DATENSCHUTZ & DATENSICHERHEIT

PROJEKTPARTNER

Universität Bremen

iaw
Institut Arbeit und Wirtschaft
Universität / Arbeitnehmerkammer Bremen

wisoak
KOMPETENZZENTRUM GESUNDHEIT & SOZIALES
Wirtschafts- und Sozialakademie der Arbeitnehmerkammer Bremen gGmbH

Qualitus

DIE JOHANNITER
Aus Liebe zum Leben

Bremer Pflegedienst

www.kolegeprojekt.de

Das Forschungs- und Entwicklungsprojekt KoLeGe wird im Rahmen des Programms „Zukunft der Arbeit" (Förderkennzeichen 02L15A010) vom Bundesministerium für Bildung und Forschung (BMBF) und dem Europäischen Sozialfonds (ESF) gefördert und vom Projektträger Karlsruhe (PTKA) betreut. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei den Autor*innen.

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung
ESF Europäischer Sozialfonds für Deutschland
EUROPÄISCHE UNION
Zusammen. Zukunft. Gestalten.

PROJEKTBESCHREIBUNG

VERBUNDPROJEKT
KoLeGe
INTERAGIEREN • KOORDINIEREN • LERNEN
Chancen und Herausforderungen der Digitalisierung in der ambulanten Pflege

Die ambulante Pflege vollzieht derzeit eine umfassende Digitalisierung ihrer Arbeits- und Kommunikationsprozesse. Diese besteht schwerpunktmäßig aus dem Einsatz von PC und Netzwerktechnik in den Pflegezentralen, umfasst zunehmend aber auch sog. »digitale Tourenbegleiter«. Das sind mit spezieller Software ausgestattete Tablets oder Smartphones, die auf den Touren der Pflegekräfte mit den Pflegezentralen verbunden sind und zu verschiedenen Zwecken eingesetzt werden. Der gängige Einsatz der Geräte und Software ist bisher stark auf die Unternehmensanforderungen zum Beispiel einer effizienten Pflegeorganisation [v. a. Tourenplanung, Leistungsdokumentation] ausgerichtet. Die Ansprüche der Pflegekräfte an gute Arbeitsqualität werden oft noch zu wenig berücksichtigt. Das kann zu Akzeptanzproblemen führen, obwohl der Einsatz digitaler Medien in der ambulanten Pflege viele Möglichkeiten bietet, die Arbeit für Pflegekräfte zu erleichtern.

Projektziele: Gute Arbeitsqualität und Arbeitsorganisation miteinander verbinden

Das Verbundprojekt KoLeGe strebt an, die Potenziale zu heben, die in der Digitalisierung der ambulanten Pflege liegen. Die Einführung digitaler Tourenbegleiter wird beteiligungsorientiert als eine soziale Innovation gestaltet, in der Effizienz und gute Arbeitsqualität miteinander verbunden werden. Im Zentrum stehen dabei das digital gestützte Kommunizieren, Informieren und Lernen

Praxisorientierte Arbeitsforschung.

Das Projekt verortet sich in der praxisorientierten Arbeitsforschung, in der Praxis, Wissenschaft und weitere Entwicklungspartner eng kooperieren und voneinander lernen. In jedem Arbeitsschritt werden die unterschiedlichen Belange aller Beteiligten in der Praxis möglichst umfassend berücksichtigt. Denn digitale Technik wird nur dann angenommen werden, wenn sie alle Beteiligten in der Praxis als Gewinn einschätzen, gerne nutzen wollen und gut nutzen können. Im Vordergrund steht dabei nicht die technische Machbarkeit, sondern die Nutzbarkeit der Technik für die Praxis und damit die Frage: wie kann Technik der Praxis helfen?

INHALTSVERZEICHNIS

LESEHILFE

LEITFADEN 1

LEITFADEN 2

LEITFADEN 3

LEITFADEN 4

LEITFADEN 5

LEITFADEN 6

ANHÄNGE

EINFÜHRUNG

Aufbau

Die Arbeit in den sozialen Dienstleistungen wird zunehmend digitalisiert. Das betrifft alle Bereiche, auch die Gesundheitsdienstleistungen und auch die Arbeit am und mit Menschen. Diese Leitfadensammlung soll Sie in der Praxis bei der Gestaltung des Digitalisierungsprozesses unterstützen. Die Praxisempfehlungen kommen aus der ambulanten Pflege und richten sich auch zuerst an die ambulante Pflege. Die Empfehlungen sind aber für die personengebundenen sozialen Dienstleistungen insgesamt und insbesondere für alle ambulanten Dienste verwertbar. Sie richten sich an Führungskräfte und an das interessierte Fachpersonal.

