Mittelstand 4.0
Kompetenzzentrum
Planen und Bauen

Leitfaden

Was ist IT-Compliance?

Eine praktische Arbeitshilfe des Mittelstand 4.0-Kompetenzzentrums Planen und Bauen für Unternehmerinnen und Unternehmer im Handwerk

Mittelstand-Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

Was ist IT-Compliance?

Eine praktische Arbeitshilfe des Mittelstand 4.0-Kompetenzzentrums Planen und Bauen für Unternehmerinnen und Unternehmer im Handwerk sowie kleinen und mittelständischen Unternehmen der Bau- und Immobilienwirtschaft.

Wie Sie uns erreichen

- info@kompetenzzentrum-planen-und-bauen.digital
- www.kompetenzzentrum-planen-und-bauen.digital
- Telefon: 08024 - 643 678

Das Mittelstand 4.0-Kompetenzzentrum Planen und Bauen wird gebildet von:

Impressum

Herausgeber: Mittelstand 4.0-Kompetenzzentrum Planen und Bauen / eBusiness-Kompetenzzentrum gUG (haftungsbeschränkt), Fraunhofer-Institut für Bauphysik IBP (Gesamtleitung), Fraunhofer Straße 10, 83626 Valley
Redaktion: Michael Weller (Autor), m.weller@ebusiness-kompetenzzentrum.de; Telefon: 0631-205 601 801
Gestaltung und Produktion: buildingSMART Deutschland, Wiener Platz 6, 01069 Dresden
Bildnachweis: Alle Bilder: www.pixbay.com, lizenziert unter CCO Public Domain Dedication, Lizenzbedingungen abrufbar unter: https://creativcommons.org/publicdomain/zero/1.0/deed.de
Druck: XXY Druckerei
Online:als PDF-Download unter: www.kompetenzzentrum-planen-und-bauen.digital
Auflage: 1.000

Der Autor:

Rechtsanwalt Michael Weller arbeitet seit März 2017 für das eBusiness-KompetenzZentrum in Kaiserslautern, dem Standort der Region Mitte des Mittelstand 4.0-Kompetenzzentrums Planen und Bauen. Zuvor war Michael Weller zehn Jahre als Rechtsanwalt und Projektverantwortlicher an einer wissenschaftlichen Einrichtung tätig. Bereits Ende der 1990er Jahre, noch während seines Jura-Studiums, hat er sich dem Recht der neuen Medien gewidmet und es sich zur Aufgabe gemacht, Berührungsängste mit Rechtsthemen bei Praktikern in kleinen und mittleren Unternehmen abzubauen. Sein Motto lautet folglich: „IT-Compliance ist keine Zauberei“.

Inhalt des Leitfadens

Wozu ein Leitfaden „Was ist IT-Compliance“?

IT-Compliance ist vielen ein nebulöser Begriff und es fällt schwer, sich eine konkrete Vorstellung zu bilden, was darunter zu verstehen ist. Als Oberbegriff für eine Vielzahl von Verhaltensanforderungen ist er auf jeden Fall erklärungsbedürftig. Dieser Leitfaden soll helfen, nicht nur den Begriff zu klären, sondern auch die nötigen Schritte aufführen, um IT-Compliance für den eigenen Betrieb zu erreichen.

Es ist zu beobachten, dass beim Einsatz von digitalen Helfern bisweilen eine gewisse Sorglosigkeit vorherrscht. Begeisterung für die neue Technik lässt so manchen Betriebsinhaber die notwendigen, im Kontext zu beachtenden Compliance-Aspekte vergessen. Die Konsequenzen fehlender Compliance sind indes hart. Sie reichen von empfindlichen Strafen für das Unternehmen bis zu persönlicher Haftung des Geschäftsführers oder Inhabers.

Verwendung des Leitfadens

Dieser Leitfaden richtet sich an alle Teilnehmer des Workshops „Was ist IT-Compliance?“ des Mittelstand 4.0-Kompetenzzentrums Planen und Bauen sowie an alle, die einen Einstieg in das Thema suchen. Er dient dazu, Problemlagen zu erkennen. Er kann natürlich nicht jeden Einzelfall beantworten. Der Autor freut sich jedoch über Rückmeldungen aus den Workshops und von Lesern des Leitfadens – wiederkehrende Fragen und Anregungen werden in folgenden Auflagen berücksichtigt.

Der Workshop, zu dem dieser Leitfaden entwickelt wurde, soll helfen, wesentliche Aspekte von IT-Compliance auch ohne ausgeprägte Rechtskenntnisse erkennen zu können. Er soll Betriebsinhabern und Betriebsleitern ermöglichen, im eigenen Betrieb vorhandene Schwachstellen zu identifizieren.

„Das Ziel des Workshops und des Leitfadens ist die Sensibilisierung für IT-Compliance-Sachverhalte.“

Dabei geht es nicht nur um den Einsatz neuer Technologie, sondern auch um die Akzeptanz fördernde Umsetzung von Digitalisierungsmaßnahmen sowie die Vermeidung persönlicher Risiken für Betriebsinhaber und Betriebsleiter, aber auch für die Mitarbeiter. Auch sollen Berührungsängste mit Rechtsthemen abgebaut werden. Nicht zuletzt sollen sowohl der Workshop wie auch dieser Leitfaden helfen, Dienstleistern und Beratern die notwendigen Fragen zu stellen.

Wichtiger Hinweis:

- Der Expertenleitfaden dient allein Informationszwecken und kann eine professionelle steuerliche oder rechtliche Beratung keinesfalls ersetzen. Es ist daher empfohlen, erkannte Probleme mit dem Steuerberater oder Rechtsanwalt zu besprechen und diese um konkrete Äußerungen und Handlungsempfehlungen zu bitten.

Ausgangspunkt: Definition der IT-Compliance und Legalitätspflicht

Im deutschsprachigen Wikipedia-Eintrag findet sich folgende Definition:

- „IT-Compliance beschreibt in der Unternehmensführung die Einhaltung der gesetzlichen, unternehmensinternen und vertraglichen Regelungen im Bereich der IT-Landschaft."

Diese Definition ist recht abstrakt und muss für den Praktiker konkretisiert werden. Anhand der hier ausgewählten praktischen Beispiele aus dem Alltag von Handwerksunternehmen kann die eigene betriebliche Situation kritisch überprüft und gegebenenfalls Handlungsanforderungen identifiziert werden. Dies kann auch bedeuten, dass erkannt wird, dass zur Lösung eines Problems weitere Informationen benötigt werden.

Legalitätspflicht – Organisation der Rechtskonformität des Betriebes als Aufgabe der Geschäftsleitung

Rechtlich findet sich die IT-Compliance verankert in der Verpflichtung des Geschäftsleiters, das Unternehmen mit der Sorgfalt eines ordentlichen Kaufmannes zu führen. Für die Gesellschaft mit beschränkter Haftung findet sich die entsprechende Verhaltensanforderung in Paragraph 43 GmbHG und ist an den Geschäftsführer gerichtet; für die Aktiengesellschaft findet sich diese Anforderung in Paragraph 93 AktG und ist an den Vorstand gerichtet. Allgemein ist die Verpflichtung zur Anwendung der Sorgfalt eines ordentlichen Kaufmannes in Paragraph 347 HGB jedem auferlegt, der aus einem Geschäft, das auf der einen Seite ein Handelsgeschäft ist, einem anderen gegenüber zur Sorgfalt verpflichtet ist. Auch wenn hier lediglich stellvertretend zwei Rechtsformen angesprochen wurden, so treffen diese Anforderungen in der Regel auf jedes Unternehmen zu, egal in welcher Rechtsform es geführt wird.

Wer gewerblich Leistungen anbietet, unterliegt bezüglich dieser Angebote einem strengeren Maßstab als derjenige, der im allgemeinen, nicht-gewerblichen Kontext anzulegen sein würde. Dies bedeutet etwa, dass der ordentliche Kaufmann die in seinem Betrieb eingesetzten Geräte und Werkzeuge gegebenenfalls austauscht, weil beispielsweise veränderte gesetzlicher Anforderungen an die Gerätesicherheit dies fordern.

IT-Sicherheit ist ebenso wie der Datenschutz lediglich ein Teil einer umfassend verstandenen IT-Compliance. Auch Aspekte des Auftretens in virtuellen Umgebungen, etwa über eine Unternehmens-Website oder ein Unternehmensprofil in einem sozialen Netzwerk (z.B. Facebook, LinkedIn, XING u.a.) dürfen nicht vernachlässigt werden.

Ferner bestimmen die Grundsätze zur ordnungsgemäßen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) Anforderungen an die Gestaltung und Einrichtung der IT-Landschaft im Unternehmen.

Neben diesen gesetzlichen oder verwaltungsinternen Bestimmungen steht das Unternehmen in vertraglichen Beziehungen, die Einfluss auf den Einsatz von digitalen Werkzeugen haben. So ist etwa die Verwendung von Software durch Lizenzverträge geregelt, deren Einhaltung ebenfalls sicherzustellen ist.

Anerkannt ist, dass die Einrichtung von Sicherheitsmaßnahmen für die IT und deren Kontrolle unabhängig von der Unternehmensform zur Sorgfalt eines ordentlichen Kaufmannes gerechnet werden muss. Verstöße und Vernachlässigungen können die persönliche Haftung der Leitungsebene gegenüber dem Unternehmen begründen.

Nicht nur wegen der gesetzlichen Anforderungen, sondern schon zum Selbstschutz gegen eine unberechtigte Inanspruchnahme etwa durch die Gesellschafter oder Gläubiger des Unternehmens, sind die eingesetzten IT-Werkzeuge – also Hard- und Software – sowie die zu einem anforderungsgerechten Umgang mit diesen ergriffenen Maßnahmen zu dokumentieren. Hierdurch kann der IT-Einsatz transparent gemacht werden und die notwendigen Maßnahmen nachgewiesen werden.

Ausgehend von dieser Verpflichtung werden die nachfolgenden Aspekte einer umfassend verstandenen IT-Compliance durch Fallbeispiele näher betrachtet:

- Kommunikationsvorgänge im Unternehmen zwischen Mitarbeitern und Kunden sowie Lieferanten und Dienstleistern, aber auch zwischen den Mitarbeitern über betriebliche Angelegenheiten.

- Unternehmenspräsentation vor allem in digitalen Umgebungen in Bezug auf das Vorhandensein von erforderlichen Belehrungen und Informationen wie z.B. einer zutreffenden Datenschutzerklärung sowie des Vorliegens und der Einhaltung von erforderlichen Nutzungsrechten an digitalen Inhalten wie etwa Texten, Bildern, Musik oder Videos.

- Aufbewahrung und Archivierung von Handels- und Geschäftsbriefen sowie von Belegen in elektronischer Form einschließlich der Gewährleistung einer den gesetzlichen Anforderungen genügenden Löschung und Vernichtung.

- Dokumentation des IT-Einsatzes zur Erfüllung der gesetzlichen Dokumentationspflichten insbesondere aus den GoBD und dem Datenschutzrecht.

- Überwachung der Betriebsabläufe im Rahmen eines internen Kontrollsystems entsprechend den Anforderungen an die Sorgfalt eines ordentlichen Kaufmannes.

- Einspielen erforderlicher Änderungen in den betrieblichen Alltag in Bezug auf technische, aber auch rechtliche Innovationen unter Einbeziehung der Mitarbeiter.

Soweit die relevanten Fragen nicht auf der Grundlage eigener Sachkunde beantwortet werden können, sollte unbedingt individuelle Beratung in Anspruch genommen werden. Dies ist allein schon deshalb wichtig, weil sowohl Workshop wie auch dieser Leitfaden zwangsläufig nur anhand ausgewählter Beispiele ein Bewusstsein für die Bedeutung der IT-Compliance im Unternehmen wecken kann (und will).

„Anhand der Fallbeispiele sollte es möglich sein, die betreffenden Abläufe im eigenen Unternehmen zu identifizieren, in denen Verbesserungen im Sinne der IT-Compliance möglich sind.“

Ein großer Vorteil individueller Beratung liegt für Unternehmensverantwortliche darin, dass das Risiko einer persönlichen Haftung für Versäumnisse drastisch reduziert werden kann. Bedient man sich fachkundiger Hilfe zur Lösung eines Problems im Betrieb, kann dem Hilfesuchenden schwerlich der Vorwurf gemacht werden, die Augen vor dem Problem verschlossen zu haben. Darüber hinaus besteht in der Regel die Möglichkeit einen gleichwohl eintretenden Schaden in den Fällen, in denen sich die Hilfe als ungeeignet oder fehlerhaft erweist, gegenüber dem Helfenden geltend zu machen. Professionelle Berater wie insbesondere Rechtsanwälte und Steuerberater unterhalten für den Fall, dass ihnen ein Fehler unterläuft, eine Berufshaftpflichtversicherung. Diese deckt auch Fälle von Falsch- oder Fehlberatung ab und der Unternehmer bleibt nicht auf einem vom Berater verursachten Schaden sitzen.

Kommunikationsvorgänge

Ganz selbstverständlich werden Smartphones und E-Mail zur Kommunikation mit Kunden, Lieferanten und Dienstleistern, aber auch zur internen Abstimmung eingesetzt. Was gilt es zu beachten?

Fallbeispiel: Betriebliches Smartphone

Ein Unternehmer gibt an seine Mitarbeiter eigens beschaffte und dienstlich zu nutzende Smartphones aus. Diese sind mit einer Reihe von Applikationen ausgestattet. Darunter befinden sich nicht nur solche, die allein im betrieblichen Kontext genutzt werden, sondern auch solche, die die Arbeitnehmern auch außerbetrieblich nutzen dürfen. Hierzu gehört z.B. eine App, die bei Kundenterminen das Auffinden von Lokalen mit der Möglichkeit zur Einnahme des Mittagessens erlaubt. Ein Mitarbeiter fühlt sich wegen der Smartphone-Benutzung bevormundet. Er verlangt im Betrieb, dass die Nutzung der Geräte künftig unterbleibt. Als sein Vorgesetzter dies ablehnt, findet er nach kurzer Recherche heraus, dass er mit dem Argument, die Gerätenutzung sei datenschutzwidrig, sich an die Datenschutz-Aufsichtsbehörde seines Bundeslandes wenden kann.

