# bvitg-Empfehlung zum Umgang mit Servicearbeits-plätzen im Homeoffice

Kontakt:
**Elias Kaiser**

Referent eHealth
elias.kaiser@bvitg.de

Die Mitgliedsunternehmen des Bundesverbandes Gesundheits-IT – bvitg e. V. möchten mit der nachfolgenden Ausarbeitung Empfehlungen zum sicheren Zugriff auf Servicearbeitsplätze im Homeoffice herausarbeiten, welcher den derzeitigen Anforderungen an Datenschutz und IT-Sicherheit gerecht wird. Dabei erfolgt anhand der Darstellung konkreter Problemstellungen eine Definition von Empfehlungen zum sicheren Betrieb von Servicearbeitsplätzen.

Haftungsausschluss: Die nachfolgende Ausarbeitung hat ausschließlich empfehlenden Charakter und dient der fachlichen Orientierung. Sie stellt keine Rechtsberatung dar und kann eine individuelle rechtliche Prüfung im Einzelfall nicht ersetzen.

## 1. Einleitung und Motivation

Im Hinblick auf die steigenden Bedrohungsszenarien durch unbefugte Dritte und den damit einhergehenden Bedarfen zur Reduktion etwaiger Risiken, möchte der bvitg e. V. gemeinsam mit seinen Mitgliedsunternehmen konkrete Empfehlungen für den Zugriff auf Ressourcen (IT-Infrastruktur) definieren, welche den hohen betrieblichen Anforderungen gerecht werden.

Insbesondere bei Tätigkeiten außerhalb der Betriebsstätten besteht häufig die Sorge, dass das Sicherheitsniveau nicht dem Standard im Unternehmen entspricht und dadurch sensible Daten einem erhöhten Risiko ausgesetzt sind.

In einigen Fällen äußern Kunden daher konkrete Anforderungen, wie etwa die Nutzung fester IP-Adressen beim Zugriff durch Dienstleistende, um den Zugriff besser kontrollieren und absichern zu können.

Das Ziel des vorliegenden Papiers ist es, Empfehlungen aufzuzeigen, wie ein hoher Standard der IT-Sicherheit auch bei mobilen beziehungsweise dezentralen Servicearbeitsplätzen gewährleistet werden kann.

## 2. 24/7 Bereitschaft und die steigenden Anforderungen – Verfügbarkeiten/ Reaktionszeiten

Durch sich verändernde Rahmenbedingungen haben neue Arbeitsmodelle, wie das

mobile Arbeiten, zu einer Flexibilisierung der Arbeitsumgebungen geführt. Damit einhergehend wurden neue Möglichkeiten für Arbeitgeber geschaffen, die vertraglich zugesicherten Reaktionszeiten und den 24/7-Bereitschaftsdienst zu gewährleisten. Vor dem Hintergrund einer erwartbaren Zunahme mobiler Arbeit ist es von Bedeutung, sowohl dem Arbeitgeber als auch dem Arbeitnehmer Empfehlungen für den sicheren Betrieb von Servicearbeitsplätzen im Kontext der Telearbeit und des mobilen Arbeitens an die Hand zu geben.

## 3. Mobiles Arbeiten als Wunsch des Mitarbeiters

Mit Blick auf § 106 Abs. 1 GewO stellt der Gesetzgeber Rahmenbedingungen für die Nutzung des mobilen Arbeitens dar. Dazu liegt folgende Definition des Geltungsbereichs vor: „Der Arbeitgeber kann Inhalt, Ort und Zeit der Arbeitsleistung nach billigem Ermessen näher bestimmen, soweit diese Arbeitsbedingungen nicht durch den Arbeitsvertrag, Bestimmungen einer Betriebsvereinbarung, eines anwendbaren Tarifvertrages oder gesetzliche Vorschriften festgelegt sind.“

Damit obliegt es dem Arbeitgeber, die Entscheidung zu treffen, ob Mitarbeitende mobil arbeiten dürfen. Dies führt auch zu der Feststellung des Gesetzgebers, dass es keinen gesetzlichen Anspruch auf mobiles Arbeiten oder Telearbeit gibt.

