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.

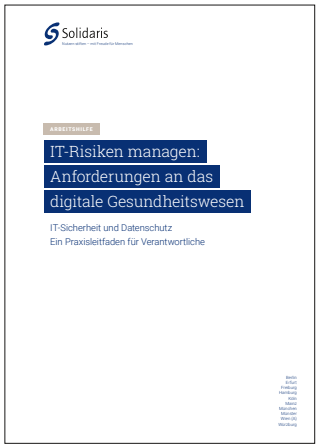
Abschnitt III verdeutlicht die Auswirkungen der Anforderungen des IT-Sicherheitsgesetzes auf die betroffenen Krankenhäuser anhand von Praxisbeispielen. In diesem Zusammenhang formulieren wir konkrete Handlungsempfehlungen hinsichtlich der Umsetzung einer IT-Sicherheitsorganisation innerhalb von Unternehmen 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.

Bestellung

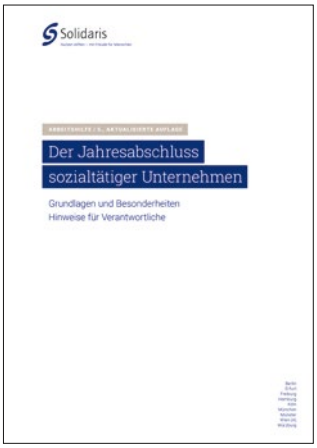
Solidaris Unternehmensberatungs-GmbH
Postfach 92 02 55
51152 Köln
Tel. 02203.8997-0
Fax 02203.8997-199
arbeitshilfe@solidaris.de



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

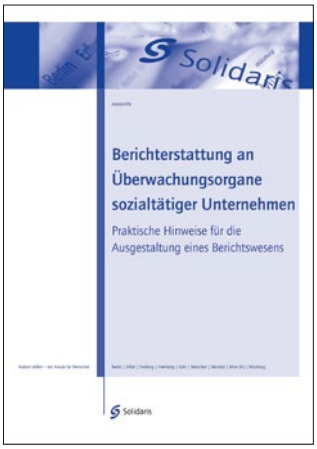
RA Alexander Gottwald, EMBA
Externer Datenschutzbeauftragter (GDDcert. EU)
0251 . 48261-173
a.gottwald@solidaris.de



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

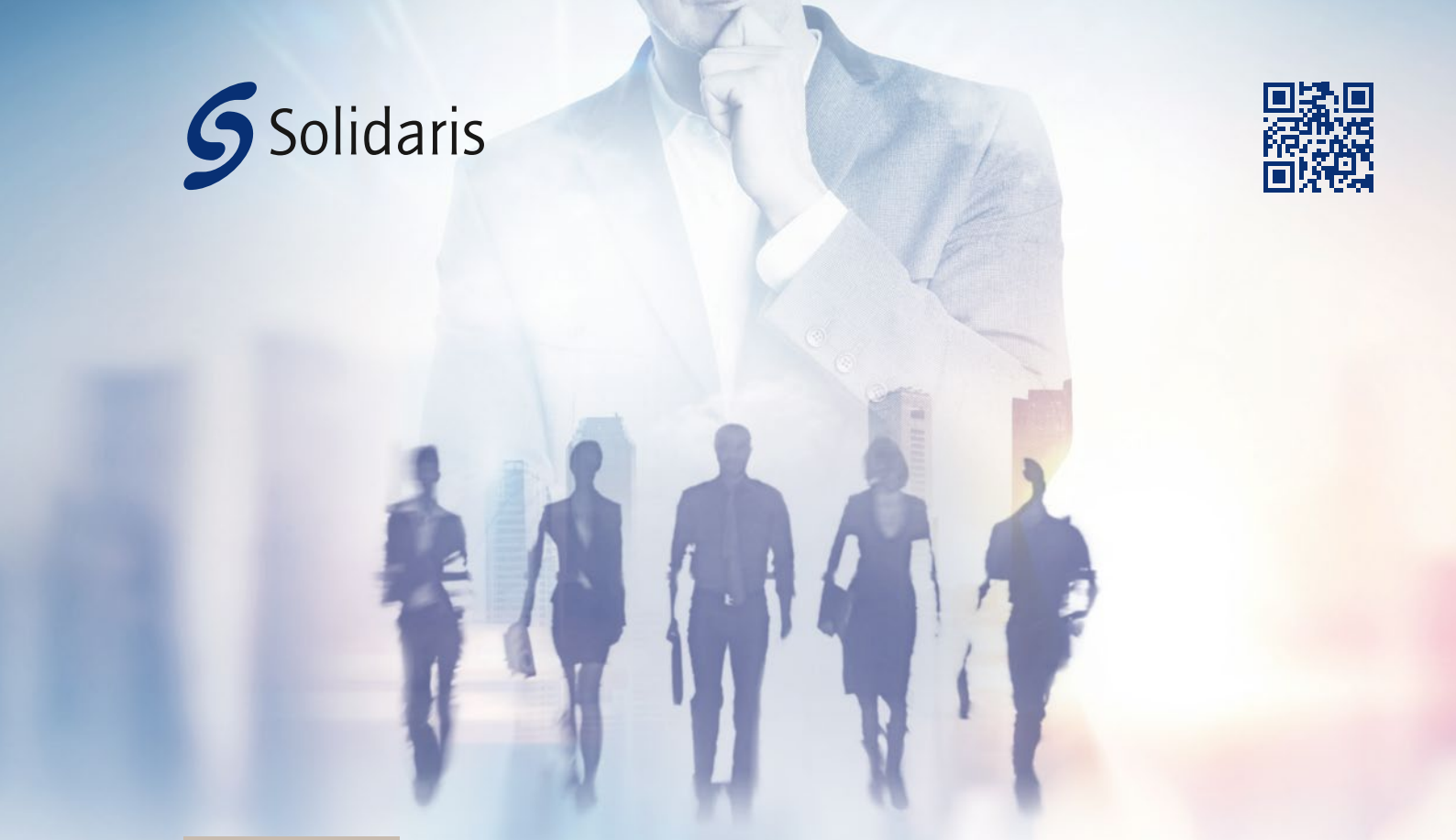
Satz und Gestaltung

Groba / Pérez Cantó
Kommunikationsdesign, Köln

Druck

Warlich Druck RheinAhr GmbH, Köln

Solidaris



SOLIDARIS.DE

Nutzen stiften – mit Freude für Menschen

WIRTSCHAFTSPRÜFUNG

PRÜFUNGSNAHE BERATUNG

STEUERBERATUNG

UNTERNEHMENSBERATUNG

RECHTSBERATUNG

Die Solidaris-Gruppe blickt auf eine über 85-jährige erfolgreiche Geschichte zurück und zählt zu den wenigen Unternehmensverbünden, die auf die Betreuung gemeinnütziger Träger und Einrichtungen des Gesundheits- und Sozialwesens sowie der Freien Wohlfahrtspflege spezialisiert sind. Als führende Prüfungs- und Beratungsgesellschaft in Deutschland bietet die Solidaris an neun Standorten bundesweit zukunftsweisende Expertise in allen wirtschaftlichen und rechtlichen Belangen gemeinnütziger Organisationen unterschiedlicher Größe und Rechtsform aus einer Hand. Sprechen Sie uns an!

02203.8997-0 info@solidaris.de

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

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