Alle Kapitel sind nach einem einheitlichen Muster aufgebaut und geben eingangs Hinweise auf **Chancen**, die Digitalisierung bietet. Dabei geht der zentrale Ansatz von der Stärkung vorhandener Ressourcen und einer Reduktion von Belastungen im Arbeitsalltag aus. Aber auch **Herausforderungen**, die Digitalisierung für einzelne Bereiche birgt, werden dargestellt. Im Anschluss geben wir Ihnen praktische Tipps für die Umsetzung von Digitalisierungsprozessen **(Vorgehen)**. Eine innere Strukturierung ergibt sich aus der Darstellung der zu beachtenden Schritte mithilfe des PDCA-Zyklus. Die Phasen PLAN, DO, CHECK, ACT bedeuten in unserem Kontext von Digitalisierungsprozessen:

- Alle vorbereitenden Maßnahmen werden im Prozessschritt PLAN festgehalten,
- die Umsetzung unter DO.
- Evaluationsschritte werden unter CHECK angesprochen und
- die nachhaltige Sicherung des Einsatzes digitaler Mittel unter ACT.

Wichtig ist dabei, dass es sich nicht um eine trennscharfe und einmalige Maßnahmenkette handelt. Im Gegenteil: die langfristig erfolgreiche Umsetzung von organisatorischen Veränderungen, die z. B. mit Digitalisierung einhergehen, erfordert immer wieder das kritische Prüfen der laufenden Prozesse, der aktuellen Neuerungen und noch nicht entdeckter Potenziale. Außerdem sind die genannten Phasen miteinander verschränkt. Die Evaluation, die mit der Einführung neuer Technik einhergehen sollte, betrifft einerseits die erste Umsetzung (DO), andererseits aber auch eine klassische Überprüfung (CHECK).

In jedem Leitfaden werden auch **Stolpersteine** dargestellt, die Digitalisierungsprozesse trotz umfassender Vorkehrungen scheitern lassen können. Diese können je nach Einsatzfeld und Umfang von Digitalisierungsprozessen unterschiedlich ausfallen. Schließlich finden Sie unter **Instrumente** Verweise auf zentrales hilfreiches Handwerkszeug (wie z. B. Checklisten zum Thema), das wir online auf der Projektseite www.kolegeprojekt.de zur Verfügung stellen.

Quick Guide

Die einzelnen Themenfelder, die uns in Zusammenhang mit der Digitalisierung sozialer Dienstleistungsunternehmen besonders wichtig erscheinen **(Grundlagen, Datenschutz und Datensicherheit, Kommunikation, Nutzerfreundlichkeit, Kompetenzen, Lernmanagement)**, werden in einzelnen Leitfäden vorgestellt, sodass Sie sich – je nach Interesse – einen schnellen Überblick über den jeweiligen Bereich verschaffen können. Zwischen den Bereichen gibt es allerdings Überschneidungen. Diese werden durch Querverweise zu den entsprechenden Kapiteln verdeutlicht.

Zentrale Botschaften werden vom Text abgesetzt in Merkkästen dargestellt. Darüber hinaus soll die Verwendung der folgenden Icons einer schnellen Orientierung in den Leitfäden dienen:

Querverweise

Merkkasten

Zielsetzung

Wir wünschen Ihnen viel Freude beim Lesen und hoffen, Sie mit den vorliegenden Leitfäden unterstützen zu können!

Datensicherheit

Datenschutz

DATENSCHUTZ UND DATENSICHERHEIT

Das vorliegende Kapitel verschafft Ihnen Klarheit darüber, was der Unterschied zwischen Datenschutz und Datensicherheit ist. Es hilft Ihnen, „Beschäftigten-Datenschutz“ von „Kund*innen-Datenschutz“[1] zu unterscheiden und bei Ihnen sowie den Beschäftigten Sensibilität und Verständnis für sensible Daten zu schaffen. Die Handlungssicherheit Ihrer Beschäftigten wird dadurch gefördert.