Gleichzeitig ist zu berücksichtigen, dass die Gesundheits-IT mit zahlreichen Technologieunternehmen um die besten Talente konkurriert. Eine Option zum Arbeiten im Homeoffice wird mittlerweile von einer Mehrheit der Arbeitnehmer als Voraussetzung angesehen, um für ein Unternehmen tätig zu werden/zu sein.

## 4. Definitorische Rahmenbedingungen

### 4.1. Definition mobiles Arbeiten

Eine Legaldefinition für mobiles Arbeiten liegt bisher nicht vor. Eine mögliche Erklärung hierfür ist, dass aktuell kein Anspruch der Arbeitnehmer auf mobiles Arbeiten besteht, da es sich um eine freiwillige Maßnahme des Arbeitgebers handelt, die in Vereinbarung zwischen Arbeitnehmer und Arbeitgeber getroffen wird. Das Bundesministerium für Arbeit und Soziales definiert das Mobile Arbeiten in Abgrenzung zur Telearbeit, wie folgt: „Mobile Arbeit zeichnet sich dadurch aus, dass Arbeitnehmer ihre Arbeit von einem Ort

außerhalb der eigentlichen Betriebsstätte erbringen. Mobile Arbeit kann entweder an einem Ort, der vom Arbeitnehmer selbst gewählt wird oder an einem fest mit dem Arbeitgeber vereinbarten Ort (z.B. Homeoffice) erbracht werden. Mobile Arbeit setzt nicht zwingend die Verwendung von Informationstechnologie voraus.“ [1]

### 4.2. Abgrenzung Telearbeit zu mobiler Arbeit

Der Gesetzgeber definiert Telearbeit in § 2 Abs. 7 der Verordnung über Arbeitsstätten (Arbeitsstättenverordnung – ArbStättV) wie folgt: „Telearbeitsplätze sind vom Arbeitgeber fest eingerichtete Bildschirmarbeitsplätze im Privatbereich der Beschäftigten, für die der Arbeitgeber eine mit den Beschäftigten vereinbarte wöchentliche Arbeitszeit und die Dauer der Einrichtung festgelegt hat. Ein Telearbeitsplatz ist vom Arbeitgeber erst dann eingerichtet, wenn Arbeitgeber und Beschäftigte die Bedingungen der Telearbeit arbeitsvertraglich oder im Rahmen einer Vereinbarung festgelegt haben und die benötigte Ausstattung des Telearbeitsplatzes mit Mobiliar, Arbeitsmitteln einschließlich der Kommunikationseinrichtungen durch den Arbeitgeber oder eine von ihm beauftragte Person im Privatbereich des Beschäftigten bereitgestellt und installiert ist.“ § 2 ArbStättV.

Der Wissenschaftliche Dienst des Deutschen Bundestages erklärt hierzu in seiner Veröffentlichung „Sachstand Telearbeit und mobiles Arbeiten“ vom 10. Juli 2017 Voraussetzungen, Merkmale und rechtliche Rahmenbedingungen: „Hierbei sind verschiedene Organisationsformen denkbar. Unterschieden wird etwa die Teleheimarbeit von der alternierenden Telearbeit. Bei der Teleheimarbeit befindet sich der Arbeitsplatz permanent im Privatbereich des Beschäftigten. Im Rahmen der alternierenden Telearbeit erfolgt ein Wechsel zwischen dem - fest installierten - Arbeitsplatz in der Betriebstätte und dem eingerichteten Arbeitsplatz in der privaten Wohnung.“ [2]

[1] Bundesministerium für Arbeit und Soziales, Homeoffice, URL: https://www.bmas.de/DE/Arbeit/Arbeitsrecht/Teilzeit-flexible-Arbeitszeit/homeoffice.html#doc387a1a0e-79c3-4c4b-a284-ac58a04d62bcbody-Text2 (abgerufen am 19.09.2025).

[2] Wissenschaftliche Dienste des Deutschen Bundestages, Telearbeit und Mobiles Arbeiten, WD 6 - 3000 - 149/16, 2017, URL: https://www.bundestag.de/resource/blob/516470/3a2134679f90bd45dc12dbef26049977/wd-6-149-16-pdf-data.pdf (abgerufen am 19.09.2025).

## 5. Problembeschreibung und Handlungsempfehlung

Im nachfolgenden Abschnitt erfolgt eine konkrete Betrachtung der identifizierten Problemstellungen, um in einem zweiten Schritt konkrete Empfehlungen auszusprechen, die einen sicheren Zugriff über Servicearbeitsplätze ermöglichen.