- Besteht die Möglichkeit, dass die Datenschutz-Aufsichtsbehörde einschreitet, wenn der Mitarbeiter sich dort beschwert?

Überlegungen zur IT-Compliance zu diesem Fallbeispiel

Die Datenschutz-Aufsichtsbehörde wird einschreiten, wenn ein Verstoß gegen datenschutzrechtliche Anforderungen vorliegt. Datenschutzrechtliche Anforderungen sind dann zu beachten, wenn personenbezogene Daten im Sinne von Art. 4, Nr. 1 der EU-Datenschutz-Grundverordnung vorliegen. Als personenbezogene Daten gelten Informationen, die auf eine identifizierte oder identifizierbare natürliche Person – einen Menschen – bezogen werden können. Hierzu gehören insbesondere der Name einer Person, dem Namen und damit der Person zuzuordnende Kennnummern und Standortdaten, aber auch eine Online-Kennung. Da auch Mobiltelefone Informationen über das Internet übermitteln ist es nur konsequent, auch die von dem Gerät übermittelten Standortdaten als personenbezogene Daten zu betrachten. Zwar muss grundsätzlich der Nutzer seine Zustimmung zum Zugriff auf Standortdaten erklären und eine entsprechende Einstellung vornehmen. Allerdings hat im Fallbeispiel der Arbeitgeber das Smartphone mit der bereits installierten und konfigurierten App an seinen Mitarbeiter ausgegeben.

Zwar darf der Arbeitgeber, wenn er ein berechtigtes Interesse nachweisen kann, auch Standortdaten seiner Mitarbeiter erheben, doch geht es im Fallbeispiel lediglich um einen Komfortgewinn. Um diesen zu ermöglichen, muss in die Verarbeitung von Standortdaten durch den App-Anbieter eingewilligt werden. Da der Standort dem betreffenden Mitarbeiter zugeordnet werden kann, steht die Einwilligung wegen des hohen Rangs des Grundrechts auf informationelle Selbstbestimmung nur dem Mitarbeiter selbst, nicht aber seinem Arbeitgeber zu. Oder anders ausgedrückt: Der Arbeitgeber kann nicht für seinen Mitarbeiter in die Verarbeitung von Mitarbeiterdaten durch einen Dritten einwilligen.

Ist die App lediglich installiert, steht es jedoch im Belieben des Mitarbeiters, sie zu aktivieren und die Erlaubnis zu erteilen, auf seine Standortdaten zuzugreifen, spricht unter datenschutzrechtlichen Gesichtspunkten nichts gegen diese „Arbeitserleichterung“. Für den Arbeitgeber besteht die Verpflichtung, das Persönlichkeitsrecht

seiner Arbeitnehmer zu wahren und zu achten. Als derjenige, der über die Datenverarbeitung und die hierzu eingesetzten Mittel entscheidet, ist er Verantwortlicher gemäß der EU-Datenschutz-Grundverordnung. Hierzu hat er von mehreren möglichen Einstellungen eines Gerätes oder einer Software immer diejenige zu wählen, die am datenschutzfreundlichsten ist. Dies ist explizit als Gestaltungsaufgabe im Hinblick auf das Gebot der Datenvermeidung und der Datensparsamkeit im Datenschutzrecht definiert. Für den Arbeitgeber bedeutet dies, dass er keine Daten von seinen Mitarbeitern erheben oder erheben lassen darf, die nicht zwingend für den Betrieb benötigt werden. Geht es nicht ohne Informationen, dürfen nur solche beschafft werden, die absolut unverzichtbar sind.

Fazit:

- Die Datenschutzaufsichtsbehörde wird dann einschreiten, wenn der Arbeitgeber die Voreinstellungen der App nicht in datenschutzfreundlicher Art und Weise vorgenommen hat.
- Der Arbeitgeber ist aufgefordert, auf zu dienstlichen Zwecken ausgegebenen Endgeräten wie Smartphones, Tablets oder Laptops etc. alle Funktionen, die nicht unbedingt zur Ausübung der arbeitsvertraglich vom Mitarbeiter geschuldeten Leistungen erforderlich sind, zu deaktivieren, um eine unzulässige Datenaufzeichnung zu verhindern.
- Es darf nur eine solche Erhebung personenbezogener Daten zugelassen werden, an der der Arbeitgeber ein berechtigtes Interesse nachweisen kann.

Die Benutzung privater Endgeräte im Betrieb birgt unter Compliance-Aspekten dieses Risiko zwar nicht, geht aber mit der Gefahr einher, dass z.B. eine ERP-Lösung auf dem privaten Endgerät deshalb nicht eingesetzt werden kann, weil das Gerät nicht in die betriebliche IT-Sicherheitsstruktur eingebunden werden kann. Ferner ist es nicht immer möglich, die Nutzung auf einem privaten Endgerät lizenzkonform zu gestalten. Im Ergebnis ist daher von dem Einsatz privater Endgeräte zu betrieblichen Zwecken abzuraten.

Fallbeispiel: Dienstliches E-Mail-Postfach

Ein Handwerksbetrieb im Allgäu, in dem zwei Bürokräfte beschäftigt sind, hat über einen IT-Dienstleister E-Mail-Postfächer zum Empfang für den Betrieb bestimmter Nachrichten eingerichtet. Der Betriebsinhaber ist während der Bürozeiten zumeist auf der Baustelle. Die Nutzung der E-Mail-Postfächer wird daher nicht kontrolliert. Tatsächlich hat es sich im Laufe eines ganzen Jahres gezeigt, dass die Bürokräfte die betriebliche E-Mail-Adresse auch für private Kommunikation nutzen. Während eine Bürokraft in den Sommerferien an der Nordsee weilt, ruft ein von ihr betreuter Kunde an. Er ist wegen einer ausstehenden Rückmeldung auf eine Rückfrage, die er per E-Mail an die im Urlaub befindliche Bürokraft gesendet hatte, verärgert.

- Darf der Betriebsinhaber von dem IT-Dienstleister verlangen, Zugriff auf das E-Mail-Postfach der im Urlaub befindlichen Bürokraft zu erhalten und die fragliche E-Mail heraussuchen?

Überlegungen zur IT-Compliance zu diesem Fallbeispiel

Der Betriebsinhaber darf von dem IT-Dienstleister die Herstellung des Zugriffs auf das E-Mail-Postfach der im Urlaub befindlichen Bürokraft verlangen, wenn er dadurch nicht widerrechtlich in Rechte dieser Bürokraft eingreift und diese verletzt.

Da die Bürokraft an der Nordsee weilt, der Betrieb sich aber recht weit vom Urlaubsort entfernt befindet, liegt nahe, dass die Bürokraft nicht selbst mal kurz im Betrieb vorbeischauen und ihrem Chef die betreffende E-Mail zur Bearbeitung weiterleiten oder die Anfrage selbst bearbeiten kann. Gleichwohl möchte der Betriebsinhaber den Kunden nicht verlieren, sondern zufriedenstellen. In dieser Situation könnte man auf den Gedanken verfallen, dass ein berechtigtes Interesse am Zugriff auf das E-Mail-Postfach der Bürokraft vorliegt. In der Tat wird durch das Fernmeldegeheimnis (Paragraph 88 Telekommunikations-Gesetz, TKG) die Auswertung der Korrespondenz nur während des Übertragungsvorgangs untersagt. Ist die E-Mail bereits im E-Mail-Postfach abgelegt, greift dieser Schutz folglich nicht mehr.

Allerdings ist anerkannt, dass auch im Postfach des E-Mail-Empfängers abgelegte E-Mails nicht ohne weiteres durch den Arbeitgeber gesichtet und ausgewertet werden dürfen. Hat der Arbeitgeber die private Nutzung der betrieblichen E-Mail-Postfächer zugelassen und sei es durch eine betriebliche Übung, schließt er sich vom Zugriff auf die Postfächer selbst aus.

Eine betriebliche Übung liegt vor, wenn ein Arbeitgeber durch ein wiederholtes oder dauerhaftes Verhalten bei seinen Arbeitnehmern das Vertrauen darin begründet, er werde sein Verhalten künftig nicht ohne triftigen Grund ändern. In Bezug auf die Nutzung des E-Mail-Postfachs bedeutet dies, dass durch das über einen langen Zeitraum andauernde Zulassen der privaten Nutzung bei den beiden Bürokräften das Vertrauen darin wachsen konnte, dass das Nutzen der betrieblichen Mails auch zu privaten Zwecken nicht ohne triftigen Grund gewährt bleibe.

Ist die private Nutzung des betrieblichen E-Mail-Postfachs zugelassen, können die Mitarbeiter sich auf das ihnen auch an ihrem Arbeitsplatz zustehende Recht auf informationelle Selbstbestimmung und die Vertraulichkeit und Integrität informationstechnischer Systeme berufen. Aufgrund der Pflicht des Arbeitgebers, die Rechte seiner Arbeitnehmer zu wahren, darf er nicht ohne ihre Zustimmung auf ein Postfach Zugriff nehmen, in dem sich auch private Kommunikation befindet.

Der Arbeitgeber hat die Möglichkeit, die private Nutzung der dienstlich überlassenen Postfächer zu untersagen. Um jedoch zu vermeiden, dass die private Nutzung im Rahmen einer betrieblichen Übung zulässig werden könnte, muss er das Verbot auch kontrollieren und ggf. durchsetzen.

Allerdings sind auch alternative Gestaltungen des Zugriffs auf ein E-Mail-Postfach im Falle der Verhinderung des Inhabers denkbar. So kann in den Vertretungsregeln für den Fall der Abwesenheit des Postfachinhabers festgelegt werden, wer und in welcher Weise Zugriff auf das Postfach nehmen können soll. Diese Vertretungsregeln müssen transparent gestaltet und im Vorfeld mit den Postfachinhabern vereinbart worden sein.

In größeren Betrieben ist es auch möglich, für den Fall der persönlichen Verhinderung einer Kollegin oder einem Kollegen, dem man vertraut, den Zugriff auf das Postfach zu gestatten. Hierzu könnte z.B. das Passwort in einem verschlossenen Umschlag bei dieser bzw. bei diesem hinterlegt werden, so dass diese Vertrauensperson in der Lage ist, im Notfall eine wichtige E-Mail zur Bearbeitung weiterzuleiten.

Fazit:

- Lässt der Arbeitgeber die private Nutzung des betrieblichen E-Mail-Postfachs durch seine Mitarbeiter zu, schließt er sich von einem Zugriff auf in dem Postfach abgelegte Kommunikation aus.
- Ein Verbot der privaten Nutzung des betrieblichen E-Mail-Postfachs muss kontrolliert und durchgesetzt werden, was bedeutet, dass ein Verstoß gegen das Verbot auch zu sanktionieren ist. Dies ist mit einem gewissen Aufwand für den Arbeitgeber verbunden, der bedacht werden muss.
- Vertretungsregeln sind denkbar, erfordern aber ebenfalls einen gewissen Aufwand bei der Einrichtung durch Durchführung. Auf ihre Datenschutzkonformität ist besonders zu achten.
- Die Frage, ob ein Verbot der privaten Nutzung des betrieblichen E-Mail-Postfachs zielführend ist, kann nur im jeweiligen Einzelfall und nicht pauschal beantwortet werden. Hier ist der Arbeitgeber aufgefordert, die für seinen Betrieb passende Vorgehensweise zu ermitteln.

Da E-Mails, insbesondere Dateianhänge zu E-Mails, besondere Risiken für das Einschleppen von Schadsoftware in die betriebliche IT bergen, ist der Einsatz immer aktuell zu haltender Virenschutzsoftware faktisch unumgänglich.

Darüber hinaus sollte durch den Arbeitgeber darauf hingewirkt werden, dass Mitarbeiter möglichst sichere Passwörter verwenden. Diese sollten dann allerdings nicht am Monitor oder auf der Rückseite der Tastatur vermerkt werden, sondern jeweils aus dem Kopf oder ggf. über sichere Applikationen eingegeben werden.

Unternehmenspräsentation

Das Erscheinungsbild eines Unternehmens in der Öffentlichkeit ist ein entscheidender Faktor für die Gewinnung neuer und die Bindung alter Kunden sowie die Anwerbung von Fachkräften.

Wesentlich für die Präsentation des Unternehmens sind neben der Unternehmens-Website auch andere Kanäle wie z.B. soziale Netzwerke. Diese Werbekanäle müssen mit Inhalten beschickt werden. Diese Inhalte können auch von spezialisierten Anbietern erworben werden und müssen nicht immer selbst erzeugt werden.

Fallbeispiel: Datenschutzerklärung auf der Website

Ein Handwerker lässt für seinen Betrieb bei einem befreundeten Webdesigner eine Unternehmenswebsite gestalten. Neben dem Impressum findet sich auch eine von der Startseite aus erreichbare Datenschutzerklärung. Diese hat folgenden Inhalt: „Sofern innerhalb des Internetangebots die Möglichkeit der Eingabe persönlicher oder geschäftlicher Daten besteht, so erfolgt die Preisgabe dieser Daten seitens des Nutzers auf ausdrücklich freiwilliger Basis.“ Weitere Angaben macht die Datenschutzerklärung nicht. Sechs Wochen nach der Freischaltung der Website erhält der Handwerker einen Brief der Datenschutz-Aufsichtsbehörde. Darin wird der Handwerker zur Stellungnahme aufgefordert, weil die Datenschutzerklärung den Nutzer nicht ausreichend über die Erhebung und Speicherung seiner personenbezogenen Daten informiert. Für den Fall, dass der Verstoß nicht binnen 14 Tagen abgestellt wird, wird ein Bußgeld angedroht.

- Liegt tatsächlich ein Datenschutzverstoß vor?

Überlegungen zur IT-Compliance zu diesem Fallbeispiel

Ein Datenschutzverstoß läge vor, wenn der Handwerker tatsächlich Informationspflichten zum Umgang mit personenbezogenen Daten gegenüber den Nutzern seines Internetangebots nicht oder nicht ausreichend nachgekommen ist. Eine Verletzung von Informationspflichten kommt vorliegend in Betracht, da die vorhandene Datenschutzerklärung nicht über den Umgang mit der IP-Adresse aufklärt. Die IP-Adresse ist die „Hausnummer“, unter der ein Computer im Internet erreicht werden kann. Ohne diese „Hausnummer“ des Computers des Nutzers zu kennen, kann die Unternehmenshomepage auf diesem Computer nicht angezeigt werden. Der Computer, auf dem die Unternehmenshomepage abgespeichert ist – der Server – muss die Information, wie die Unternehmenshomepage auf dem Bildschirm des Nutzers angezeigt werden soll, an den Computer des Nutzers ausliefern. Wie der Postbote, der die Zustelladresse ja kennen muss, um eine Postsendung zustellen zu können, muss der Server ebenfalls die Adresse des Computers kennen, an den die Anzeigeinformationen zuzustellen sind.