Zusammenfassung

Der Umgang mit sensiblen Daten gehört in den sozialen Dienstleistungen zum Alltag. In der Pflege beispielsweise gehören alle Informationen über Patient*innen zu „sensiblen Daten“ – von Namen, Telefonnummern und Adressen über Diagnosen bis zu Schichtzuteilungen der Kolleg*innen. Auch ist mit dem Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) im Mai 2018 das Thema Datenschutz wieder mehr in den Fokus getreten.

Datenschutz und Datensicherheit sind aber nicht nur aus rechtlichen Gründen in einem Digitalisierungsprozess zu beachten. Auch die Handlungssicherheit Ihrer Mitarbeiter*innen steigt, wenn Sie darüber informieren, welche Daten schützenswert sind, was auf welchem Weg kommuniziert und erfasst werden darf – und was nicht.

Das Kapitel soll jedem Unternehmen und jedem bzw. jeder Beschäftigten die Relevanz dieses Themas aufzeigen und Möglichkeiten an die Hand geben, „datenschutzkonform“ digital zu werden.

Orientierung

Datenschutz und Datensicherheit bedingen einander. Daten*schutz* hat eine eher personelle Perspektive, bei der es darum geht, dass nur berechtigte Personen bestimmte Daten nutzen können und diese vertraulich behandeln sollten. Daten*sicherheit* hat eine eher technische Perspektive, bei der es darum geht, Daten technisch vor unbefugtem Zugriff zu schützen. Es sind stets drei Ebenen zu beachten: Ihr Unternehmen, Ihre Beschäftigten und Ihre Kund*innen. Ihr Unternehmen definiert und nutzt dabei verschiedene zu beachtende Rahmenbedingungen.

Datenschutz und Datensicherheit hängen zusammen, haben aber einen unterschiedlichen Fokus:

Datenschutz dient dem (Zugriffs-)Schutz von personenbezogenen Daten. Datenschutz soll sicherstellen, dass personenbezogene Daten vertraulich behandelt werden und nur von dazu berechtigten Personen eingesehen werden können. *Leitfrage: Darf Person X die Daten verarbeiten?*

[1] In Zusammenhang mit datenschutzrechtlichen Betrachtungen wird in der Regel von „Kund*innen“ gesprochen. Daher übernehmen wir in diesem Kapitel ebenfalls diese Begrifflichkeit, die hier Patient*innen betrifft sowie in einigen Fällen auch ihre Angehörigen, da in der Regel auch diese vom guten Umgang mit Daten überzeugt sein müssen.

Datensicherheit umfasst alles, was die Sicherheit bereits erfasster Daten betrifft, z. B. Software zur Verschlüsselung von Daten oder Virenscanner. Leitfrage: *Wie können die Daten vor unbefugtem Zugriff geschützt werden?*

Beides gilt für zwei Arten von Daten: Die Ihrer Mitarbeiter*innen und die Ihrer Kund*innen. Ersteres bezeichnet man als *Beschäftigten-Datenschutz* bzw. *-sicherheit*, letzteres als *Kund*innen-Datenschutz, bzw. -sicherheit.*

Chancen

Chancen ergeben sich bei den Themen Datenschutz und Datensicherheit auf drei Ebenen: für Mitarbeiter*innen, für Kund*innen und für das gesamte Unternehmen.

*Handlungssicherheit bei Ihren Mitarbeiter*innen*

Erstens können Schulungen und klare Regelungen die Handlungssicherheit ihrer Mitarbeiter*innen verbessern. Die Mitarbeiter*innen können bei genügend Informationen vorhandene und neue Technik nutzen, ohne Angst etwas Falsches oder gar Strafbares zu tun. Dies bezieht z. B. die Frage ein, welche Technik oder Software für welche Art von Kommunikation genutzt werden sollte oder darf. Zudem schafft die intensive und transparente Auseinandersetzung mit Datenschutz und Datensicherheit auch bei Ihren Mitarbeiter*innen Vertrauen, dass mit ihren eigenen Daten vernünftig umgegangen wird – also z. B. dass keine Daten erhoben werden, die dann für Beurteilungen verwendet werden.

*Vertrauen bei Ihren Kund*innen*

Zweitens gilt dies in ähnlicher Form auch für Ihre Kund*innen: Wenn Sie diesen genau sagen, welche Daten wozu verwendet werden – Sie die Themen Datenschutz und Datensicherheit also transparent behandeln – wächst das Vertrauen bei Kund*innen, dass sie ihre Daten in guten Händen wissen.