### 5.1. Technische und Organisatorische Maßnahmen (TOMs) für das mobile Arbeiten und Telearbeit

| Problembeschreibung: |
| --- |
| Der nachfolgenden Betrachtung liegt die Prämisse zugrunde, dass Abweichungen von technischen und organisatorischen Maßnahmen (TOMs) im Unternehmen zum mobilen Arbeiten nur möglich sind, wenn sichergestellt werden kann, dass das vereinbarte Sicherheitsniveau zwischen Arbeitgeber und Arbeitnehmer nicht unterschritten wird. |

Die bestehenden technischen und organisatorischen Maßnahmen werden um gezielte Vorgaben für das mobile Arbeiten ergänzt. Ziel ist es, auch außerhalb des Unternehmens sicherzustellen, dass der Schutz personenbezogener und vertraulicher Daten sowie die IT-Sicherheit auf einem gleichwertigen Niveau wie im Büro gewährleistet werden.

Zu ergreifende Maßnahmen umfassen insbesondere:

- Sichere Anbindung: Verpflichtender Einsatz eines VPN zur verschlüsselten Verbindung mit dem Firmennetzwerk.
- Informationssicherheits-Grundschutz: Vorgabe und Kontrolle aktueller Sicherheitsupdates, aktiver Viren- und Malware-Schutz sowie Firewall für alle eingesetzten Endgeräte.
- Arbeitsmittel: Nutzung ausschließlich vom Arbeitgeber zur Verfügung gestellter Endgeräte; private Geräte nur nach expliziter Freigabe und richtlinienkonformer Absicherung.
- Zugriffsmanagement: Strikte Zugangsbeschränkungen auf die für die Tätigkeit erforderlichen Systeme und Daten.
- Datenspeicherung: Verbot der Speicherung personenbezogener oder

vertraulicher Unternehmensdaten auf privaten Geräten oder Speichermedien.

- Sensibilisierung und Schulung: Regelmäßige Unterweisung der Mitarbeitenden zu Datenschutz und Informationssicherheit im mobilen Arbeiten.
- Arbeitsumgebung: Sicherstellung der Vertraulichkeit (z. B. Sichtschutz bei Bildschirmarbeit, kein unbefugter Zugriff am mobilen Arbeitsplatz durch Dritte.).

### 5.2. Private Internetverbindung

| Problembeschreibung: |
| --- |
| In den privaten Umgebungen ist eine konsequente Trennung zwischen geschäftlichen und privaten Datenbereichen nicht immer möglich. Werden in diesem Kontext berufliche und private Aktivitäten parallel über dasselbe Netzwerk – beispielsweise das gemeinsame WLAN – abgewickelt, sind personenbezogene und unternehmensbezogene Daten erhöhten Risiken wie unbefugtem Zugriff, Datenverlust oder Schadsoftware ausgesetzt. Dies birgt die Gefahr, dass zentrale Anforderungen der DSGVO nicht erfüllt werden. Um diese Risiken zu minimieren, sind gezielte und geeignete Maßnahmen zur Netzwerktrennung zu implementieren. |

Für die sichere Nutzung der privaten Internetverbindung werden folgende Punkte als elementar gesehen:

VPN-Pflicht: Für die berufliche Tätigkeit muss eine *VPN-Verbindung* zum Unternehmensnetzwerk verwendet werden. Damit werden Daten verschlüsselt übertragen und die Verbindung abgesichert.

Firewall aktivieren: Am Router muss eine Firewall aktiviert sein, um unerwünschte Zugriffe auf das Heimnetzwerk zu verhindern.

WLAN-Sicherheit: Das Heim-WLAN muss mit einem komplexen, nicht-erratbaren Passwort gesichert sein und sollte die Verschlüsselung mittels WPA2 (AES-CCMP) oder besser WPA3 verwenden.

Multifaktorauthenifizierung: Für die Anmeldung im Unternehmensnetzwerk ist neben der VPN-Verbindung immer eine Multifaktorauthentifizierung zu verwenden.