Damit stellt sich die Frage, ob man aus der IP-Adresse auf einen menschlichen Nutzer zurückschließen kann oder anders ausgedrückt: ob es sich bei der IP-Adresse um ein personenbezogenes Datum gem. Art. 4, Nr. 1 DS-GVO handelt. Dies ist wie zuvor im Rahmen der Betrachtungen der ▶ Kommunikationsvorgänge gezeigt der Fall. Da die IP-Adresse von dem Server mitgeschrieben – *geloggt* – wird, könnte der Handwerker unter bestimmten Voraussetzungen über den Anbieter des Internetzugangs des Nutzers dessen Namen in Erfahrung bringen. So würde etwa der Anbieter des Nutzers z.B. im Falle einer Rechtsverletzung durch den Nutzer ein entsprechendes Auskunftsersuchen beantworten,

damit der Verletzte Schadensersatz erlangen und ggf. eine Strafverfolgung eingeleitet werden kann. Die IP-Adresse ist daher ein personenbezogenes Datum.

Da wie gerade gezeigt in Form der IP-Adresse ein personenbezogenes Datum vorliegt, ist der Anwendungsbereich des Datenschutzrechts eröffnet. Dem Anbieter einer Internetseite treffen also die im Datenschutzrecht festgelegten Informations-, Transparenz- und Rechenschaftspflichten. Anbieter einer Internetseite ist gem. Paragraph 2 des Telemediengesetzes (TMG) derjenige, der einen mit den menschlichen Sinnen wahrnehmbaren Inhalt so im Internet anbietet, dass er von den Nutzern abgerufen werden kann. Damit fällt auch der Handwerker mit seiner Unternehmenshomepage unter diesen Begriff, da er ja letztlich bestimmt, was auf der Homepage zu sehen ist. In Bezug auf das Anbieten einer Internetseite bestimmen sich die maßgeblichen Pflichten nach den Anforderungen in Paragraph 13 TMG. So ist der Handwerker verpflichtet, die Nutzer seiner Unternehmenshomepage bereits zu Beginn des Nutzungsvorganges, also beim erstmaligen Aufruf der Internetseite, darüber zu informieren, welche personenbezogenen Daten von ihm oder dem von ihm beauftragten Dienstleister erhoben werden. Weiter muss darüber aufgeklärt werden, zu welchem Zweck die Erhebung und Verarbeitung erfolgt sowie auch darüber, wie lange die Daten gespeichert werden. Dies erfolgt in der Regel über die Datenschutzerklärung, die von jeder einzelnen (Unter-)Seite des Internetauftritts mit nur einem einzigen Klick erreichbar sein muss. Werden zulässigerweise besondere Technologien etwa zur Verfolgung des Nutzerverhaltens oder zum Marketing eingesetzt, ist regelmäßig die Einbindung eines sog. „Cookie-Banners“ erforderlich, um gleich beim ersten Seitenaufruf dem Nutzer die Möglichkeit zu bieten, die Verarbeitung seiner IP-Adresse zu unterbinden.

Im Fallbeispiel ist die Datenschutzerklärung lediglich von der Startseite aus erreichbar, womit die 1-Klick-Regel nicht eingehalten ist. Ferner erwähnt die Erklärung nicht, dass die IP-Adresse – was technisch wie bereits dargelegt unvermeidbar ist – erfasst und zumindest für die Dauer des Nutzungsvorgangs verarbeitet wird, da es anderenfalls ja gar nicht möglich wäre, die Unternehmenshomepage den Nutzern auf ihren Geräten anzuzeigen. Hierüber ist aber der Nutzer in Kenntnis zu setzen. Somit liegt also ein Datenschutzverstoß vor.

Dieser wäre besonders kritisch, wenn – wofür jedoch im Fallbeispiel nichts spricht – die IP-Adresse an Anbieter anderer Dienste in ein Land außerhalb der EU und des Europäischen Wirtschaftsraumes übertragen würde. Dies ist z.B. dann der Fall, wenn Dienste von Anbietern wie Facebook – etwa der Like-Button – oder Google – etwa die Google Maps – über die betreffende Schnittstellenfunktion (API) eingebunden sind, da hier die IP-Adresse auf Server der betreffenden Anbieter in den USA übertragen wird. Insbesondere wegen der hier beispielhaft aufgezählten Dienste herrscht derzeit unter Fachleuten große Unsicherheit. Zum Zeitpunkt der Manuskripterstellung zu diesem Leitfaden lagen dem Europäischen Gerichtshof gleich mehrere Fragen vor, von deren Beantwortung die Zulässigkeit der Benutzung dieser Dienste abhängt.

Ein Datenschutzverstoß kann gem. Paragraph 16 Abs. 2 Nr. 2, Abs. 3 TMG mit einem Bußgeld von bis zu 50.000 Euro geahndet werden. Darüber hinaus liegt im Fallbeispiel eine wettbewerbsrechtlich relevante Irreführung durch Unterlassen gem. Paragraph 5a Abs. 2 Nr. 2 des Gesetzes gegen den unlauteren Wettbewerb (UWG) vor. Allerdings findet sich in der Rechtsprechung die Auffassung, dass ein Vorenthalten von Informationen in einer Datenschutzerklärung im Sinne von Paragraph 5a Abs. 1 UWG nicht geeignet ist, eine geschäftliche Entscheidung zu beeinflussen oder jedenfalls keinen wesentlichen Einfluss auf das Verhalten eines Verbrauchers i.S. von Paragraph 3 Abs. 2 UWG habe.

Ein Verstoß gegen verbraucherschützende Datenschutzvorschriften könnte zuletzt von einer sog. qualifizierten Einrichtung gem. Paragraph 2 Abs. 2 S. 1 Nr. 11 des Unterlassungsklagengesetzes (UKlaG) abgemahnt werden. Wehrt sich indes der Abgemahnte gegen die Abmahnung gerichtlich, würde in einer anzuberaumenden mündlichen Verhandlung die zuständige Datenschutz-Aufsichtsbehörde gehört werden (Paragraph 12a S. 1 UKlaG). Diese kann ihre eigene Einschätzung zum Datenschutzverstoß abgeben und damit die gerichtliche Entscheidung beeinflussen.

Fazit:

- Wer als Unternehmer sein Unternehmen im Internet auf einer Website präsentiert, unterliegt als Dienstanbieter Informationspflichten hinsichtlich des Umgangs mit personenbezogenen Daten, die er über die Nutzer erlangt.

- Wenigstens die IP-Adresse des Computers des Nutzers muss der Websiteanbieter zumindest für die Dauer der Nutzung kennen – darüber ist also im Rahmen der Datenschutzerklärung zu informieren. Wird der Besuch darüber hinaus systematisch ausgewertet, steigen die Informationspflichten entsprechend an.

- Nicht zutreffende oder fehlende Informationen bergen das Risiko, abgemahnt oder mit einem Bußgeld belegt zu werden.

In der Praxis dürfte es nur bei besonders eklatanten Fehlverhaltens dazu kommen, dass die Bußgeldbe-

hörde den Bußgeldrahmen ausschöpft. Dies dürfte insbesondere in Fällen der Unbelehrbarkeit und Wiederholung eines bereits beanstandeten Verhaltens der Fall sein. Gleichwohl können die Auswirkungen auch eines niedrigeren Bußgeldes gravierend sein. Bei wettbewerbsrechtlichen Abmahnungen ist zu bedenken, dass der Abmahnende lediglich Ersatz der Kosten verlangen kann, die ihm durch die Beauftragung eines Rechtsanwalts entstehen. Der Wettbewerber kann sich folglich keine neue Einnahmequelle erschließen, sondern er schafft sich vielmehr das Risiko, dass ein Abgemahnter sich erfolgreich gerichtlich zur Wehr setzt. Dies würde dazu führen, dass der Abmahnende sämtliche Kosten der Abmahnung und des Rechtsstreits zu tragen hätte. Vor diesem Hintergrund sind Abmahnungen grundsätzlich ernst zu nehmen, denn sie bergen ein erhebliches finanzielles Risiko im Falle ihrer Berechtigung.

Fühlt man sich als juristischer Laie mit der Abfassung einer erforderlichen Datenschutzerklärung für die eigene Homepage überfordert, sollte man sich unbedingt individuellen rechtlichen Rat einholen.

Fallbeispiel: Produktfoto auf der Unternehmenswebsite

Ein Handwerker möchte auf seiner Unternehmenswebsite ein Foto des von ihm bevorzugt verwendeten Produkts einbinden, um für seine Leistungen zu werben. Auf der Suche nach einem geeigneten Foto wird er auf der Website des Produktherstellers fündig. Er kopiert das Foto aus dem elektronischen Produktkatalog und legt es auf seinem Webserver ab. Vor dort bindet er das Foto auf seine Unternehmenswebsite ein. Vierzehn Tage nach Freischalten der Website erhält der Handwerker eine Abmahnung. Darin wird ihm vorgeworfen, das Produktfoto ohne die erforderliche Erlaubnis des Produktherstellers zu verwenden. Er wird aufgefordert, das Foto von seiner Website zu entfernen. Ferner soll er die Kosten des beauftragten Rechtsanwalts ersetzen und ein mit „Verpflichtungs- und Unterlassungserklärung“ überschriebenes Dokument unterzeichnen und zurücksenden. Darin enthalten ist die Verpflichtung, es künftig zu unterlassen, Fotos des Produktherstellers ohne dessen ausdrückliche Erlaubnis zu verwenden. Für den Fall, dass hiergegen verstoßen wird, soll eine Vertragsstrafe in Höhe von 6.000 Euro als vereinbart gelten.

- Ist den Forderungen nachzukommen?

Überlegungen zur IT-Compliance zu diesem Fallbeispiel

In der Werbung ist es üblich, dass ein Fotograf seinem Auftraggeber alle Rechte am Foto zur Ausübung überträgt. Diese Übertragung geschieht in einem urheberrechtlichen Vertrag, der Lizenz. In den meisten Fällen wird eine exklusive Lizenz vereinbart, das bedeutet, dass nach dem Fotografen nur der Lizenznehmer über die konkrete Verwendung des Fotos entscheiden darf. Der Lizenznehmer wird damit zum Rechteinhaber.

Gem. Paragraph 97 Abs. 1 UrhG darf der Rechteinhaber – im Fallbeispiel also der Produkthersteller – von demjenigen, der ohne seine Erlaubnis das Foto verwendet, Beseitigung und Unterlassung der konkreten Verwendung verlangen. Eine erlaubnispflichtige Verwendung liegt z.B. vor, wenn das Foto über das Internet zugänglich gemacht wird, Paragraph 19a UrhG.

Aufgrund der Regelung in Paragraph 97a UrhG ist der Produkthersteller als Rechteinhaber gehalten, vor einer gerichtlichen Geltendmachung seiner Ansprüche eine außergerichtliche Lösung zu suchen. Diese außergerichtliche Lösung beinhaltet die Beseitigung der bereits eingetretenen Verletzung von Verwertungsrechten durch das Entfernen des Fotos von der Homepage des Handwerkers. Andererseits bedeutet es auch die Absicherung gegen neue, gleichartige Verletzungen. Dies wird durch das Versprechen einer Vertragsstrafe abgesichert. Die Vertragsstrafe soll immer dann zu zahlen sein, wenn der Handwerker sich an sein Versprechen, keine Fotos des Produktherstellers ohne dessen ausdrückliche Genehmigung zu verwenden, nicht hält.

Ist eine Abmahnung berechtigt und erfüllt sie die formalen Anforderungen gem. Paragraph 97a Abs. 2 UrhG, kann der Verletzte verlangen, dass die für den Rechtsanwalt aufgewendeten Kosten ersetzt werden. Fazit:

- Texte, Fotos, Musik, Videos etc. von anderen Urhebern dürfen in der Regel nur mit deren Erlaubnis auf der eigenen Website gezeigt werden. Ausnahmen gibt es für amtliche und sonst gemeinfreie Werke.

- Es gibt eine Reihe von Werken, deren Verwendung der Rechteinhaber von vornherein erlaubt hat, indem er eine sog. offene Lizenz wie z.B. eine Creative-Commons-Lizenz an jedermann vergibt. Die Nutzungsmöglichkeiten richten sich dann nach den stets am Werk anzugebenen Lizenzbestimmungen.

- Kommt es zu einer Urheberrechtsverletzung, sind neben Rechtsanwaltskosten bei schuldhaften, d.h. vorsätzlichem oder fahrlässigem Handeln, auch Schadensersatzansprüche des Rechteinhabers gegeben, Paragraph 97 Abs. 2 UrhG. Die Höhe des Schadensersatzes wird häufig dadurch ermittelt, dass der für die Erlaubnis zu zahlende Betrag mit einem Aufschlag, dem sog. „Verletzerzuschlag“, versehen wird.

- Verpflichtungs- und Unterlassungserklärungen sollten immer durch einen Rechtskundigen überprüft werden.

Aufbewahrung und Archivierung

E-Mails werden häufig aus dem verwendeten E-Mail-Programm wie z.B. Outlook, Thunderbird oder Web-Mail abgelegt und dann gelöscht, wenn der Speicherplatz des Postfachs knapp wird. E-Mail-Anhänge werden häufig ausgedruckt und klassisch aufbewahrt. Dass jedoch gesetzliche Anforderungen einer solchen Praxis entgegenstehen können, wird dabei zu oft nicht erkannt.

