten

Bestellung

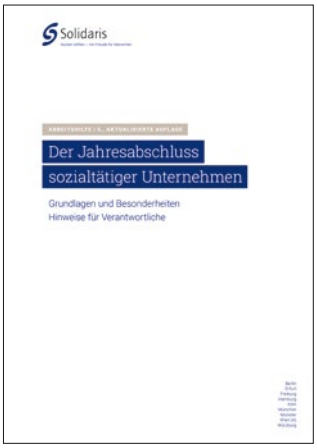
Solidaris Unternehmensberatungs-GmbH
Postfach 92 02 55
51152 Köln
Tel. 02203.8997-0
Fax 02203.8997-199
arbeitshilfe@solidaris.de



Ihre Ansprechpartner zum Thema IT-Sicherheit und Datenschutz

Oliver Schikora
Certified Information Systems Auditor (CISA),
IT-Auditor (IDW), IT-Security-Beauftragter
02203 . 8997-228
o.schikora@solidaris.de

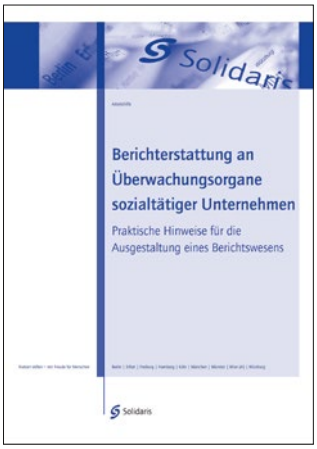
RA Alexander Gottwald, EMBA
Externer Datenschutzbeauftragter (GDDcert. EU)
0251 . 48261-173
a.gottwald@solidaris.de



Ihre Ansprechpartner zum Thema Rechnungslegung und Jahresabschluss

WP StB Dirk Riesenbeck-Müller
02203 . 8997-201
d.riesenbeck-mueller@solidaris.de

WP StB Stefan Szük
02203 . 8997-210
s.szuek@solidaris.de



Ihre Ansprechpartnerin zum Thema Berichtswesen und Berichterstattung

WPin StBin Claudia Dues
02203 . 8997-143
c.dues@solidaris.de

Impressum

Herausgeber

Solidaris Unternehmensberatungs-GmbH
51149 Köln, Von-der-Wettern-Str.11
51152 Köln, Postfach 92 02 55

Je Exemplar wird eine Schutzgebühr in Höhe
von 20,00 EUR inklusive Mehrwertsteuer
zuzüglich Versandkosten erhoben.

Redaktion

Michael Basangeac
Alexander Gottwald
Ingo Kreutz
Ines Martenstein
Ivan Panayotov
Oliver Schikora
Ulf Werheit
Martin Wohlgemuth

02203 . 8997-153
m.basangeac@solidaris.de

Stand: Januar 2018

Satz und Gestaltung

Groba / Pérez Cantó
Kommunikationsdesign, Köln

Druck

Warlich Druck RheinAhr GmbH, Köln

Solidaris

Nutzen stiften – mit Freude für Menschen

UNSERE STANDORTE IN DEUTSCHLAND

Berlin

030.72382-3
berlin@solidaris.de

Erfurt

0361.60106-0
erfurt@solidaris.de

Freiburg

0761.79186-0
freiburg@solidaris.de

Hamburg

040.61136048-0
hamburg@solidaris.de

Köln

02203.8997-0
koeln@solidaris.de

Mainz

06131 . 21136-0
mainz@solidaris.de

München

089.179005-0
muenchen@solidaris.de

Münster

0251.48261-0
muenster@solidaris.de

Würzburg

0931.3041809-0
wuerzburg@solidaris.de