Sicherheit für Ihr Unternehmen

Und drittens erhöht sich für Ihr Unternehmen die Sicherheit, dass es nicht aus Unwissenheit der Mitarbeitenden rechtswidrig handelt oder dass es rechtswidrig gegenüber den Mitarbeitenden handelt. Für Pflegedienste ist z. B. die Frage relevant, ob und wie Daten über Erkrankungen und Diagnosen der Kund*innen gespeichert und verarbeitet werden dürfen. Denn: Bei Verstößen gegen die DSGVO drohen Unternehmen Bußgelder, und Verstöße müssen öffentlich angezeigt werden. So geraten Unternehmen, die es mit dem Datenschutz nicht so genau nehmen, schnell in Verruf und können dadurch sowohl Kund*innen wie auch Beschäftigte verlieren.

Herausforderungen

Herausforderungen bestehen v.a. darin, Datenschutz und Datensicherheit in die Praxis Ihres Unternehmens zu bringen und alle Beteiligte für deren Wichtigkeit zu sensibilisieren.

Hiermit verbunden ist möglicherweise eine Abkehr von alten Handlungsroutinen; Führungskräfte und Beschäftigte müssen

ihre Gewohnheiten durchbrechen und als sicher empfundene Handlungen zugunsten von Ungewohntem aufgeben.

So können zu wenige Informationen zu dem Thema bei Mitarbeiter*innen zu Unsicherheit führen, ob und welche Informationen auf welchem Weg kommuniziert und verarbeitet werden dürfen. Dies führt mitunter dazu, dass Informationen, die nicht verarbeitet werden dürfen, trotzdem verarbeitet werden. Oder: nicht gesicherte Kommunikationswege werden genutzt (z. B. herkömmliche Messengerdienste), bei denen nicht klar ist, wie die Informationen übermittelt oder wo sie gespeichert werden.

Im Gegensatz dazu werden Informationen ggf. lieber persönlich weitergegeben, was die Schnelligkeit und Genauigkeit der Kommunikation bremsen kann. KAPITEL KOMMUNIKATION

Herausforderungen sind daher
- alle Beteiligten transparent zu informieren,
- das Vereinbarte in verbindlichen Regeln festzuhalten und
- die Einhaltung dieser Regeln zu beobachten.

Hierbei kann die Nennung von verschiedenen Ansprechpartner*innen eine Hilfe sein, die sich mit den Themen auskennen und den Beschäftigten zur Seite stehen.

Eine weitere Herausforderung ist, dass die Beachtung von Datenschutz und Datensicherheit den Umgang mit Daten zwar sicherer, aber mitunter weniger nutzerfreundlich macht.

So macht z. B. die Nutzung von Akronymen statt Klarnamen von Patient*innen die Übermittelung sensibler Daten gegen das Auslesen Außenstehender sicherer, allerdings ist das Hantieren mit Akronymen für Beschäftigte zunächst umständlich. Umständlichkeit kann aber zu Ablehnung bei den Beschäftigten führen – wir empfehlen daher, entsprechende Regelungen klar zu begründen, einfach zu halten und den Beschäftigten Hilfen im täglichen Umgang anzubieten.

Vorgehen

Für die Daten Ihrer Mitarbeiter*innen gilt: Sie als Arbeitgeber dürfen auch ohne Einwilligung der Mitarbeiter*innen solche personenbezogenen Daten verarbeiten, die für die Durchführung, Beendigung oder Aufnahme eines Dienstverhältnisses erforderlich sind. Belassen Sie es bei den wirklich notwendigen Daten, so tragen Sie zu einem guten Vertrauensverhältnis bei, das Ihre Beschäftigten zum Unternehmen und seinen Führungskräften haben.

Für Ihre Kund*innen gilt: Sie als Unternehmen dürfen all jene personenbezogenen Daten erheben und verarbeiten, die mit Vertragsabschluss und -erfüllung in Zusammenhang stehen. In einem ambulanten Pflegedienst fallen hierunter z. B. auch Adressinformationen. Aber: Informationen über Gesundheit zählen zu den besonderen Arten personenbezogener Daten und sind durch den Datenschutz besonders geschützt. Die Speicherung von Patient*innendaten ist nur dann zulässig, wenn die/der Betroffene dem Vorgang zugestimmt hat und/oder die Erhebung gesundheitliche Interessen der/des Betroffenen verfolgt.