Fallbeispiel: Elektronische Eingangsrechnung

Ein Handwerker bestellt Material über eine Einkaufsgenossenschaft, der er angehört. Die Abrechnung erfolgt auf elektronischem Wege. Hierzu wird dem Betrieb von der Genossenschaft eine Monatsrechnung als PDF-Dokument im Anhang zu einer E-Mail übermittelt. Im Betrieb wird die Rechnung ausgedruckt. Sie wird mit den übrigen Belegen an den Steuerberater weitergereicht. Da das Aufrufen der PDF-Rechnung regelmäßig zu Fehlermeldungen führt, wird sie in ein Grafikformat umgewandelt. Die Grafikdatei wird im System abgelegt, die PDF bleibt bei der E-Mail. Mail und Anhang werden entsprechend den Postfacheinstellungen sechs Monate nach Eingang gelöscht. Bei einer Außenprüfungen beanstandet das Finanzamt diese Vorgehensweise und möchte den Vorsteuerabzug nicht gewähren.

- Haben Rechtsmittel des Handwerkers gegen die Versagung des Vorsteuerabzuges Aussicht auf Erfolg?

Überlegungen zur IT-Compliance

Rechtsmittel des Handwerkers gegen die Versagung des Vorsteuerabzuges haben – unabhängig von der in diesem Rahmen übergangenen Frage, welches Rechtsmittel hier statthaft ist – nur dann Aussicht auf Erfolg, wenn dem Handwerksbetrieb der Abzug zu Unrecht versagt wurde. Dies wäre insbesondere dann der Fall, wenn der Betrieb mit den vorhandenen Dokumenten eine zum Vorsteuerabzug berechtigende Rechnung vorlegen kann, die den Anforderungen aus Paragraph 14 und 15 des Umsatzsteuergesetzes (UStG) genügt.

Gemäß Paragraph 14 Abs. 1 S. 8 UStG kann es sich bei einer Rechnung, die in einem elektronischen Format ausgestellt und auch empfangen wird, um eine solche zum Vorsteuerabzug berechtigende Rechnung handeln. Es handelt sich um eine solche, wenn insbesondere die Echtheit der Herkunft der Rechnung und die Unversehrtheit ihres Inhaltes gewährleistet sind (Paragraph 14 Abs. 3 Nr. 1 UStG). In der Praxis werden PDF-Rechnungen daher mit einer qualifizierten elektronischen Signatur versehen. Bei der qualifizierten elektronischen Signatur handelt es sich der Sache nach um ein besonderes technisches Verfahren, in dem Daten mit Authentizitäts- und Identitätsmerkmalen so verwoben werden, dass jede nachträgliche Änderung die Signatur als elektronisches Siegel zerstört. Folglich führt auch die Umwandlung der PDF-Rechnung in ein Grafikformat wie z.B. JPEG oder eine Bitmap zur Zerstörung des Siegels. Als Ergebnis dieser Zerstörung lassen sich die Identität des Ausstellers und die Authentizität des Inhalts nicht mehr belegen. Letztlich taugt damit die umgewandelte Datei nicht mehr als zum Vorsteuerabzug berechtigende Rechnung.

Aus einem weiteren Grund sollte die Umwandlung der PDF-Rechnung in ein anderes Format unterbleiben. Aufgrund der Anforderungen der Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff (GoBD) des Bundesfinanzministeriums ist es erforderlich, eine einmal hergestellte

maschinelle Auswertbarkeit von steuerrelevanten Unterlagen – also auch von Eingangsrechnungen – beizubehalten. So ist es nach Randziffer (Rz.) 129 der GoBD ausdrücklich unzulässig, PDF/A-Dateien der Norm PDF/A-3 in eine reine Bilddatei wie z.B. ein JPEG, TIFF oder BMP etc. umzuwandeln. Durch die Umwandlung geht der für den Nutzer nicht ohne weiteres sichtbare, der Datei aber beigegebene XML-Datensatz, in dem in strukturierter Form die Rechnungsinformationen maschinenlesbar abgelegt sind, verloren.

Fazit:

- Eingangsrechnungen wie auch Ausgangsrechnungen, die in einem elektronischen Format vorliegen, müssen in diesem Format auch revisionssicher aufbewahrt werden, so dass sie bei einer Prüfung durch das Finanzamt vorgelegt und ggf. maschinell ausgewertet werden können.

- Werden als PDF-Datei eingehende Rechnungen in andere Formate umgewandelt, muss die Originaldatei als für die Prüfung maßgebliches Dokument aufbewahrt und vorgelegt werden können.

- Elektronische Signaturen gewährleisten die Echtheit und die Unversehrtheit elektronischer Dokumente. Werden signierte elektronische Dokumente verändert, wird das elektronische Sigel gebrochen und die Manipulation dadurch erkennbar. Manipulierte Dokumente sind zur Beweisführung ungeeignet.

Im Ergebnis dürfte daher mit sehr hoher Wahrscheinlichkeit ein Rechtsmittel des Handwerkers gegen die Versagung des Vorsteuerabzuges im Fallbeispiel keine Aussicht auf Erfolg haben. Wegen der Verletzung der Anforderungen der GoBD hat das Finanzamt darüber hinaus die Möglichkeit, eine Steuerschätzung vorzunehmen. Auch wenn die GoBD „lediglich“ interne Verwaltungsanweisungen an den Außenprüfer des Finanzamtes darstellen und nicht völlig ausgeschlossen ist, dass einzelne Anforderungen einer gerichtlichen Überprüfung nicht Stand halten würden, ist das wirtschaftliche Risiko der Außerachtlassung der Vorgaben beachtlich und kann existenzbedrohend wirken.

Fallbeispiel: E-Mail als Geschäftsbrief

Vorgang ähnlich wie im vorherigen Fallbeispiel. Allerdings verlangt der Prüfer die Vorlage von weiteren Unterlagen, aus denen einzelne Geschäftsvorfälle hervorgehen und mit denen insbesondere Änderungen plausibilisiert werden können. Es stellt sich heraus, dass Absprachen mit Kunden per E-Mail getroffen wurden. Die E-Mails werden aber entsprechend den Einstellungen des E-Mail-Programms sechs Monate nach Eingang gelöscht und nicht aufbewahrt.

- Liegt ein Verstoß gegen Aufbewahrungspflichten vor?

Überlegungen zur IT-Compliance

Es ist möglich, Geschäftsbriefe in Form einer E-Mail zu versenden. Ob eine E-Mail ein Geschäftsbrief im Rechtssinne ist, richtet sich allein nach dem Zweck, zu dem sie versendet wird. Möchte man auf Papier verzichten, muss folglich auch die E-Mail alle Angaben enthalten, die beim klassischen Papier-Brief in den Pflichtangaben zum Unternehmen anzubringen sind. Wenn ein Geschäftsbrief versendet oder empfangen wird, gelten für diesen unabhängig von dem gewählten Kommunikationsformat stets die handels- und steuerrechtlichen Vorgaben. Je nach Branchenzugehörigkeit sind weitere spezifische Aufbewahrungspflichten zu beachten.

Die bereits zum vorherigen Fallbeispiel erwähnten GoBD gelten sowohl für eine Aufbewahrung in Papier wie auch eine solche in elektronischer Form. Es ist also sicherzustellen, dass eingegangene und abgesendete Geschäftsbriefe nicht mehr nachträglich verändert werden können und Veränderungen nachvollziehbar sind. Dies ist nicht gewährleistet, wenn E-Mails lediglich im E-Mail-Programm beim Empfänger lokal abgelegt werden. Denn bleiben E-Mails im E-Mail-Postfach abrufbar ist eine Änderung des Erklärungsinhalts möglich, ohne dass dies auffallen muss.

Fazit:

- Es erscheint empfehlenswert, eine am Markt etablierte Archivierungslösung einzusetzen.

- Die auf dem Markt befindlichen Archivierungslösungen basieren auf verschiedenen Sicherungsstrategien und unterscheiden sich teils recht erheblich in ihrer technischen Komplexität sowie den mit ihrer Einrichtung und ihrem Betrieb verbundenen Aufwänden und Kosten.

- Die für den jeweiligen Betrieb passende Archivierungslösung lässt sich nur durch einen Abgleich der individuellen Anforderungen im jeweiligen Betrieb mit den Leistungsumfängen der beziehbaren Archivierungslösung ermitteln.

Setzt ein Handwerker in seinem Betrieb eine der gängigen Branchenlösungen ein, bietet der Hersteller regelmäßig auch eine GoBD-konforme Archivierungskomponente für mit seiner Software erzeugte Geschäftsbriefe an, die als PDF oder in Papier versendet werden. Geschäftsbriefe, die als E-Mail versendet werden, werden jedenfalls derzeit nach Auskunft der Hersteller noch nicht automatisiert archiviert. Hierzu ist der Einsatz einer eigenen E-Mail-Archivierungslösung erforderlich.

Dokumentation des IT-Einsatzes

Mit der Datenschutz-Grundverordnung wird das Rechenschaftsprinzip in das Datenschutzrecht eingeführt. Das bedeutet, dass der für eine Verarbeitung personenbezogener Daten Verantwortliche jederzeit den Nachweis führen können muss, dass die Datenverarbeitung durch ihn rechtmäßig erfolgt. Auch im Steuerrecht muss der Umgang mit Belegen nachvollzogen werden können, weshalb die Finanzverwaltung davon ausgeht, dass eine Steuerprüfung nur dann sinnvoll durchgeführt werden kann, wenn eine Verfahrensdokumentation vom Steuerpflichtigen zur Verfügung gestellt wird, aus der die Erzeugung und die Behandlung von aus- sowie eingehenden steuerrelevanten Unterlagen ersichtlich ist.

Fallbeispiel: Elektronisches Kassensystem

In einem Betrieb mit mehreren Betriebsstätten werden an den jeweiligen Standorten Bargeschäfte mit Kunden getätigt. Die Einnahmen werden mittels eines eigens beschafften PC-gestützten Kassensystems erfasst. Das Kassensystem verfügt über eine Schnittstelle zur eingesetzten Branchensoftware. Diese Software ermöglicht die Erstellung nach Standorten getrennter Kassenberichte. Diese Berichte lassen sich im System abspeichern. Bei einer Prüfung moniert das Finanzamt in der Sache zutreffend das Fehlen von Einrichtungsunterlagen. Ferner beanstandet der Prüfer, dass die abgespeicherten Kassenberichte weder unveränderbar fortlaufend nummeriert, noch mit einem Erzeugungsdatum versehen sind. Wegen der Mängel schätzt das Finanzamt zusätzliche Einnahmen von insgesamt 135.000 Euro. Der Betriebsinhaber ist sich keines Fehlers bewusst und bestreitet jede Manipulation. Das bei der Behörde eingelegte Rechtsmittel blieb erfolglos.

- Hat eine Klage vor dem Finanzgericht Aussicht auf Erfolg?

Überlegungen zur IT-Compliance

Eine Klage gegen den Steuerbescheid in Form des Widerspruchsbescheides hat Aussicht auf Erfolg, wenn der Steuerpflichtige durch den angefochtenen Verwaltungsakt in seinen Rechten verletzt wird. Das wäre nach dem Fallbeispiel dann der Fall, wenn der Prüfer nicht berechtigt gewesen ist, Hinzuschätzungen in dem genannten Umfang vorzunehmen.

Das Finanzgericht wird also fragen, ob das Fehlen von Einrichtungsunterlagen des Kassensystems, eine nicht fortlaufende Nummerierung und das Fehlen eines Zeitstempels bei der Erzeugung von Kassenberichten geeignet ist, die Hinzuschätzungen zu rechtfertigen. Gemäß Paragraph 96 der Finanzgerichtsordnung (FGO) i.V. mit Paragraph 162 AO kann auch das Finanzgericht die Besteuerungsgrundlagen schätzen, soweit diese nicht anders ermittelt oder berechnet werden können. Besteuerungsgrundlagen sind dann nicht anders ermittel- oder berechenbar, wenn die Kassenführung des Steuerpflichtigen nicht ordnungsgemäß ist. Nicht ordnungsgemäß ist die Kassenführung dann, wenn Bücher und Aufzeichnungen, die zu führen sind, nicht vorgelegt werden können oder die vorhandenen Unterlagen der Besteuerung nicht zugrunde gelegt werden können.

Vorhandene Kassenberichte können dann der Besteuerung nicht zugrunde gelegt werden, wenn sie die Kasseneinnahmen und die Kassenausgaben nicht täglich festhalten und Aufzeichnungen, die für die Besteuerung von Bedeutung sind, nicht geordnet aufbewahrt werden. Geordnet bedeutet, dass die erforderlichen Unterlagen

und Aufzeichnungen einem sachverständigen Dritten ermöglichen, sich in angemessener Zeit einen Überblick über die Geschäftsvorfälle zu verschaffen. Dies ist dann nicht mehr der Fall, wenn bei der Nutzung programmierter elektronischer Kassensysteme Programmierprotokolle nicht vorgelegt werden können.

Fazit:

- Es ist im Betrieb sicherzustellen, dass die Belegerzeugung und die Behandlung von Eingangs- sowie Ausgangsbelegen von einem sachverständigen Dritten, insbesondere dem Prüfer des Finanzamtes nachvollzogen werden kann.

- In den GoBD ist festgehalten, dass eine Verfahrensdokumentation zu führen und erforderlichenfalls auch vorzulegen ist. Zu dieser Dokumentation gehören auch ggf. Handbücher des eingesetzten Datenverarbeitungssystems.

- Für die Verfahrensdokumentation gelten dieselben Aufbewahrungsfristen wie für die am längsten innerhalb des Verfahrens erzeugten und empfangenen Belege, d.h. bei Änderungen des Verfahrens muss die Dokumentation des zuvor angewendeten Verfahrens archiviert und darf nicht vernichtet werden, ggf. ist eine Versionierung vorzunehmen und kenntlich zu machen.

Im Ergebnis wird daher das Finanzgericht den Widerspruchsbescheid vermutlich nicht abändern oder aufheben. Die Einrichtung des Kassensystems, seine Funktionsweise sowie die Art und Weise der Erzeugung und der anschließende Umgang mit den Belegen können im Fallbeispiel von dem Prüfer nicht nachvollzogen werden. Es hätte von dem mit der Einrichtung befassten Mitarbeiter oder Dienstleister eine Dokumentation erstellt und diese zur Vorlage bei einer Prüfung zur Verfügung gestellt werden müssen.