### 5.3. BYOD – Regelung und technische Ausstattung (privater Drucker, usw.)

| Problembeschreibung: |
| --- |
| Es ist zu beobachten, dass Unternehmen in jüngerer Vergangenheit vermehrt den Ansatz „Bring Your Own Device“ (BYOD) verfolgen. Aufgrund der Tatsache, dass der Arbeitgeber keine rechtliche Handhabe hat, ein Privatgerät im Rahmen eines Mobile Device Managements (MDM) zu überwachen sowie den Service- und Update-Stand oder installierte Apps zu kontrollieren bzw. einzuschränken, stellt die Verwendung privater elektronischer Geräte ein unkalkulierbares Sicherheitsrisiko dar. Hieraus lässt sich ableiten, dass die Möglichkeit der Überwachung nicht im Interesse des Mitarbeitenden sein kann. |

Bezüglich des Ansatzes „Bring Your Own Device“ wird empfohlen, die Nutzung privat angeschaffter Geräte mithilfe der technischen und organisatorischen Maßnahmen (TOMs) zu untersagen. Diese Empfehlung beruht auf dem Umstand, dass der Einsatz eines MDM nicht zielführend möglich ist und eine „Fernlöschung“ des Geräts im Bedarfsfall nicht durchgeführt werden kann.

Die obige Darstellung verdeutlicht dennoch, dass eine pauschale Aussage nicht ohne Weiteres möglich ist. Daher empfehlen wir an dieser Stelle folgende Zweckbestimmung: Privat angeschaffte Smartphones können für die Durchführung einer Multifaktorauthentifizierung genutzt werden, sofern sichergestellt ist, dass dabei weder Unternehmensdaten noch den Unternehmen von Dritten zur Verfügung gestellte Daten verarbeitet werden. Alle weiteren Geräte sind vom BYOD-Ansatz auszuschließen.

## 6. Kontrollmaßnahmen durch AG, Verantwortlichen (Kunde) und ggfs. Aufsichtsbehörden

| Problembeschreibung: |
| --- |
| Das Kontrollrecht des Arbeitgebers ergibt sich aus Art. 29 DSGVO in Verbindung mit Art. 24 DSGVO. Demnach trägt der Arbeitgeber die Verantwortung für die datenschutzkonforme Verarbeitung personenbezogener Daten durch seine Beschäftigten. Dieses |

| |
|---|
| steht jedoch im Widerspruch zu Art. 13 GG, welcher die Unverletzbarkeit der Wohnung garantiert. Ohne eine vertragliche Zustimmung des Mitarbeiters, kann somit kein Zutritt zu dem privaten Wohnbereich des Mitarbeiters durch den Arbeitgeber erfolgen. Diese Zustimmung kann jedoch durch den Mitarbeiter jederzeit ohne Angabe von Gründen widerrufen werden, was eine Ausübung des Zutrittsrechtes verhindern würde. Hierbei gilt es daher abzuwägen, ob nicht weniger invasive und zielführendere Maßnahmen durch den Arbeitgeber ergriffen werden können. |

Vor diesem Hintergrund wird empfohlen, die Mitarbeitenden ausdrücklich zur Einhaltung der technischen und organisatorischen Maßnahmen (TOMs) im mobilen Arbeiten zu verpflichten und dies mit einer regelmäßigen Schulung zu verbinden. Eine vergleichbare Vorgehensweise findet sich auch im Datenschutz, etwa bei der Verpflichtung auf das Datengeheimnis gemäß DSGVO oder der Verschwiegenheitsverpflichtung nach § 203 StGB.

Ergänzend wird die Prüfung der Möglichkeit einer „digitalen Kontrolle“ empfohlen, die einen grundrechtsschonenderen sowie praktikablen Ansatz darstellt. Ein Beispiel hierfür bietet die Zeit der Corona-Pandemie, in der zahlreiche ISO-Audits virtuell durchgeführt wurden. Es ist anzumerken, dass bei einem virtuellen Audit, eine Anfertigung von Bildaufnahmen der Räumlichkeiten des Arbeitnehmers nicht zulässig ist.

Auch bei digitalen Prüfungen ist es gängige Praxis, dass Auditoren die Arbeitsumgebung per Videoübertragung besichtigen. Hier besitzt der Arbeitgeber zudem ein Weisungsrecht, das er durch eine verpflichtende Kameranutzung ohne größere Schwierigkeiten durchsetzen kann.