PLAN

Die Verantwortlichen eines Unternehmens müssen zunächst einen Überblick über Datenschutz und Datensicherheit in der täglichen Arbeit ihrer Mitarbeitenden haben. Ein erster Ansatzpunkt dafür sind interne oder externe Datenschutzbeauftragte, die zu Beginn der Digitalisierung und in der laufenden Nutzung zu Rate gezogen werden sollten. Wichtig ist, dass Sie bei allen Daten, die verarbeitet werden, hinterfragen, ob die Daten tatsächlich benötigt werden. Das kann von Pflegedienst zu Pflegedienst unterschiedlich sein.

Ein Beispiel ist hier das Geburtsdatum der Beschäftigten. Bei mit digitalen Medien erworbenen Zertifikaten/Teilnahmebescheinigungen im E-Learning KAPITEL LERNMANAGEMENT kann es sinnvoll sein, dieses auf dem Zertifikat mit ausgeben zu lassen. Wenn Sie das Geburtsdatum bisher nicht auf Zertifikaten oder Teilnahmenachweisen nutzen, besteht auch keine Notwendigkeit, durch die Möglichkeiten der Digitalisierung hieran etwas zu ändern.

Orientieren Sie sich auch an Ihren bisherigen Prozessen. Nur weil sich durch die Digitalisierung neue Möglichkeiten ergeben, müssen Sie diese nicht zwangsweise nutzen.

Identifizieren Sie eine Person im Unternehmen, die über aktuelle Gesetzeslagen informiert bleibt und bei Bedarf notwendige Maßnahmen einleitet. Zusätzlich sollten Sie eine Person identifizieren, die die Datenschutzeinstellungen von Software und Geräten regelmäßig überprüft, sowie eine Person, die als Ansprechpartner*in für Zugriffsbeschränkungen durch persönliche Zugänge mit Passwort zur Verfügung steht. Diese drei Aufgaben können, müssen aber nicht von derselben Person durchgeführt werden. Definieren Sie diese Aufgaben am besten als weitere Zuständigkeiten vorhandener Ansprechpartner*innen wie IT-Verantwortlichen oder schon vorhandene Datenschutz-Beauftragten – so fällt es ihren Mitarbeiter*innen auch leichter, den/die Ansprechpartner*in anzusprechen.

DO

Sensibilität und Sicherheit im Umgang mit Datenschutz und Datensicherheit kann auf zwei Arten gefördert werden: Einerseits sind Aufklärung der Beschäftigten, Schulungen und Dienstanweisungen sehr wichtig.
Andererseits muss sich die Geschäftsführung eines Unternehmens mit technischen Voraussetzungen auseinandersetzen, mit dem Ziel, hier eine Handlungssicherheit bei allen Beteiligten ermöglichen zu können.

Stehen die Rahmenbedingungen fest, sollten Sie die Beschäftigten über das Thema Datenschutz und die Datensicherheit informieren. Dafür sollte vor der ersten Nutzung der Geräte eine entsprechende Einweisung stattfinden. Zudem ist zu empfehlen, die Informationen in Form von leicht verständlichen und schnell zugreifbaren Nutzungsregeln/-richtlinien/-vereinbarungen vorzulegen.

Diese Nutzungsrichtlinien sollten regelmäßig aktualisiert, sowie die Beschäftigten regelmäßig für das Thema sensibilisiert werden. Eine jährliche Unterweisung bietet sich hierzu an.

Zum Thema Datenschutz gehört auch das Vertrauen der Beschäftigten, ob das eigene Unternehmen mit ihren Daten sensibel umgeht. Ein „heimliches“ Sammeln von Daten kann schnell Ängste bei den Beschäftigten hervorrufen, ob die Daten zu Kontroll- oder Vergleichszwecken gebraucht werden könnten. Machen Sie daher transparent, welche Daten Ihrer Beschäftigten Sie aus welchem Grund erheben und nutzen!