Fallbeispiel: Verzeichnis der Verarbeitungstätigkeiten

Ein Handwerksbetrieb hat nach mehreren Einbrüchen in die Werkhalle eine Videokamera an der Gebäudeecke zur Zufahrt zur Straße angebracht. Ein Nachbar, dem die Kamera ein Dorn im Auge ist, hat sich an die Datenschutz-Aufsichtsbehörde mit der Behauptung gewendet, die Kamera erfasse auch den öffentlichen Gehsteig. Ein Mitarbeiter der Behörde sucht den Betrieb auf. Er erhält von dem Betriebsinhaber die zutreffende Auskunft, dass die Kamera während der Zeiten, in denen das Büro besetzt ist, abgeschaltet ist. Außerhalb dieser Zeiten wird dann eine Aufnahme ausgelöst und auf Festplatte aufgezeichnet, wenn ein Bewegungsmelder anspricht. Die Aufzeichnungen werden am Folgetag durchgesehen und gelöscht, wenn keine auffälligen Aktivitäten erkennbar sind. Der Mitarbeiter der Aufsichtsbehörde erbittet das Verzeichnis der Verarbeitungstätigkeiten. Als der Inhaber angibt, ein solches nicht vorlegen zu können, wird ihm Gelegenheit gegeben, das Versäumnis zu beheben und für den Fall, dass er diese Chance ungenutzt verstreichen lässt, eine Geldbuße angedroht.

- Kann die Datenschutz-Aufsichtsbehörde wegen der Nichtvorlage des Verzeichnisses tatsächlich eine Geldbuße verhängen?

Überlegungen zur IT-Compliance

Gemäß Art. 30 DS-GVO ist ein für die Verarbeitung personenbezogener Daten Verantwortlicher verpflichtet, ein Verzeichnis der Verarbeitungstätigkeiten zu führen. Dieses hat den in der vorgenannten Norm definierten Inhalt aufzuweisen. Für die Datenverarbeitung Verantwortlicher ist gem. Art. 4 Nr. 7 DS-GVO vereinfacht ausgedrückt derjenige, der über das *Ob* und das *Wie* der Datenverarbeitung entscheidet. Da hier der Betriebsinhaber die Kamera angebracht und die Einrichtung vorgenommen und den Umgang mit den Aufnahmen definiert hat, ist er Verantwortlicher in diesem Sinne.

Allerdings könnte es fraglich erscheinen, ob durch das Kamerasystem überhaupt personenbezogene Daten im Sinne der DS-GVO erhoben werden. Betrachtet man die Vorgänge genauer und berücksichtigt man den mit der Videoaufzeichnung verfolgten Zweck, dann wird deutlich, dass es darum geht, einen potenziellen Einbrecher bei seiner Tat zu beobachten und möglicherweise nachträglich ausfindig machen zu können. Da derjenige, der – gleich ob als Besucher oder Einbrecher – den Bewegungsmelder aktiviert und dadurch die Aufzeichnung auslöst, betroffene Person gem. Art. 4 Nr. 1 DS-GVO ist, muss ein Verzeichnis der Verarbeitungstätigkeiten gem. Art. 30 DS-GVO geführt werden.

Verletzt der Verantwortliche die Pflicht zur Führung eines Verzeichnisses der Verarbeitungstätigkeiten, kann die Datenschutz-Aufsichtsbehörde eine Geldbuße verhängen. Bei der Bestimmung der Höhe des Bußgeldes berücksichtigt die Behörde insbesondere die Art, Schwere und Dauer des Verstoßes. Ferner bezieht die Behörde den Zweck der Verarbeitung und die Zahl der betroffenen Personen ein.

Besondere Berücksichtigung findet auch ein etwa entstandener Schaden. Schließlich finden auch der Grad des Verschuldens und Milderungs- sowie Wiedergutmachungsbemühungen Eingang in die Bemessung.
Das mögliche Bußgeld ist gemäß DS-GVO auf 10 Millionen Euro bzw. 2 Prozent des weltweit erzielten Vorjahresumsatzes begrenzt.

Fazit:

- In einem Betrieb ist das Führen eines Verzeichnisses der Verarbeitungstätigkeiten gem. Art. 30 DS-GVO regelmäßig vorgeschrieben und erforderlich.

- Die Ausnahme von der Pflicht zum Führen eines Verzeichnisses für Betriebe mit weniger als 250 Mitarbeitern greift in Deutschland wegen der notwendigen Verarbeitung besonderer personenbezogener Daten i.S. von Art. 9 DS-GVO in Form von Religionszugehörigkeits- und Arbeitsunfähigkeitsinformationen im Rahmen der Lohn- und Gehaltsabrechnung der Mitarbeiter nicht ein.

Braucht man einen Datenschutzbeauftragten?

Betriebsinhaber und Geschäftsführer sehen sich regelmäßig mit datenschutzrechtlichen Anforderungen konfrontiert, deren Bedeutung und Tragweite das Gefühl von Überforderung hervorrufen. In dieser Situation stellt sich für sie insbesondere die Frage, ob die Bestellung eines Datenschutzbeauftragten erforderlich ist. Ferner wird überlegt, ob durch eine Bestellung Haftungsrisiken auf diesen delegiert werden können.

Ob ein Datenschutzbeauftragter für den Betrieb bestellt werden muss, richtet sich nach der Zahl der im Betrieb mit der ständigen Verarbeitung personenbezogener Daten betrautenr Mitarbeiter. Betriebe, die regelmäßig mehr als zehn Mitarbeiter mit der Verarbeitung personenbezogener Daten betrauen, sind zur Benennung eines internen oder externen Datenschutzbeauftragten verpflichtet. Es kann nicht irgendein Mitarbeiter zum Datenschutzbeauftragten ernannt werden, sondern es muss eine an den gesetzlichen Anforderungen ausgerichtete Auswahl erfolgen.

Da der Datenschutzbeauftragte in der Hauptsache den für die Datenverarbeitung bei der Erfüllung seiner datenschutzrechtlichen Verpflichtungen beraten und unterstützen soll, bleibt es im Verhältnis zum von der Verarbeitung Betroffenen stets bei einer umfassenden Verantwortlichkeit des Betriebes und damit letztlich im Falle eines Organisationsmangels bei einer Haftung des Betriebsinhabers bzw. des Geschäftsführers. Im Innenverhältnis zwischen dem Betrieb und dem Datenschutzbeauftragten kann sich eine Haftung des Beauftragten aus der konkreten Gestaltung des betreffenden Dienstverhältnisses ergeben.

Fazit:

- Werden mehr als zehn Personen mit der regelmäßigen Verarbeitung personenbezogener Daten betraut, ist gem. § 38 Abs. 1 BDSG ein betrieblicher Datenschutzbeauftragter zu bestellen. Die Zahl von zehn Mitarbeitern wird schnell erreicht, wenn die Mitarbeiter mit mobilen Endgeräten ausgestattet werden, die zur Verarbeitung von Kundendaten wie z.B. Auftragsinformationen zu einem bestimmten Projekt unter einer bestimmten Anschrift bestimmt sind.

- Der Datenschutzbeauftragte darf Mitarbeiter des bestellenden Betriebes sein (interner Datenschutzbeauftragter). Es darf aber auch ein externer, in jedem Fall aber namentlich zu benennender Dienstleister sein (externer Datenschutzbeauftragter).

- Bestellt werden darf nur, wer über die persönliche und fachliche Eignung verfügt. Die Bestellung darf den Datenschutzbeauftragten nicht in Interessenkonflikte stürzen. Daher können insbesondere der Geschäftsführer und ein etwa angestellter Leiter einer betriebsinternen IT-Abteilung nicht zu Datenschutzbeauftragten bestellt werden.

Ist ein Datenschutzbeauftragter bestellt, wird dieser auf das Erstellen und Führen eines Verzeichnisses der Verarbeitungstätigkeiten hinwirken. Da ein Formularzwang nicht besteht und schon deshalb bei den zur Führung des Verzeichnisses Verpflichteten eine allenfalls vage Vorstellung davon vorhanden, wie ein solches Verzeichnis konkret zu gestalten ist, hat das Bayerische Landesamt für Datenschutzaufsicht seine Vorstellung in recht konkreten Mustern über seinen Internetauftritt öffentlich zugänglich gemacht. Der Internetauftritt des Landesamtes ist erreichbar unter https://www.lda.bayern.de.

Auf die Ausgangsfrage ist also zu antworten, dass die Datenschutz-Aufsichtsbehörde eine Geldbuße verhängen kann. Im Falle von Organisationsmängeln kann sie von dem Geschäftsführer des Betriebs zu ersetzen sein. Wegen seiner Beratungsfunktion kann Ersatz für die Geldbuße nur im Ausnahmefall von dem Datenschutzbeauftragten erlangt werden.

Überwachung der Betriebsabläufe

Im betrieblichen Alltag ist es bisweilen schwer leistbar, alle Einzelheiten im Blick zu haben. Daher muss man als Geschäftsleiter auf ein weisungskonformes Verhalten seiner Mitarbeiter vertrauen können. Gleichwohl muss auch gewährleistet werden, dass Betriebs- und Arbeitsanweisungen auch befolgt werden.

Fallbeispiel: Arbeitsanweisungen zur Belegablage

Nachdem der Betrieb aus der Beanstandung des Umgangs mit elektronischen Rechnungen durch den Außenprüfer des Finanzamtes (s.o. ▶Aufbewahrung und Archivierung) gelernt hat, wie eine GoBD-konforme Belegablage zu erfolgen hat, hat der Betriebsleiter eine entsprechende Arbeitsanweisung herausgegeben. Nach dieser Arbeitsanweisung sind von elektronischen Eingangsrechnungen am Tag des Eingangs Ausdrucke zu fertigen und diese in den Belegordner für den Steuerberater zu heften. Ferner ist die betreffende E-Mail samt Rechnungsdatei in einem speziell eingerichteten Rechnungseingangsarchiv abzulegen. Trotz einer Teilautomatisierung erfordert die Ablage im Archiv noch eine manuelle Auswahl der betreffenden E-Mail und händisches Verschieben ins Rechnungsarchiv. Weil ihm die Handhabung zu umständlich ist, lässt der zuständige Mitarbeiter die Belegablage schleifen und archiviert die Rechnungseingänge erst kurz vor Monatsende. Dadurch werden Belege nicht immer chronologisch durch das System nummeriert und archiviert.

- Droht dem Betrieb bei der nächsten Prüfung durch das Finanzamt erneut eine Beanstandung?

Überlegungen zur IT-Compliance

Dem Betrieb droht dann eine erneute Beanstandung durch den Prüfer des Finanzamtes, wenn die tatsächliche Vorgehensweise des Mitarbeiters bei der Belegablage nicht den gesetzlichen Anforderungen genügen kann. Für die Außenprüfung hat das Bundesministerium der Finanzen die GoBD an die obersten Finanzbehörden der Länder herausgegeben. Die GoBD enthalten Anweisungen an den Außenprüfer, wie bei einer Außenprüfung vorzugehen und worauf besonderes Augenmerk im Hinblick auf die Frage der Einhaltung der gesetzlichen Anforderungen an eine ordnungsgemäße Buchführung und Aufbewahrung zu richten ist.

In Ziffer 4 der GoBD ist das Belegwesen behandelt. Darin ist insbesondere bestimmt, dass Belege in Papier oder in elektronischer Form möglichst zeitnah, d.h. unmittelbar nach ihrem Eingang oder ihrer Entstehung gegen einen Verlust zu sichern sind. Es ist ausdrücklich zulässig, bei elektronischen Belegen die fortlaufende Nummer automatisiert durch ein IT-System vergeben zu lassen. Der Steuerpflichtige ist verpflichtet, organisatorisch und technisch sicherzustellen, dass elektronische Buchungen und Aufzeichnungen, vollständig, richtig, zeitgerecht und geordnet vorgenommen werden. Dies erfordert insbesondere im Falle der doppelten Buchführung die Abbildung aller Geschäftsvorfälle in ihrer zeitlichen Reihenfolge.

Die Einhaltung dieser Anforderungen hat der Steuerpflichtige mittels eines internen Kontrollsystems (IKS) fortlaufend zu kontrollieren. Art und Weise der Kontrolle haben sich nach der Komplexität des Geschäftsbetriebes und des eingesetzten Systems zu richten. Die Ausübung der Kontrolle ist zu protokollieren. Für durch mangelnde Kontrolle entstandene Fehler ist der Steuerpflichtige verantwortlich. Treten Fehler auf, genügen die technischen und organisatorischen Maßnahmen nicht, um die Einhaltung der steuerrechtlichen Anforderungen

sicherzustellen. Es muss folglich nachgebessert werden.

Wie das IKS konkret ausgestaltet ist, muss von dem Steuerpflichtigen in der gemäß GoBD erforderlichen Dokumentation (s.o. ▶Dokumentation des IT-Einsatzes, 1. Fallbeispiel) festgehalten werden. Allerdings sind mit Kontrollen nicht nur persönliche und händische Kontrollen des Steuerpflichtigen gemeint, sondern es lassen sich auch Prüfungsvorgänge automatisieren. So werden in gängigen Branchensoftware-Lösungen bereits eine Reihe von Maßnahmen realisiert, die eine GoBD-konforme Behandlung von Geschäftsvorfällen sicherstellen helfen. So gehören etwa die Abbildung von Rechte- und Rollenkonzepten sowie Plausibilitätskontrollen bei der Eingabe und Ausgabe von Daten regelmäßig zur Standardfunktionalität der angebotenen Softwarelösungen.

Fazit:

- Zur Erfüllung von Organisationspflichten ist es nicht ausreichend, die Einhaltung gesetzlicher Anforderungen im Wege von Betriebs- und Arbeitsanweisungen abzusichern. Es braucht auch automatisierte sowie persönliche Kontrollen.

- Auf Abweichungen von Betriebs- und Arbeitsanweisungen muss zur Vermeidung von Nachteilen unverzüglich reagiert werden.

- Unerwünschtes, weisungswidriges Verhalten ist zu dokumentieren, mit dem betreffenden Mitarbeiter zu erörtern und abzustellen. Die Abhilfemaßnahmen sollten ebenfalls dokumentiert werden.

Im Fallbeispiel droht eine erneute Beanstandung des Umgangs mit elektronischen Eingangsrechnungen. Zwar wurde der rechtskonforme Umgang mit Eingangsrechnungen in einer Arbeitsanweisung gegenüber dem betreffenden Mitarbeiter verbindlich modelliert. Letztlich wurde aber die Einhaltung der Arbeitsanweisung nicht ausreichend kontrolliert, um einen Verstoß gegen die Arbeitsanweisung unmittelbar abstellen zu können.