### 6.1. Zugang zu Informationen durch Dritte im Haushalt, Hotel, etc.

| Problembeschreibung**:** |
|---|
| Durch die zunehmende Verschmelzung von beruflichen und privaten Kontexten steigt das Risiko, dass unbefugte Dritte Zugang zu regelmäßig genutzten Räumlichkeiten wie dem privaten Haushalt oder dem mobilen Arbeitsplatz erhalten können. Besonders kritisch ist dabei, dass in privaten Räumlichkeiten häufig keine Zugangskontrollen oder abschließbaren Arbeitsplätze vorhanden sind. Unbefugte treffen daher auf deutlich |

| |
|---|
| weniger zugriffserschwerende Maßnahmen als in klassischen Bürogebäuden.<br><br>Um Informationsabflüsse vor diesem Hintergrund auszuschließen, sind technische und organisatorische Schutzmaßnahmen zwingend erforderlich. |

Zur Reduzierung der möglichen Risiken können folgende Maßnahmen ergriffen werden:

- Schutzfolie: Die Nutzung einer Schutzfolie (Blickschutzfolie) auf dem Laptop, um den Bildschirm vor neugierigen Blicken zu schützen und die Vertraulichkeit sensibler Daten zu gewährleisten. Die Folie verhindert, dass Unbefugte von der Seite Einblick auf die Bildschirminhalte erhalten und trägt so aktiv zum Datenschutz bei.
- Bildschirmschoner mit Passwortschutz: Entsprechend des BSI-Grundschutzes wird ein Bildschirmschoner mit Passwortschutz, der automatisch aktiviert wird, sowie eine Passwortabfrage bei Reaktivierung empfohlen.
- VPN Split Tunneling: Im Rahmen dieser Sicherheitsmaßnahme ist der Einsatz von Split Tunneling strikt untersagt. Das bedeutet:
  - Sämtlicher Netzwerkverkehr (ohne Ausnahme) muss durch den aktiven VPN-Tunnel geleitet werden.
  - Es ist nicht gestattet, Verbindungen ins Internet parallel oder außerhalb des VPN zu nutzen.
  - Die gleichzeitige Nutzung lokaler Netzwerkressourcen und direkter Internetzugriffe außerhalb des VPN ist zu unterbinden.

## 7. Definition von NoGo-Areas von Telearbeit und mobilem Arbeiten

| Problembeschreibung: |
|---|
| Durch die zunehmende Flexibilisierung der Arbeitsorte steigt auch die Wahrscheinlichkeit, dass unterwegs über öffentliche WLAN-Netzwerke wie an Flughäfen, in Hotels, Restaurants oder ähnlichen Orten auf die IT-Ressourcen des Unternehmens |

| |
|---|
| zugegriffen wird. |

Die für das mobile Arbeiten erforderlichen Arbeitsunterlagen dürfen nur mit Zustimmung der vorgesetzten Person an einen anderen Ort mitgenommen werden. Sie sind verschlüsselt oder in verschlossenen Behältnissen zu transportieren.

Die Nutzung öffentlich zugänglicher WLANs (z. B. in Cafés, Restaurants, Schwimmbädern, Bahnhöfen, Flughäfen etc.) zum Arbeiten ist grundsätzlich ausgeschlossen. Eine Ausnahme besteht lediglich für WLANs in Hotelzimmern; in diesem Fall ist zwingend eine VPN-Verbindung zu verwenden.

Für dienstliche Gespräche ist zu beachten, dass keine unbefugten Dritten Kenntnis vom Inhalt erlangen dürfen. Beispielsweise: Telefonate in der Bahn oder an Orten, wo die Vertraulichkeit nicht gewährleistet werden kann.

### 7.1. Standard für Arbeitsumgebung inkl. Arbeitszimmer

| Problembeschreibung**:** |
|---|
| Die Vermischung von Privatleben und Beruf ist die größte zu lösende Aufgabe im Arbeitszimmer. Der Küchentisch ist eben kein Arbeitszimmer und so bedarf es klarer Regeln und wenn möglich auch eines abschließbaren Raumes. Arbeitsunterlagen sind, wenn nicht benötigt, in einem Schrank zu verschließen. Die Checkliste[3] der deutschen gesetzlichen Unfallversicherung stellt eine gute Arbeitshilfe zur Arbeitsumgebung, Arbeitsmitteln, Arbeitsorganisation und zum Arbeitsplatz dar. Die Sensibilisierung der Mitarbeiter beim mobilen Arbeiten und im Homeoffice kann über Schulungen und Vereinbarungen zwischen dem Arbeitgeber und den Mitarbeitern erfolgen. |

Für die verbindliche Festlegung von Standards durch den Arbeitgeber wird empfohlen, die anerkannten Regelungen den Mitarbeitenden in Form einer Betriebs- oder Zusatzvereinbarung zur Verfügung zu stellen. So kann ein unternehmenseinheitliches Vorgehen definiert und gefördert werden.