Die für Datensicherheit und Datenschutz identifizierte(n) Person(en) sollte(n)

- sich über aktuelle Gesetzeslagen informieren und bei Bedarf notwendige Maßnahmen einleiten
- Datenschutzeinstellungen von Software und Geräten regelmäßig überprüfen
- die Datensicherheit auf stationären PC, Smartphones, Tablets und weiteren Geräten, die im Unternehmen verwendet werden, durch Berechtigungskonzepte und Zugriffsbeschränkungen durch persönliche Zugänge mit Passwort sichern.

Zudem sollten IT-Verantwortliche damit beauftragt werden, Betriebssysteme, Virenschutzprogramme, Firewalls und die Software (z. B. Branchensoftware) immer auf dem aktuellsten Stand zu halten, um wichtige Sicherheitsupdates zu erhalten. Dazu gehört ebenfalls, Übertragungswege (z. B. WLAN, Bluetooth) vor Zugriff durch Externe zu schützen. Es sollten nur verschlüsselte Kommunikationswege zu dienstlichen Zwecken genutzt werden (z. B. https, verschlüsselte E-Mails, Intranetnutzung) – sprechen Sie bei Bedarf Ihre IT oder die Softwareanbieter darauf an. Und: Bei der Auswahl der passenden Software sollte nur Software aus sicheren Quellen verwendet werden. Hierzu zählen in der Regel die von den Herstellern der Software genannten Downloadlinks.

CHECK

Die Themen Datenschutz und Datensicherheit sind sensibel. Sie sollten daher regelmäßig prüfen, ob die vereinbarten Handlungsweisen und Prozesse praktikabel sind und eingehalten werden. Dabei können Ihnen die Checklisten ➲ SICHERE KOMMUNIKATION (ONLINE) | DATENSICHERHEIT | BESCHÄFTIGTEN- UND KUND*INNENDATENSCHUTZ & SICHERE INTERNETNUTZUNG helfen sowie folgende Leitfragen:

- Erfüllen die benannten Verantwortlichen ihre Aufgaben, und ist den Mitarbeiter*innen klar, wer die Verantwortlichen sind?
- Halten sich die Mitarbeiter*innen an die vereinbarten Vorgaben zu Datenschutz und Datensicherheit? Hierbei ist eine rein technische Kontrolle nicht möglich; vielmehr sind die Führungskräfte u.a. durch Beobachtung und Befragung ihrer Mitarbeiter*innen gefordert.
- Werden die verteilten Nutzungsrichtlinien von Ihren Mitarbeiter*innen als praktikabel und handlungsleitend in der täglichen Arbeit angesehen?

ACT

Sichern Sie den Praxiseinsatz durch folgende Maßnahmen:

- Anerkennen der Wichtigkeit der Themen Datenschutz und Datensicherheit auf der Ebene der Unternehmensleitung; Durchführung regelmäßiger Qualitätszirkel
- Verstetigung der Schulungen/Unterweisungen Ihrer Beschäftigten – nur eine regelmäßige Beschäftigung mit den Themen sensibilisiert auch dauerhaft.

Stolpersteine

Missachtung von Regelungen

Ein erster Stolperstein ist, wenn entsprechende Regelungen von Ihnen oder Ihren Beschäftigten nicht beachtet werden. Dies kann unter Umständen rechtliche Konsequenzen für Ihr Unternehmen und/oder Ihre Beschäftigten haben, es kann zu Rufschädigung und als Konsequenz zum Verlust von Kund*innen führen.

Daher ist es umso wichtiger, dass Führungskräfte mit gutem Beispiel vorangehen, helfen, motivieren und auch die Folgen der Nicht-Beachtung von Regelungen verdeutlichen.

Verantwortung auf Beschäftigte abwälzen

Ein zweiter Stolperstein ist, wenn Sie als Unternehmen (zu viel) Verantwortlichkeit auf Ihre Beschäftigten abwälzen. Folgen können dann einerseits eine Überforderung der Beschäftigten sein, was zum Verlust der Fachkräfte führen kann. Andererseits kann es Fehler geben beim Umgang mit Daten – mit den beschriebenen Folgen.

Daher: Die rechtliche Verantwortung bleibt bei Ihrem Unternehmen! Sie sollten dementsprechend Vorkehrungen und Regelungen auch zum eigenen Schutz treffen. Sie und Ihre Führungskräfte sollten verantwortlich bleiben und sich auch so fühlen.

Instrumente

- Checkliste „Beschäftigten- und Kund*innendatenschutz“
- Checkliste „Datensicherheit“
- Checkliste „Sichere Internetnutzung“