Fallbeispiel: WLAN-Sicherung

Ein Unternehmen hat im Bürotrakt des Betriebsgebäudes ein WLAN eingerichtet. Dieses wird über einen handelsüblichen Router zur Verfügung gestellt. Über das WLAN werden den Mitarbeitern auf ihre betrieblichen Smartphones und Tablet-PC die Kundendaten und Arbeitsaufträge aufgespielt. Damit keine Betriebsfremden das WLAN nutzen oder gar missbrauchen, hat der Geschäftsführer einen Netzwerkschlüssel individuell eingerichtet. Dabei bediente er sich der zu dieser Zeit üblichen Verschlüsselung sowie deren Einrichtung.

- Muss der Betriebsinhaber eine stärkere Verschlüsselungstechnik einsetzen, wenn eine solche verfügbar wird?

Überlegungen zur IT-Compliance

Die Frage, ob ein WLAN nur verschlüsselt betrieben werden darf, wird seit der umfassenden Verfügbarkeit der Funknetzwerktechnik recht kontrovers unter Juristen diskutiert. In der Regel streiten sich die Vertreter von Inhabern von Urheber- und Leistungsschutzrechten mit Gewerbetreibenden unterschiedlichster Branchen, die ihren Kunden während eines Aufenthalts in Geschäftsräumen als kleinen Service den Zugang zum Internet eröffnen möchten, um die Verantwortlichkeit für Rechtsverletzungen unter Nutzung dieses Internetzugangs. Aber auch gegen private WLAN-Betreiber werden gerichtliche Verfahren angestrengt. Ein solcher Rechtsstreit endete mit einem grundlegenden Urteil des Bundesgerichtshofes (BGH), das unter dem Namen des Musiktitels bekannt ist, das rechtswidrig über eine Internet-Tauschbörse anderen Internetnutzern zugänglich gemacht worden sein soll: „Sommer unseres Lebens“.

In seiner Entscheidung führt der Erste Zivilsenat des BGH zur Frage der Verschlüsselungspflicht aus, dass der Betreiber eines privaten WLAN dann für eine Rechtsverletzung durch einen Nutzer seines Funknetzwerks haftet, wenn das Funknetzwerk nicht durch den Einsatz von im Zeitpunkt der Anschaffung des Routers üblicher Verschlüsselungstechnik gegen eine unbefugte Nutzung durch Dritte geschützt wird.

Diese sogenannte Störerhaftung sollte durch eine Reform des Telemediengesetzes abgemildert werden. Dies stellte den Gesetzgeber vor ganz erhebliche Herausforderungen, so dass die Reform zweimalig nachgebessert werden musste. Schließlich wurde die Störerhaftung durch einen Anspruch des Rechteinhabers gegen den WLAN-Betreiber auf Sperrung gem. Paragraph 7 Abs. 4 S. 1 TMG ersetzt. Der Anspruch entsteht allerdings nur, wenn das WLAN zur Verletzung von Rechten am geistigen Eigentum genutzt wurde und dem Rechteinhaber keine anderen Möglichkeiten zum Schutz seiner Rechtsposition zur Verfügung stehen. Der Umfang des Anspruchs ist auf dem WLAN-Betreiber zumutbare Maßnahmen begrenzt.

Fazit:

- Die Verschlüsselung des WLAN zur Verhinderung von Verletzungen des Rechts am geistigen Eigentum durch einen Nutzer war vor der Reform des Telemediengesetzes nach dem im Zeitpunkt der Anschaffung üblichen Technik und Methode vorzunehmen.

- Nach der Reform des Telemediengesetzes lässt sich

mit Wirkung vom 13. Oktober 2017 an eine solche präventive Verpflichtung des WLAN-Betreibers nicht mehr erkennen.

- Der WLAN-Betreiber kann im Falle einer Rechtsverletzung zu Lasten eines Dritten durch einen WLAN-Nutzer gem. Paragraph 7 Abs. 4 S. 1 TMG gleichwohl verpflichtet sein, Sperr- und Schutzmaßnahmen zu ergreifen.

Neben der Verpflichtung, den Internetzugang über ein WLAN so zu konfigurieren, dass es nicht zu Rechtsverletzungen zu Lasten Dritter kommt, stellt sich die Frage, ob ein WLAN, über das personenbezogene Daten übertragen werden, schon unter datenschutzrechtlichen Gesichtspunkten nicht offen, das heißt also unverschlüsselt betrieben werden darf.

Mit Blick auf die Sicherheit der Verarbeitung personenbezogener Daten – also auch einer Übertragung von einem Gerät auf ein anderes und damit wie im Fallbeispiel von Kunden- und Personalinformationen – ist in der DS-GVO angeordnet, dass der für die Datenverarbeitung Verantwortliche – im Fallbeispiel also das Unternehmen vertreten durch seinen Geschäftsführer – geeignete technische und organisatorische Maßnahmen trifft, die geeignet sind sicherzustellen, dass die betreffenden Daten nur von Berechtigten wahrgenommen werden können. Ob eine Maßnahme geeignet ist, beurteilt sich nach der Art und dem Umfang sowie der Umstände und Zwecke der Datenverarbeitung. Es muss betrachtet werden, mit welcher Wahrscheinlichkeit es zu Beeinträchtigungen der Rechte der betroffenen Personen – im Fallbeispiel also der Mitarbeiter und der Kunden – kommen kann und wie schwerwiegend die denkbare Beeinträchtigung sein würde.

Als technische und organisatorische Maßnahme wird explizit die Verschlüsselung genannt. Ferner werden Verfahren zur regelmäßigen Überprüfung der ergriffenen Maßnahmen erwähnt. Bewertung und Evaluation der der Wirksamkeit von technisch-organisatorischen Maßnahmen zur Gewährleistung von Sicherheit sind ebenfalls explizit in der DS-GVO aufgeführt. Es ist kritisch zu fragen, ob das mittels der tatsächlich ergriffenen technischen und organisatorischen Maßnahmen erreichte Schutzniveau ausreicht. Dabei ist gemäß DS-GVO besonders zu berücksichtigen, welche Risiken für die betroffenen Personen aus einer Offenlegung oder der Ermöglichung unberechtigten Zugriffs auf die ihnen zuzuordnenden Informationen entstehen.

Die von dem für die Datenverarbeitung Verantwortlichen eingesetzten technischen Maßnahmen zur Gewährleistung des Datenschutzes müssen sowohl im Zeitpunkt ihrer Festlegung wie auch zu jedem späteren Zeitpunkt das erforderliche Schutzniveau gewährleisten können. Unter Anwendung der Anforderungen aus der Datenschutz-Grundverordnung ist das einmal erreichte Schutzniveau dauerhaft nachzuhalten. Dies bedeutet, dass rechtlichen und technischen Neuerungen Rechnung getragen werden muss.

Im Ergebnis genügt es daher nicht (mehr), bei der Beschaffung eines Systems die zu diesem Zeitpunkt üblichen Standards zur Sicherung anzuwenden. Vielmehr ist erforderlich, ein gleichbleibendes Schutzniveau über den gesamten Lebenszyklus eines Datenverarbeitungsvorgangs aufrecht zu erhalten.

Fazit:

- Die Verwendung eines WLAN-Schlüssels ist bei der Nutzung eines Funknetzwerks zur Übertragung (auch) personenbezogener Daten unter datenschutzrechtlichen Gesichtspunkten alternativlos.

- Ein Unternehmen ist nicht gehindert, seinen Kunden ein gesondert zu betreibendes „Kunden-WLAN“ zur Verfügung zu stellen. Dieses sollte so konfiguriert sein, dass Rechtsverletzungen zu Lasten Dritter vermieden werden.

- Die Dynamik in Technik und Recht setzt voraus, dass der für die Datenverarbeitung Verantwortliche technische und rechtliche Entwicklungen kontinuierlich überwacht, um zur Aufrechterhaltung des Datenschutzes und der Datensicherheit ggf. erforderliche Anpassungen zeitgerecht vornehmen zu können.

Die Frage, ob eine am Markt verfügbare stärkere Verschlüsselung tatsächlich eingesetzt werden muss, beantwortet sich nach der Zumutbarkeit – insbesondere dem Verhältnis zwischen Kosten und Sicherheitsgewinn – der zu tätigenden Investitionen und Aufwände.

Einspielen erforderlicher Änderungen

Die Notwendigkeit, Verfahrensweisen festzulegen, wie man mit veralteter Technik umgeht, und in welcher Weise auf die Änderung rechtlicher Rahmenbedingungen zu reagieren ist, folgt aus dem oben zur Überwachung der Betriebsabläufe Gesagten. Eine Verletzung der Pflicht, den Betrieb in einer Weise zu organisieren, dass es nicht zur Verletzung von gesetzlichen Vorgaben und Anforderungen kommt, ist – wie bereits eingangs (s.o. ▶Ausgangspunkt: Definition der IT-Compliance und Legalitätspflicht) ausgeführt – zu vermeiden. Dies bedeutet jedoch nicht, dass dem Unternehmer jeglicher Freiraum für die Gestaltung seines Betriebes genommen wäre.

Fallbeispiel: Assistierte Maschinenbedienung

Der Geschäftsführer eines Malerbetriebes hat zur Erhöhung der Effizienz ein Spritzgerät angeschafft, mit dem Farbe nicht mehr mittels Farbrolle aufgebracht werden muss, sondern zeitsparend gespritzt werden kann. Die Bedienung des Spritzgeräts erfordert allerdings einige besondere Kenntnisse, die sowohl bei der Einrichtung der Baustelle wie auch im Störungsfalle eine schnelle Problemlösung ermöglichen. Deshalb ist die Arbeit mit der Maschine bei den Mitarbeitern nicht sonderlich beliebt und die recht teure Anschaffung bleibt regelmäßig ungenutzt im Betrieb. Der Geschäftsführer überlegt, wie er die Mitarbeiter dazu bewegen kann, das zeitsparende und ressourcenschonende Spritzen mit der Maschine dem Auftragen der Farbe mit der Farbrolle vorzuziehen...

- Welche grundlegenden Überlegungen sind anzustellen?

Überlegungen zum Technikeinsatz

Der Einsatz moderner Maschinentechnik verspricht in der Regel eine höhere Effizienz. Diese Effizienzerhöhung muss betriebswirtschaftlich die Ausgabe für die Anschaffung der Maschine rechtfertigen. Dies gelingt jedoch nicht, wenn die neue Technik gar nicht zum Einsatz kommt. Mangelnde Akzeptanz der Änderung der Arbeitsweise und eine für den in der Maschinenbedienung nicht geübten Anwender un- oder missverständliche Anleitungen setzen Hürden, die von dem Unternehmer überwunden werden müssen, um das Ziel erreichen zu können.

Im Einzelfall lässt sich auch die Angst einzelner Mitarbeiter beobachten, wegen fehlender Kompetenz im Umgang mit der Technik den Arbeitsplatz zu verlieren. Dabei möchte der Geschäftsführer auf die im Laufe des Berufslebens erworbene Problemlösungskompetenz des erfahrenen Mitarbeiters gar nicht verzichten.

Diese Gemengelage aufzulösen ist keine Aufgabe, die simple Lösungen erlaubt. Eine naheliegende Schulung der Mitarbeiter an der Maschine kann nur bedingt helfen, soweit keine neuen Mitarbeiter in den Betrieb eintreten, die nachgeschult werden müssten. Der Schulungsaufwand wäre extrem hoch und es ist nicht sicher vorhersagbar, dass die in der Schulung erworbenen Kompetenzen nach Ablauf einer gewissen Zeit noch ohne weiteres abgerufen werden können. Die Maschine nur einem einzigen Mitarbeiter anzuvertrauen, der alle mit ihr auszuführenden Arbeiten verrichtet, vernichtet den Vorteil des flexiblen Einsatzes. Kaum zielführend wäre es auch, einen leibhaftigen Assistenten für die Maschinenbedienung zu beschäftigen. Dies ändert sich aber, wenn dieser Assistent elektronisch und auf Zuruf zur Verfügung stehen könnte.

Eine elektronische Bedienungsanleitung, die dem Maschinenbediener im Betrieb den sicheren Umgang mit der Maschine in einer Weise vermittelt, dass sich der Mitarbeiter nicht bevormundet, sondern unterstützt fühlt, kann helfen, Effizienzpotenziale zu heben. Dies gilt insbesondere dann, wenn die erforderlichen Informationen im situativen Kontext so zur Verfügung gestellt werden, dass sie den Mitarbeiter im Übrigen bei der Verrichtung der im übertragenen Arbeiten nicht behindern oder stören.

Ein solcher elektronischer Assistent ist heute bereits mit der SmartWerker Assistance- and Training-Suite (SWATS) vorhanden. Hier werden dem Mitarbeiter mittels einer Datenbrille diejenigen Informationen in den Sichtbereich eingespielt, die ihn in die Lage versetzen, die Maschine korrekt und effizient zu bedienen. Die Hände bleiben frei und das Blättern in einer Bedienungsanleitung aus Papier kann auch im Störungsfalle entbehrlich sein. Nicht benötigte Informationen kann der Mitarbeiter ausblenden. Erfahrungsgemäß wird nach anfänglicher Skepsis bereits nach kurzer Trainingszeit der Einsatz des Assistenten als hilfreich empfunden und geschätzt.

Fazit:

- Der Einsatz elektronischer Assistenzsysteme ermöglicht, Akzeptanzhürden beim Einsatz von neuer Maschinentechnik zu senken.
- Der Einsatz elektronischer Assistenzsysteme ermöglicht weiter, Fehlbedienungen zu vermeiden und Störungs- sowie Ausfallzeiten zu reduzieren.
- Die Anschaffungskosten für Maschine und Assistenzsystem lassen sich gut erfassen und somit leicht in eine Angebotskalkulation einstellen.

Die Anschaffung von Assistenzsystemen für die Maschinenbedienung auf der Baustelle gehört heute noch zur Ausnahme. Die Schaffung von übergreifend arbeitenden Systemen, in denen diese elektronische Assistenz ein Baustein des Gesamtsystems darstellt, scheint jedoch lediglich als eine Frage der Zeit. Dabei geht es nicht allein um Effizienz- und Gewinnmaximierung, sondern auch um messbare Qualitätsverbesserung. Diese Qualitätsverbesserung betrifft nicht nur die Ausführung der jeweiligen Arbeiten, sondern auch ein Zuwachs an Zufriedenheit und Lebensqualität bei Mitarbeitern und Kunden.