[3] Deutsche Gesetzliche Unfallversicherung e.V., Praxishilfe Homeoffice, 2022, URL: https://publikationen.dguv.de/widgets/pdf/download/article/4019 (abgerufen am 19.09.2025).

## 8. Rechtliche und vertragliche Empfehlungen

Gemäß Art. 24 DSGVO legt der Verantwortliche „unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt."

Somit sind die TOMs für das mobile Arbeiten oder bei der Telearbeit durch den Arbeitgeber festzulegen. Abweichungen von diesen Vorgaben müssen zwingend durch den Arbeitgeber genehmigt werden. Bei der Verarbeitung personenbezogener Daten im Auftrag richten sich die TOMs zudem nach den im Auftragsverarbeitungsvertrag (AVV) gemäß Art. 28 DSGVO vereinbarten Maßnahmen, die auch im mobilen Arbeiten Anwendung finden müssen. Empfehlenswert wäre demnach eine Ergänzung der TOM zu den AV-Verträgen zwischen Verantwortlichem und Auftragsverarbeiter.

Zudem möchten wir an dieser Stelle auf den vom BSI bereitgestellten Grundschutzkatalog hinweisen, insbesondere auf den Baustein OPS 1.2.4[4], der ebenfalls technische und organisatorische Anforderungen an die Telearbeit beschreibt.

## 9. Ausblick und Zusammenfassung

Abschließend lässt sich festhalten, dass das mobile Arbeiten aus der heutigen Arbeitswelt nicht mehr wegzudenken und in den heimischen Büros endgültig angekommen ist. Dieser Umstand macht es erforderlich, dass Arbeitgeber geeignete Maßnahmen ergreifen, um mögliche Risiken bei der Nutzung von Servicearbeitsplätzen zu reduzieren.

Dazu zählen insbesondere technische und organisatorische Maßnahmen (TOMs) sowie entsprechende Regelungen im Auftragsverarbeitungsvertrag, die einen sicheren Zugriff auf Kundensysteme gewährleisten. Ein Beispiel hierfür ist die verpflichtende Nutzung eines VPN ohne Split-Tunneling. Ergänzend können vertragliche Regelungen zwischen

[4] Bundesamt für Sicherheit in der Informationstechnik, OPS.1.2.4 Telearbeit, 2021; URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2022/04_OPS_Betrieb/OPS_1_2_4_Telearbeit_Edition_2022.pdf?__blob=publicationFile&v=3 (abgerufen am 19.09.2025).

Arbeitgeber und Arbeitnehmer, wie beispielsweise in der Form von Betriebsvereinbarungen, helfen, die den möglichen Rahmen zur Durchführung des mobilen Arbeitens darstellen.

Zusätzlich werden Empfehlungen zum Thema „Bring Your Own Device“ (BYOD) ausgesprochen: Die Nutzung privater Geräte ist unzulässig, sofern auf diesen Kunden- oder Firmendaten verarbeitet werden. Eigene Geräte dürfen jedoch für den alleinigen Zweck der Multi-Faktor-Authentifizierung eingesetzt werden.

Der Bundesverband Gesundheits-IT – bvitg e. V. steht seinen Mitgliedsunternehmen zur Stärkung der IT-Sicherheit im Gesundheitswesen als kompetenter Ansprechpartner zur Verfügung.

## 10. Danksagung

Besonderer Dank gilt an dieser Stelle den Personen, die an dieser Ausarbeitung mitgewirkt haben:

- Christoph Isele (Oracle Health)
- Marc Sittler (Oracle Health)
- Jens Schreiber (medatixx GmbH & Co KG)
- Philipp Barschkies (Solventum Germany GmbH)
- Christof Schelian (RpDoc Solutions GmbH)