Überlegungen zur IT-Compliance

Fällt die Entscheidung zugunsten der Anschaffung eines elektronischen Assistenzsystems wie im Fallbeispiel, so stellt sich nicht nur die Frage des betriebswirtschaftlich sinnvollen Einsatzes der Technik, sondern auch deren rechtskonforme Einbindung in die IT-Landschaft des Betriebes.

Besonders datenschutzrechtliche Aspekte sind von Bedeutung. In größeren Betrieben ist bei der Einführung von Systemen, die potenziell die Möglichkeit zur Leistungskontrolle beinhalten, die Beteiligung des vorhandenen Betriebsrats zu gewährleisten. Neu eingeführte Systeme müssen in einer Weise gestaltet sein, dass sie möglichste ohne und dort wo unvermeidbar, mit so wenig wie möglich personenbezogenen Daten auskommen. Beinhaltet das System die Möglichkeit, Einstellungen personalisiert vorzunehmen, also etwa dem Assistenten „mitzuteilen“ welche spezifischen Informationen er nicht mehr anzeigen soll und welche besonders wichtig für den jeweiligen Mitarbeiter sind, dann muss in der Grundeinstellung diejenige vorgenommen werden, die am wenigsten personenbezogene Daten erfasst.

Fazit:

- Neue elektronische Systeme im Betrieb sollten möglichst ohne personenbezogene Daten betrieben werden können.
- Ist ein Betrieb ohne personenbezogene Daten nicht möglich, ist das System so zu gestalten, dass nur unverzichtbare Informationen erhoben und diese datenschutzkonform behandelt werden (Datenschutz durch Technikgestaltung).
- Ist vorgesehen, Einstellungen personalisiert vornehmen zu können, muss diejenige Voreinstellung vorgenommen werden, die am wenigsten personenbezogene Daten verarbeitet (Datenschutz durch datenschutzfreundliche Voreinstellungen).

Sind diese Grundregeln beachtet und ist geklärt, dass die Verarbeitung personenbezogener Daten im konkreten Anwendungsfall erlaubt ist, ist der neue Technikeinsatz als Verfahren in das Verzeichnis der Verarbeitungstätigkeiten (s.o. ▶ Dokumentation des IT-Einsatzes) aufzunehmen.

Vorgehensweise

Diese kleinen Fallbeispiele mit der konzentrierten und keinesfalls der juristischen Arbeitsweise vollumfänglich entsprechenden Darstellung rechtlicher Implikationen sollten dazu dienen, kritisch die im eigenen Betrieb eingeschliffenen Arbeits- und Vorgehensweisen zu hinterfragen. Gleichwohl wäre es vermessen anzunehmen, dass hierdurch eine umfassende Problemlösungskompetenz hätte vermittelt werden können.

Die Frage, die sich jeder stellen sollte ist also: „Was ist zu tun?“

Der erste Schritt ist die Prüfung der eigenen betrieblichen Organisation. Dies gelingt am ehesten, wenn man die eigene Lage mit den geschilderten Fallbeispielen vergleicht und überlegt, ob von den geschilderten Verhaltensweisen im eigenen Betrieb abgewichen wird. Dies erfordert keinesfalls, dass man im Falle des Feststellens einer Abweichung sogleich eine juristische Würdigung derselben vorzunehmen hat. Vielmehr kann es erforderlich sein, weitere Informationen zu beschaffen, um sicher feststellen zu können, ob tatsächlich eine Abweichung von dem hier beschriebenen Verhalten vorliegt und ob die Variation eine von der hier vorgestellten abweichende juristische Schlussfolgerung bedingt. Die Lösung des Problems kann also sein, weiteren Informationsbedarf zu identifizieren.

Wird ein Informationsbedarf identifiziert, um die Frage nach dem Handlungsbedarf beantworten zu können, so muss die nächste Frage lauten, auf welche Weise die Informationslücke geschlossen werden kann. Neben zahlreichen kostenfreien Angeboten insbesondere des Mittelstand 4.0-Kompetenzzentrums Planen und Bauen kann es wegen der besonderen Situation eines Betriebes sinnvoll sein, schon zur Vermeidung persönlicher Haftungsrisiken sich eines gewerblich tätigen Unternehmensberaters zu bedienen. Ist dieser für die Teilnahme an Fördermaßnahmen des Bundesministeriums für Wirtschaft und Energie (BMWi) wie z.B. Unternehmens-Wert:Mensch oder goDigital zugelassen, kann die individuelle Beratung mit einer Übernahme eines Teils der Beratungskosten gefördert werden.

Fazit:

- Die Beschaffung valider Informationen geht einer Bestimmung von Handlungsbedarf stets vor, d.h. die Ermittlung des Handlungsbedarfs setzt voraus, dass sie auf einer soliden Informationsbasis vorgenommen wird.

- Hat man in einem der geschilderten Fallbeispiele einen Sachverhalt erkannt, der sich in dieser oder in ähnlicher Form im eigenen Betrieb hätte zutragen können, spricht dies dafür, dass jedenfalls eine individuelle Prüfung der betreffenden Vorgänge erfolgen sollte.

Der zweite Schritt ist die Priorisierung von Maßnahmen. Dies erfordert eine Wertung der Dringlichkeit der Umsetzung von Maßnahmen zur Gewährleistung der IT-Compliance im Unternehmen. Dabei kann als Maßstab für Dringlichkeit die Höhe des Risikos eines dem Unternehmen entstehenden Schadens dienen.

Eine Maßnahme ist umso dringlicher, je höher das Risiko ist, dass ein Zuwarten zu einem Schaden für das Unternehmen und gegebenenfalls auch einer persönlichen Haftung des Betriebsleiters oder des Betriebsinhabers führt.

Sollte eine Gewichtung nicht ohne weiteres möglich sein, so gilt auch hier, dass die Einholung valider Infor-

mationen der Gewichtung vorgeht. Auch insoweit kann auf die fachkundige Beratung von Experten zurückgegriffen werden, die gegebenenfalls auch durch das Bundeswirtschaftsministerium in einem der diversen Programme zur Förderung der Digitalisierung unterstützt wird.

Der dritte Schritt besteht in der Erstellung eines Maßnahmenplanes. In diesem werden auf der Grundlage ausreichender Informationen der ermittelte Handlungsbedarf nach einer Priorisierung von Maßnahmen in eine zeitliche Abfolge gebracht. Der Maßnahmenplan muss berücksichtigen, ob die umzusetzenden Maßnahmen im laufenden Betrieb oder außerhalb desselben vorgenommen werden müssen bzw. können. Soweit Maßnahmen innerhalb eines laufenden Geschäftsbetriebes umzusetzen sind, kann vor allzu ambitionierten Zeitplänen nur gewarnt werden. Zu kurze Fristen zur Umsetzung bergen das Risiko von Enttäuschungen, da Ziele meist nicht kurzfristig erreicht werden können.

„Eine besondere Problematik von Compliance-Themen liegt in dem nicht ohne weiteres erkennbaren Vorteil, den das Unternehmen aus der Einhaltung von gesetzlichen Vorgaben zieht.“

Größen wie das Risiko einer Entdeckung und einer Ahndung eines rechtswidrigen Verhaltens lassen sich nur sehr schwer betriebswirtschaftlich fassen. Allerdings haben die enormen Weiterungen des Sanktionsrahmens insbesondere im Bereich der Verstöße gegen datenschutzrechtliche Grenzen im Umgang mit personenbezogenen Daten aufgeschreckt. Auch die Praxis einiger Finanzämter bei der Anwendung der GoBD und deren Rezeption in Branchenpublikationen haben einen merklichen Effekt auf die Betrachtung von Compliance-Aspekten in der betrieblichen Praxis herbeigeführt.

Dabei sind Vorteile bei näherer Betrachtung offensichtlich: Durch eine sorgfältige Planung der Vorgänge erspart man sich letztlich Aufwände und Ressourcen, die mittel- und langfristig erhebliche materielle Einsparungen mit sich bringen und die vorhandenen knappen Kapazitäten schonen. Hinzu tritt der Wegfall eines Entdeckungs- und Sanktionsrisikos, das im Hinblick auf den Rahmen der Abgabenordnung und der Datenschutz-Grundverordnung ganz erhebliche finanzielle Folgen für das Unternehmen nach sich ziehen könnte.

Die Inanspruchnahme qualifizierter Beratung wird durch verschiedene Stellen mit Zuschüssen zu Beraterhonoraren und je nach Förderprogramm auch zu Anschaffungen gefördert. Die Zuschüsse können je nach Programm und Größe des Betriebes bis zu 80 Prozent der angefallenen Kosten decken.

Fazit:

- Fehlen Informationen, um einen Handlungsbedarf beurteilen zu können, bietet das Mittelstand 4.0-Kompetenzzentrum Planen und Bauen die Möglichkeit, die für eine Bewertung erforderlichen Informationen zu erhalten oder zu beschaffen.
- Ist Handlungsbedarf identifiziert, sollten die daraus abzuleitenden Maßnahmen priorisiert werden. Dabei muss berücksichtigt werden, dass die Umsetzung von Maßnahmen im Unternehmen Zeit erfordert. Es gilt, Überforderungen des Unternehmens und der Mitarbeiter zu vermeiden.
- Das Hinzuziehen von externen Beratern ist in vielen Fällen förderfähig. Es sollte daher eine Prüfung von Fördermöglichkeiten erfolgen.

IT-Compliance ist keine Zauberei, erfordert aber ein überlegtes Vorgehen bei der Schaffung einer Unternehmensorganisation, die der Einhaltung der rechtlichen Rahmenbedingungen förderlich ist.

Weiterführende Informationen

Bei der Auswahl der in diesem für Referenten und Interessierte konzipierten Leitfaden angeführten gerichtlichen Entscheidungen wurde Wert darauf gelegt, dass diese nicht nur für Fachleute, sondern für jedermann frei im Internet abrufbar zur Verfügung stehen. Sollte eine hier angegebene Quelle gleichwohl nicht mehr erreichbar sein, so lässt sich eine gerichtliche Entscheidung mittels der Angabe von Spruchkörper, Art und Tag der Entscheidung sowie Geschäftszeichen mittels einer Suchmaschine leicht auffinden. Eine weitere Hilfe beim Auffinden gerichtlicher Entscheidungen ist der European Case Law Identifier, kurz: ECLI. Dabei handelt es sich um eine eindeutige, für jede Entscheidung separat und nur einmal vergebene Kombination aus Buchstaben und Ziffern, aus denen Land, Gericht und Jahr ersichtlich sind.

Übersicht der gerichtlichen Entscheidungen:

- OLG Naumburg, Urt. v. 15.07.2002, 1 U 153/99: Der Kaufmann hat seinen Betrieb so einzurichten und zu führen, dass es nicht zu Rechtsverletzungen kommt, wobei er diesbezüglich einem strengeren Sorgfaltsmaßstab unterliegt, als er im Übrigen anzulegen sein würde.
  Entscheidung abrufbar unter: https://judicialis.de/Oberlandesgericht-Naumburg_1-U-153-99_Urteil_15.07.2002.html

- BVerfG, Urt. v. 27.02.2008, 1 BvR 595/01: Der Nutzer hat als besondere Ausprägung seines allgemeinen Persönlichkeitsrechts einen Anspruch darauf, dass die Vertraulichkeit und Integrität der von ihm eingesetzten technischen Systeme gewährleistet ist.
  Entscheidung abrufbar unter: http://www.bundesverfassungsgericht.de/SharedDocs/Entscheidungen/DE/2008/02/rs20080227_1bvr037007.html

- VGH Kassel, Urt. v. 19.05.2009, 6 A 2672/08 Z: Arbeitnehmer haben einen Anspruch darauf, dass die Vertraulichkeit und Integrität von ihnen auch privat genutzter Systeme nicht dadurch verletzt wird, dass Kontrollen der dienstlichen E-Mail-Postfächer ohne ihre ausdrückliche Zustimmung erfolgen.
  Entscheidung abrufbar unter: https://openjur.de/u/713314.html

- BGH, Urt. v. 12.05.2010, I ZR 121/08: Der Betreiber eines WLAN-Routers ist verpflichtet, die zum Zeitpunkt des Geräteerwerbs üblichen Sicherungsmaßnahmen zur Verhinderung einer unbefugten Nutzung seines Internetanschlusses zu ergreifen.
  Entscheidung abrufbar unter: http://www.jurpc.de/jurpc/show?id=20100114

- BFH, Urt. v. 16.01.2014, V R 28/13: Elektronisch eingegangene Geschäftsbriefe wie z.B. E-Mails und elektronische Rechnungen müssen so archiviert werden, dass nachträgliche Veränderungen ausgeschlossen sind.
  Entscheidung abrufbar unter: https://openjur.de/u/708672.html

- OLG Düsseldorf, Urt. v. 16.06.2015, I-20 U 203/14: Das Leistungsschutzrecht des Fotografen ordnet diesem die Befugnis zu, die Vervielfältigung und öffentliche Zugänglichmachung der von ihm hergestellten Fotografie zu erlauben sowie Bedingungen für die Ausübung dieses Rechts zur Vervielfältigung und öffentlichen Zugänglichmachung zu bestimmen.
  Entscheidung abrufbar unter: https://www.justiz.nrw.de/nrwe/olgs/duesseldorf/j2015/I_20_U_203_14_Urteil_20150616.html

- LG Berlin, Urt. v. 04.02.2016, 52 O 394/15: Fehler in der Datenschutzerklärung betreffend das Angebot von Telemedien eines Unternehmens begründen mangels Spürbarkeit der Beeinträchtigung des Wettbewerbs in der Regel keinen Unterlassungsanspruch eines Mitbewerbers und berechtigen folglich auch nicht zur Geltendmachung von mit einer Abmahnung verbundenen Kosten der Beauftragung eines Rechtsanwalts.
  Entscheidung abrufbar unter: https://www.iww.de/quellenmaterial/id/186288

- OVG Nordrhein-Westfalen, Urt. v. 12.09.2016, 14 A 1501/15: Der ordentliche Kaufmann stellt sich vorausschauend auf Kostensteigerungen ein und gewährleistet, dass ein aufgrund rechtlicher Vorgaben erforderlicher Austausch von ihm eingesetzter Geräte zeitgerecht durchgeführt werden kann.
  Entscheidung abrufbar unter: https://www.justiz.nrw.de/nrwe/ovgs/ovg_nrw/j2016/14_A_1501_15_Urteil_20160912.html

- OLG Düsseldorf, Beschl. v. 19.01.2017, I-20 U 40/16: Mit der Vorlage von Rechtsfragen an den EuGH möchte das Oberlandesgericht Klarheit über die Auslegung von Normen des Unionsrechts erlangen, um beurteilen zu können, ob die Einbindung sog. Social-Plugins auf Internetseiten in dem ihm zur Beurteilung vorgelegten Sachverhalt zulässig ist.
  Entscheidung abrufbar unter: https://www.justiz.nrw.de/nrwe/olgs/duesseldorf/j2017/I_20_U_40_16_Beschluss_20170119.html

- EuGH, Urt. v. 19.10.2016, C-582/14: Die einem einer Privatperson zugewiesene Internet-Protokolladresse (IP-Adresse) stellt für den Anbieter von über das Internet abrufbaren Telemedien, dem diese Adresse technisch notwendigerweise bekannt wird, ein personenbezogenes Datum dar.
  Entscheidung abrufbar unter: https://medien-internet-und-recht.de/volltext.php?mir_dok_id=2791

- FG Münster, Urt. v. 29.03.2017, 7 K 3675/13: Die Buchführung ist formal fehlerhaft, wenn Unterlagen über die Einrichtung und Programmierung des elektronischen Kassensystems im Rahmen der Prüfung nicht oder nur unvollständig vorgelegt werden können.
  Entscheidung abrufbar unter: https://www.justiz.nrw.de/nrwe/fgs/muenster/j2017/7_K_3675_13_E_G_U_Urteil_20170329.html

- EGMR, Urt. v. 05.09.2017, 61496/08: Der Schutz der privaten Kommunikation wird auch innerhalb eines bestehenden Arbeits- oder Dienstverhältnisses gewährleistet.
  Entscheidung abrufbar unter: http://hudoc.echr.coe.int/fre?i=001-177083

- BGH, Urt. v. 16.05.2017, VI ZR 135/13: Die dem Internetanschluss einer Privatperson zugewiesene IP-Adresse stellt für den Diensteanbieter, dem diese Adresse technisch notwendigerweise bekannt wird, ein personenbezogenes Datum dar (Anschluss an EuGH, Urt. v. 19.10.2016, C-582/14).
  Entscheidung abrufbar unter: http://www.jurpc.de/jurpc/show?id=20170115

Auch wenn hier einige ältere Entscheidungen angeführt werden, haben diese für die Beantwortung rechtlicher Fragen im Zeitpunkt der Manuskriptlegung noch nichts an Aktualität verloren. Da das Recht aber eine lebendige Materie ist, können künftige Entwicklungen dazu führen, dass die hier aufgeführten Entscheidungen durch neuere Judikate überholt werden. Die Entscheidungsauswahl ist an dieser Stelle keinesfalls abschließend zu verstehen, d.h. es lassen sich sicherlich leicht weitere gerichtliche Entscheidungen auffinden, die bei der Beantwortung von Fragen der IT-Compliance helfen können. Es ist jedoch insoweit empfehlenswert, rechtliche Fragen mit einem rechtskundigen Berater zu erörtern, um Fehlinterpretationen zu vermeiden und eine Einordnung einer gerichtlichen Antwort in den Kontext sicherzustellen.

Übersicht über weiterführende Arbeitshilfen:

Die hier aufgeführten Arbeitshilfen setzen in unterschiedlicher Ausprägung besondere technische und rechtliche Kompetenzen beim Verwender voraus. Da erfahrungsgemäß das Vorhandensein aller benötigten Kompetenzen bei Workshop-Teilnehmern mit ihren in der Regel recht unterschiedlichen Ausbildungs- und Berufshintergründen nicht vorausgesetzt werden kann, wurde darauf verzichtet, diese Arbeitshilfen in den Folienvortrag explizit aufzunehmen. Für besonders qualifizierte Teilnehmer oder aber im Rahmen einer begleitenden Information können die Arbeitshilfen Orientierung bieten.

- Mittelstand 4.0-Komptenzzentrum Chemnitz: Prof. Dr. Dagmar Gesmann-Nuissl und Dipl. Jur. Univ. Gernot Kirchner geben in der Broschüre „Angst vor der EU-Datenschutz-Grundverordnung? – Nicht mit uns!“ auf etwas mehr als 30 Seiten (DIN-A-5) einen Überblick über die Eckpunkte des neuen Datenschutzrechts, das seit dem 25.05.2018 anzuwenden ist. Vorgestellt werden neben dem persönlichen und räumlichen Anwendungsbereich auch die wesentlichen an Datenverarbeiter gerichteten Anforderungen zur Gewährleistung des Schutzes persönlicher Informationen.
  Herunterzuladen unter: https://betrieb-machen.de/dsgvo-handlungsleitfaden/

- Mittelstand 4.0-Kompetenzzentrum Saarbrücken (Rechtsanwaltskanzlei DURY/Websitecheck GmbH, Saarbrücken): Angeboten wird ein Leitfaden „Rechtssichere Internetseiten & Online-Shops – DS-GVO-konform“ im Umfang von rund 40 Seiten DIN-A-4 mit einzelnen Checklisten. Das fachlich-juristische ausgerichtete Skript soll einen konzentrierten Überblick vermitteln.
  Herunterzuladen unter: http://www.mittelstand-digital.de/DE/Wissenspool/ITSicherheitRecht/publikationen,did=639216.html

- Zentralverband des deutschen Handwerks (ZDH): Neben einem Leitfaden zu den neuen Pflichten für Betriebe nach Anwendbarwerden der Regelungen der DS-GVO werden auch Einzelfragen, wie z.B. die Voraussetzungen der Zulässigkeit einer Verarbeitung personenbezogener Daten oder die Dokumentationspflichten erläutert. Zusätzlich werden Muster für Formulare wie eine standardisierte Einwilligungserklärung in die Datenverarbeitung im Zusammenhang mit der Versendung eines Newsletters oder das Verzeichnis der Verarbeitungstätigkeiten.
  Abrufbar ist das Angebot unter: https://www.zdh.de/fachbereiche/organisation-und-recht/datenschutz/datenschutz-fuer-handwerksbetriebe/

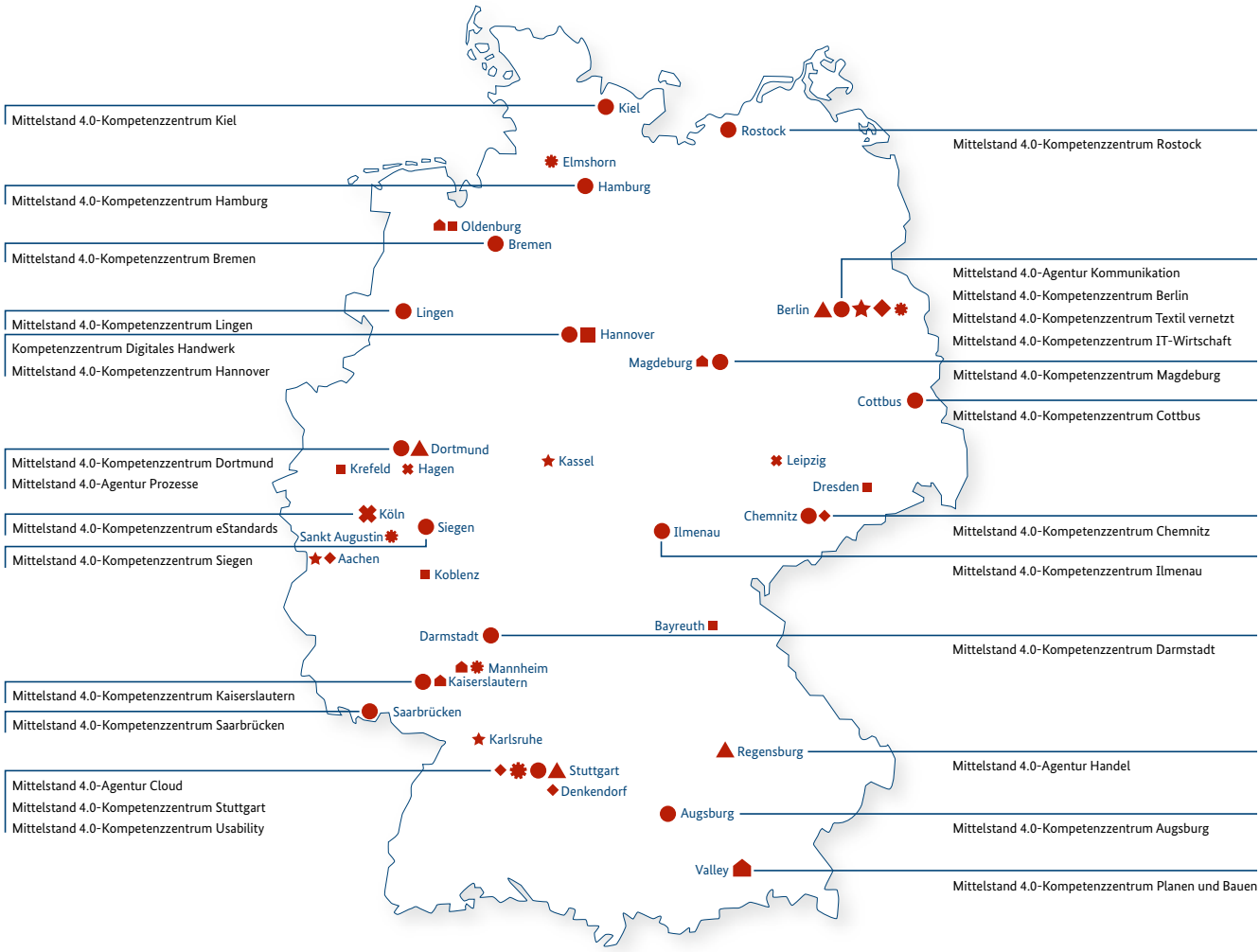
- IHK Rhein-Neckar: Als Checkliste bezeichnet liefert die IHK einen kompakten Überblick nicht nur über speziell die Betreiber von Online-Shops, sondern auch die jeden Anbieter einer Website treffenden Pflichten wie insbesondere die Anbringung einer Anbieterkennzeichnung und einer Datenschutzerklärung sowie die aus dem Urheber- und Leistungsschutzrecht fließenden Konsequenzen für die Verwendung von Inhalten Dritter wie etwa von Texten, Fotos, Musik oder Videos.
  Abrufbar ist das Angebot unter: https://www.rhein-neckar.ihk24.de/recht/wirtschaftsrecht/Internet/checkliste-rechtssicherer-online-shop/3639702

- IHK Schleswig-Holstein: In ihrer Broschüre „Aufbau eines rechtssicheren Online-Shops informiert die IHK nicht nur über die Anforderungen an Shop-Betreiber, sondern bietet einen ersten Einblick in rechtliche Rahmenbedingungen der Online-Werbung. Es werden Suchmaschinen wie z.B. Google ebenso angesprochen wie die Werbung mit Gütesiegeln. Auch urheber- und leistungsschutzrechtliche Aspekte der Nutzung von Inhalten wie z.B. Texten, Fotos, Musik oder Videos werden besprochen.
  Abrufbar ist die Broschüre unter: https://www.ihk-schleswig-holstein.de/blob/swhihk24/servicemarken/serviceleistungen/broschueren/1373948/7235c012267d902ad67dd243d271fdac/Broschuere_Aufbau_eines_rechtssicheren_Onlineshops-data.pdf

- Bundesministerium für Wirtschaft (BMWi): In seinem Internetangebot „IT-Sicherheit in der Wirtschaft“ bietet das BMWi ein umfassendes Informationsangebot zu allen Aspekten der IT-Sicherheit mit einem besonderen Fokus auf KMU. Neben Informationsbroschüren werden Checklisten angeboten.
  Abrufbar ist das Angebot unter: http://www.it-sicherheit-in-der-wirtschaft.de/IT-Sicherheit/Navigation/root.html

- Bayerisches Landesamt für Datenschutzaufsicht (BayLDA): Wie ein Verzeichnis der Verarbeitungstätigkeiten gem. Art. 30 DS-GVO nach Auffassung einer Datenschutz-Aufsichtsbehörde konkret aussehen könnte, hat das Landesamt auf seiner Website veröffentlicht. Es wird eine recht typische Fallkonstellation zugrunde gelegt. Die weiterführenden Hinweise in den Kurzpapieren ermöglichen zu erkennen, in welcher Weise Anpassungen auf das eigene Unternehmen vorgenommen werden müssen. Abrufbar ist das Angebot unter: https://www.lda.bayern.de/de/kleine-unternehmen.html

Mittelstand 4.0
Kompetenzzentrum Planen und Bauen



- Kompetenzzentren der Förderinitiative „Mittelstand 4.0 – Digitale Produktions- und Arbeitsprozesse“
- Agenturen der Förderinitiative „Mittelstand 4.0 – Digitale Produktions- und Arbeitsprozesse“
- Kompetenzzentrum Digitales Handwerk
- Regionale Schaufenster Digitales Handwerk
- Kompetenzzentrum Usability
- Regionale Anlaufstellen Usability
- Kompetenzzentrum IT-Wirtschaft
- Regionale Stützpunkte IT-Wirtschaft
- Kompetenzzentrum Textil vernetzt
- Regionale Schaufenster Textil vernetzt
- Kompetenzzentrum eStandards
- Offene Werkstätten eStandards
- Kompetenzzentrum Planen und Bauen
- Regionale Anlaufstellen Planen und Bauen

Über Mittelstand Digital

Mittelstand-Digital informiert kleine und mittlere Unternehmen über die Chancen und Herausforderungen der Digitalsierung. Kompetenzzentren helfen vor Ort dem kleinen Einzelhändler genauso wie dem größeren Produktionsbetrieb mit Expertenwissen, Demonstrationszentren, Netzwerken zum Erfahrungsaustausch und praktischen Beispielen. Das Bundesministerium für Wirtschaft und Energie ermöglicht die kostenfreie Nutzung aller Angebote von Mittelstand-Digital.

Weitere Informationen finden Sie unter www.mittelstand-digital.de

Mittelstand-Digital

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages