Praxistipps IT

Datenschutz in Zeiten digitaler Transformation

Zukunftssicher in der Kanzlei 4.0

Inklusive Downloads

Rouven Friederich / Andreas Schneider

IDW VERLAG GMBH

Ihr Zugang zum Download-Bereich von „Datenschutz in Zeiten digitaler Transformation“

Folgende Schritte sind zur Freischaltung erforderlich:

1. Melden Sie sich mit Ihren Zugangsdaten im IDW Internetportal an. Falls Sie noch keine Zugangsdaten besitzen, führen Sie bitte zunächst eine Erstregistrierung durch.
2. Unter **www.idw.de/idw-verlag > Produkt Updates >Datenschutz in Zeiten digitaler Transformation** geben Sie bitte anschließend den unten abgedruckten Freischaltcode in die dafür vorgesehene Box ein.

Nun stehen Ihnen nach jedem Einloggen die Dateien zum Download zur Verfügung.

Freischalt-Code:

IDW VERLAG GMBH

Praxistipps IT

Datenschutz in Zeiten digitaler Transformation

Zukunftssicher in der Kanzlei 4.0

Rouven Friederich / Andreas Schneider

IDW VERLAG GMBH

Die IDW Verlag GmbH ist ein Unternehmen des Instituts der Wirtschaftsprüfer in Deutschland e. V. (IDW).

Satz: Reemers Publishing Services GmbH, Krefeld
Druck und Bindung: C.H.Beck, Nördlingen
KN 11884/0/0

ISBN 978-3-8021-2467-9

Bibliografische Information der Deutschen Bibliothek
Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://www.d-nb.de abrufbar.

Coverfoto: www.istock.com/ByoungJoo

www.idw-verlag.de

Inhaltsverzeichnis

1 Einleitung

Die Hauptaufgabe von Steuerberater- und Wirtschafsprüferkanzleien besteht darin, Beratungen durchzuführen, Abschlüsse zu erstellen und Mandanten in fachspezifischen Problemstellungen zu unterstützen. Die gesamte Arbeit beruht bei diesen Tätigkeiten maßgeblich auf personenbezogenen Daten. Das oberste Gebot der DSGVO ist es, personenbezogene Daten bestmöglich zu schützen und die Verarbeitung für die Betroffenen so transparent wie möglich zu gestalten. Ein Jahr nach der Einführung der DSGVO stellt sich jetzt die Frage, ob die Integration der DSGVO in den Kanzleialltag gelungen ist, und welche Umstellungen damit verbunden sind.

Das Ziel der DSGVO ist, einen weitreichenden Schutz der personenbezogenen Daten für natürliche Personen zu gewährleisten. Der mediale Wirbel zur Einführung der DSGVO war enorm und der Bedarf an schnellen Lösungen zur Umsetzung groß. Mehr als ein Jahr später ist es ruhiger geworden. Die anfängliche Angst ist verflogen und bei vielen Kanzleien ist wieder der Alltag eingekehrt wie im April 2018.

Dennoch spielt ein umfassender Datenschutz in der Zeit der Digitalisierung noch immer eine entscheidende Rolle – mehr als je zuvor. In einer Zeit, in der sukzessiv alle Geräte miteinander verbunden werden, weltweit agierende Konzerne wie Facebook, Google oder Microsoft mächtiger als manche Regierungen werden und die Kommunikation unter den Menschen zum größten Teil nur noch digital abgebildet wird, ist ein funktionierender Datenschutz wichtiger als je zuvor. Die Verbreitung der Daten, die einmal ins Internet gelangt sind, ist kaum mehr aufzuhalten, weil Dutzende von Kopien bereits in den Tiefen des WWW schlummern.

Die Digitalisierung findet aber nicht nur im privaten Gebrauch, sondern ebenfalls im geschäftlichen Umfeld statt. Maßgeblich davon betroffen sind auch Steuerberater- und Wirtschaftsprüferkanzleien. Während die Arbeit vor wenigen Jahren noch sehr papierlastig war, gehören Laptop und Smartphone heutzutage zum klassischen Berufswerkzeug des Steuerberaters/Wirtschaftsprüfers.

Der händische Abgleich von Abstimmsummen gehört der Vergangenheit an und die Überprüfung der Summen/Salden-Listen mit dem spitzen Bleistift wurde von mächtigen Tabellenprogrammen wie Excel oder IDEA abgelöst. Große Datensätze mit Millionen von Buchungssätzen können binnen weniger Sekunden verarbeitet und teilweise mit künstlicher Intelligenz automatisch ausgewertet werden. Prüfungshandlungen können in branchenspezifischen Programmen mit wenigen Mausklicks definiert und im Anschluss automatisch anschaulich aufbereitet werden.

Optimierungspotenziale bei der Steuer können durch automatische Mustererkennung entdeckt werden. Die Berichterstattung gegenüber dem Mandanten erfolgt selbstverständlich in digitaler Form und selbst das letzte Überbleibsel aus der vergangenen Zeit, die Unterschrift unter den Dokumenten, ist meist nur ein eingescanntes Duplikat oder eine elektronische Signatur.

Während früher noch Dutzende Meetings auf der Tagesordnung standen, wird der größte Teil des Kundenkontakts heute über E-Mail-Verkehr oder Webmeetings abgebildet. Die Erinnerung an Geburtstage wird von dem in Outlook eingepflegten Geburtstagskalender übernommen und die klassische Notiz beim Mandanten wird direkt beim Mandanten auf dem Tablet mitgeschrieben und anschließend in die Cloud oder direkt in die digitale Mandantenakte auf den kanzleiinternen File-Server geladen.

Die obigen Beispiele, die vor wenigen Jahren noch als Science-Fiction abgestempelt worden wären, gehören heute in weiten Teilen zum ganz normalen Alltag eines Steuerberaters oder Wirtschaftsprüfers. Die Verarbeitung, Kommunikation, Kalkulation und Beratung sind durch den digitalen Wandel deutlich komfortabler, effizienter und digitaler geworden.

Der digitale Wandel bringt jedoch nicht nur Vorteile mit sich. Der höhere Komfort, die größere Effizienz, die bahnbrechende Geschwindigkeit – all das ist nur möglich geworden durch eine deutlich weiterentwickelte Infrastruktur und eine applikationsübergreifende Vernetzung der Benutzerkonten und Daten. Deren Grundlage bilden neben kalkulatorischen oder systemseitigen Daten zu weiten Teilen personenbezogene Daten.

Aus diesen personenbezogenen Daten lassen sich, mit wenig Aufwand, detaillierte Profile erstellen, die später für Marketingaktivitäten gewinnbringend weiterverkauft werden können. Diese Vorgehensweise ist jedoch mit der in den jeweiligen Berufssatzungen verankerten beruflichen Verschwiegenheit in der Kanzlei nicht vereinbar. Dennoch kann bzw. möchte man in der Kanzlei nicht auf den Komfort und die Effizienz der Digitalisierung verzichten.

Die einzige Möglichkeit, dieses Problem zu bewältigen, ist eine strikte Trennung der Daten und ein umfassender, prozessübergreifender Datenschutz. Hierfür bietet die DSGVO eine gute Richtlinie für die Kanzlei, wie einerseits von der Digitalisierung profitiert werden kann und andererseits der Schutz der Daten nicht vernachlässigt wird.

Mitunter kann es für Kanzleien schwierig sein, eine Brücke zwischen Digitalisierung und DSGVO zu schlagen. Eine abteilungsübergreifende Umsetzung, die alle Mitarbeiter und Prozesse mit einbezieht, bietet der Kanzlei viele Vorteile. Während einerseits kostspielige Strafen durch Nichteinhaltung der DSGVO ausgeschlossen werden können, kann gleichzeitig der Komfort neuer Dienste bedenkenlos genutzt werden, da bestehende Bedenken von vornherein ausgeräumt werden können. Durch die genaue Beleuchtung der Prozesse können zusätzlich Optimierungspotenziale entdeckt und somit ein weiterer Nutzen generiert werden.

Von vornherein ist allerdings zu beachten, dass die Umsetzung der DSGVO ein langfristiger Prozess ist, der über längere Zeit gedeihen muss. Hilfestellung bei der Umsetzung kann beispielsweise ein externer Datenschutzbeauftragter leisten. Dennoch sollte klar sein, dass eine Umsetzung nicht innerhalb eines Tages geschehen und der Datenschutzbeauftragte nicht ohne die Unterstützung der Kanzlei arbeiten kann.

Dieses Buch kann in allen Abteilungen der Kanzlei unterstützend wirken. Hilfreiche Praxistipps und Beispiele veranschaulichen, welche Prozesse in der Kanzlei von der DSGVO maßgeblich betroffen sind, wie sie umgestaltet werden und welche Vorteile sich daraus ergeben können. Ein Vorteil, der mit der kanzleiweiten Einführung der DSGVO einhergeht, ist die spürbare Erhöhung der IT-Sicherheit.

Mehrere Kapitel dieses Buches beschäftigen sich mit sicherheitskritischen Themen wie E-Mail-Verschlüsselung oder auch Rechtetrennung,

denen im Kanzleialltag oftmals nicht ausreichend Beachtung geschenkt wird. An dieser Stelle dient die Einführung der DSGVO oftmals als Startschuss für die Umsetzung mehrerer Sicherheitsmaßnahmen, die mit wenig Aufwand die Kanzlei zukunftssicherer machen und zusätzlich den Schaden eines Hacker-Angriffs reduzieren.

Ergänzend bietet Ihnen dieses Buch hilfreiche Tipps, wie sie in kleinen Schritten die DSGVO sukzessiv in Ihren Kanzlei-Alltag integrieren können. Zusätzlich bietet das Buch einen umfangreichen Anhang, der viele Vorlagen enthält, die mit wenigen Anpassungen direkt in das Datenschutzkonzept der Kanzlei übernommen werden können.

2 Ein Jahr DSGVO/BDSG neu – ein Rückblick

Am 25. Mai 2018 trat die neue Datenschutz-Grundverordnung in Kraft. Bereits Monate vor dem Inkrafttreten verbreitete sich Unruhe und Ungewissheit in den Vorstandsetagen großer Unternehmen. Spürbar war diese Unsicherheit aber auch bei kleinen und mittelständischen Unternehmen, bei denen das Thema Datenschutz bis zu diesem Zeitpunkt eher einen geringeren Stellenwert hatte. Strafen für Nichteinhaltung von bis zu 4% des gesamten, weltweit erzielten Jahresumsatzes standen für Vergehen und Nichteinhaltung der Datenschutz-Grundverordnung im Raum.

Angebote verschiedenster Datenschutzberater versprachen sofortige Unterstützung für zum Teil horrende Preise. Jetzt, ein Jahr nach der Einführung der DSGVO, wurde der neuen Grundverordnung der Wind aus den Segeln genommen. Die Höchststrafe, die bisher in der europäischen Union verhängt wurde, beläuft sich auf 50 Millionen Euro und wurde von der französischen Behörde CNIL verhängt.[1]

50 Millionen Euro klingen für die Vorstände und Geschäftsführer eines mittelständischen Unternehmens äußerst schmerzlich, wenn nicht sogar existenzbedrohend. Fügt man der Aussage jedoch hinzu, dass der Schuldige der Suchmaschinengigant Google Frankreich war, relativiert sich dieser Betrag allerdings wieder.

In Deutschland betrug die bisher höchste verhängte Strafe 80.000 Euro. Diese Einzelstrafe wurde von der Landesdatenschutzbeauftragten von Baden-Württemberg verhängt, da aufgrund unzureichender interner Kontrollmechanismen eines Unternehmens Gesundheitsdaten ins Internet gelangt waren.[2]

Rückblickend gesehen zeichnet sich also ein anderes Bild als zum Start der DSGVO ab. Von den Behörden wurden zwar konsequent Strafen

[1] Quelle: https://www.handelsblatt.com/politik/deutschland/datenschutzregeln-nach-rekordstrafe-gegen-google-dsgvo-entfaltet-langsam-ihr-potenzial/23894666.html?ticket=ST-2693939-cbP5ZpiHvqTqXSZEC54e-ap6, abger. am 02.07.2019

[2] Quelle: https://www.handelsblatt.com/politik/deutschland/datenschutzgrundverordnung-behoerden-verhaengen-erste-bussgelder-wegen-verstoessen-gegen-dsgvo/23872806.html?ticket=ST-44545780-sezw0Vi6HlgxulErHkDh-ap2, abger. am 21.10.2019

verhängt, dennoch betrifft dies nur eine geringe Zahl von Unternehmen und die Strafen füllen bei Weitem noch nicht den maximalen Spielraum, der dafür vorgesehen war. Aber was bedeutet dies speziell für kleinere Unternehmen wie beispielsweise Steuer- und Wirtschaftsberaterkanzleien? Können Kanzleien durch ihre geringe Größe de facto „unter dem Radar fliegen"?

Eine konkrete Antwort darauf zu geben, ist nicht einfach. Natürlich kann es sein, dass die Kanzlei ohne jegliche Umsetzung des Datenschutzes nicht auffällt und möglicherweise auch nicht kontrolliert wird. Dennoch besteht das Risiko stets und die Folgen eines Datenschutzskandals können äußerst unangenehm für die Kanzlei sein.

Da Kanzleien mit höchst sensiblen Daten des Mandanten arbeiten, wäre ein Verlust der Daten oder eine nicht geplante Veröffentlichung der Daten möglicherweise der Untergang der Kanzlei. Abgesehen von den Strafen, die von den Behörden verhängt werden können, ist das Risiko des Reputationsverlusts mindestens gleichwertig aufzuwiegen. Die Kanzlei würde in diesem Fall das Vertrauen der Mandanten aufs Spiel setzen und somit ihr höchstes Gut verschenken.

2.1 Sinn und Zweck der DSGVO

Der Sinn und Zweck der neuen DSGVO ist nach einem Jahr nach wie vor derselbe wie zur Einführung – der umfangreiche Schutz der Daten von natürlichen Personen und die angemessene Bestrafung derjenigen, die nicht um den Schutz der Daten bemüht sind.

Grundsätzlich sollte der Schutz der Daten oberstes Gebot in jedem Unternehmen sein, welches personenbezogene Daten verarbeitet. Ein Blick in die Medien reicht oft, um zu sehen, dass dieses Gebot scheinbar selbst bei größeren Konzernen wie Facebook oder Google, deren Kerngeschäft aus der Auswertung personenbezogener Daten besteht, noch nicht an oberster Stelle steht, was die Datenskandale der letzten Jahre bestätigt haben.

Im letzten Jahrzehnt war es schlicht und ergreifend noch nicht möglich, so viele personenbezogene Daten zu sammeln, wie es zur heutigen Zeit möglich ist. Heutzutage ist es nur noch schwer möglich, alltägliche Aufgaben zu erledigen, ohne dabei getrackt und analysiert zu werden.

Bonuskarten, Cookies und Smartphones sind die Werkzeuge der großen Konzerne, um Unmengen an personenbezogenen Daten zu sammeln. Diesen neuen Formen des Datensammelns war das alte Bundesdatenschutzgesetz nicht mehr gerecht geworden. Um auch zukünftig einen umfassenden Schutz für die Bürgerinnen und Bürger der europäischen Gemeinschaft zu gewährleisten, wurde im Jahr 2016 beschlossen, ein europaweites Datenschutzgesetz zu entwickeln, welches auf die Gefahrenlage der heutigen Zeit zugeschnitten ist. Um diesen Schutz zu gewährleisten, bedarf es strikter Vorschriften und Vorkehrungen, die in der Datenschutz-Grundverordnung exakt beschrieben sind.

2.2 Notwendige formale Regelungen vs. Bürokratiemonster

Wie die meisten Gesetze und Regelungen, die durch den deutschen Staat oder die EU auf den Weg gebracht werden, ist auch die Datenschutz-Grundverordnung eine umfassende Sammlung von Paragrafen, die für Otto Normalverbraucher nicht unbedingt klar verständlich sind.

Um möglichst alle Fälle, die aus datenschutzrechtlicher Sicht kritisch sein könnten, abzudecken, ist die DSGVO sehr allgemein gehalten. Formale Paragrafen beschreiben grundsätzliche Ansprüche an den Datenschutz, wie er in jedem Unternehmen gelebt werden sollte. Notwendige Dokumentationen und Formalitäten, die jedes Unternehmen erfüllen muss, können in unzähligen Paragrafen abgelesen werden.

An dieser Stelle stellt sich die erste Kernfrage: Muss umfangreicher Datenschutz so detailliert dokumentiert werden? Oder besser: Ist eine umfangreiche Dokumentation gleichzusetzten mit einem gut funktionierenden Datenschutzkonzept? Eine klare Antwort auf diese Frage gibt es schlichtweg nicht. Juristen behaupten, ein funktionierender Datenschutz basiere auf zahlreichen Dokumenten, um im Fall eines Datenschutzvorfalls sauber dokumentierte Nachweise zu haben, dass alle Regularien eingehalten wurden. Andere Stimmen sagen, Datenschutz müsse von den Mitarbeitern gelebt werden, da sonst die beste Dokumentation auch nicht ausreichend sei.

Was an diesen Aussagen zutrifft und was nicht, muss jeder für sich selbst entscheiden. Einen guten Anfang bildet zumindest eine gesunde Mischung aus Umsetzung und Dokumentation.

Einerseits ist die Dokumentation ein elementarer Bestandteil eines Datenschutzkonzepts. Andererseits bedeutet eine saubere Dokumentation nicht zwingend den optimalen Schutz für persönliche Daten. Der Dokumentationsaufwand eines umfassenden Datenschutzkonzepts inklusive aller Verzeichnisse der Verarbeitungstätigkeit, eines Datenschutzhandbuches, Löschkonzept und Virenschutzkonzept ist, speziell für kleinere Unternehmen, Handwerksbetriebe oder Kanzleien, enorm hoch.

Eine kurzfristige Erstellung ist ohne vorherige Fachkenntnis kaum machbar. Um diesen Aufwand zu vermeiden bzw. einzudämmen, bedarf es meist professioneller Hilfe.

Unzählige Online-Anbieter versprechen die schnelle, unkomplizierte Umsetzung der DSGVO im Unternehmen. Oftmals wird dies aber dann nicht gründlich genug durchgeführt oder die komplette Umsetzung basiert auf Universaltemplates, die für jedes Unternehmen gleich aussehen, aber nicht den Ansprüchen einer Kanzlei gerecht werden.

Dieser Weg ist zwar meist verhältnismäßig günstig, im Vergleich zu den Kosten, die bei einer Umsetzung in Eigenregie entstehen können, jedoch nur teilweise sinnvoll. Grundsätzlich ist diese Lösung zwar nicht verwerflich, ein langfristiger Mehrwert für das Unternehmen entsteht dadurch allerdings nicht.

Auch wenn durch die Dokumentation, selbst in gemeinschaftlicher Umsetzung mit Experten, ein gewisser Zeitaufwand notwendig ist, hilft es dem Unternehmen und seinen Mitarbeitern auch oft schon, über viele Jahre praktizierte Prozesse neu zu beleuchten und gegebenenfalls Verbesserungspotenziale aufzudecken. Die DSGVO empfiehlt den Unternehmen das Prinzip der Datenminimierung.

Oft finden sich in unterschiedlichen Prozessen nicht benötigte Daten, die standardmäßig mit erhoben werden, obwohl sie rein faktisch gar nicht benötigt werden. Durch eine strukturierte Beleuchtung mit anschließender Dokumentation dieser Prozesse können Potenziale entfaltet werden, die sonst möglicherweise unentdeckt bleiben würden.

Schlussendlich, um nochmals auf die Frage zu Beginn zurückzukommen, zeigt sich, dass die DSGVO mit Recht als Bürokratiemonster bezeichnet wird. Dennoch kann bei sauberer Umsetzung auch ein

Mehrwert für die Kanzlei entstehen. Ein weiterer Benefit ist die Wahrung des Vertrauens gegenüber dem Mandanten, der so seine Daten mit gutem Gewissen in sichere Hände legen kann.

Der Aufwand zu Beginn ist nicht zu unterschätzen – der Mehrwert, der daraus generiert werden kann, jedoch auch nicht.

2.3 Häufige Problemfälle und Irrtümer im Umgang mit der DSGVO

Wie bei jeder großen Gesetzesänderung bestand auch bei der Einführung der DSGVO in einzelnen Regelungsbereichen ein hoher Interpretationsspielraum. Aufgrund einer fehlenden Praxiserfahrung im Umgang mit bestimmten Vorschriften war bei Unternehmen wie Kanzleien häufig Unsicherheit in Bezug auf die Anwendung der Vorschriften vorhanden.

Wer vorher schon das Bundesdatenschutzgesetz erfüllt hat, erfüllt jetzt auch die DSGVO

Es wäre naheliegend, dass Unternehmen, die bereits alle Kriterien des Bundesdatenschutzgesetzes erfüllten, jetzt auch die DSGVO erfüllen. Leider stimmt das nur bedingt. Die DSGVO baut zwar auf dem Bundesdatenschutzgesetz auf, jedoch nur in Teilen. Grundsätzlich ist zu sagen, dass durch die Erfüllung des Bundesdatenschutzgesetztes schon ein Grundstein für eine erfolgreiche Umsetzung der DSGVO gelegt ist. Eine vollständige Umsetzung der DSGVO bedarf jedoch weiterer Regelungen. Während sich das Bundesdatenschutzgesetz auf 26 Seiten erstreckte, ist die DSGVO nun auf über 80 Seiten angewachsen. Die Grundzüge der beiden Gesetze sind zwar gleich, die Anforderungen der DSGVO jedoch viel höher.

Für unser Unternehmen gilt die DSGVO nicht, da es zu klein ist

Dies ist ein Irrtum. Die DSGVO betrifft alle Unternehmen und Dienstleister. Selbst ein Einmann-Betrieb muss die Regeln der DSGVO einhalten und umsetzen. Einziger Unterschied ist die Bestellung des Datenschutzbeauftragten. Während bei Neueinführung Unternehmen ab zehn Mitarbeitern einen Datenschutzbeauftragten benötigten, wurde dies nun reformiert und die Grenze auf 20 Mitarbeiter angehoben. Für Unternehmen, deren Mitarbeiterzahl darunter liegt, muss kein

Datenschutzbeauftragter bestimmt werden – die Umsetzung der DSGVO muss jedoch trotzdem erfolgen. Denn für die Umsetzung gibt es bei der DSGVO keine Ausnahmen. Jeder ist verpflichtet, sich an die Grundsätze der Datenschutz-Grundverordnung zu halten.

Unser Unternehmen ist so klein, da fällt es nicht auf, wenn wir die DSGVO nicht umsetzen

Diese Aussage ist ein Trugschluss. Da im Fokus der Medien hauptsächlich große Unternehmen wie Google stehen, erweckt es oft den Anschein, dass kleine Unternehmen nicht beachtet werden. Diese Fehlinformation birgt jedoch ein großes Risiko. Werden die Aufsichtsbehörden darüber in Kenntnis gesetzt, dass in einem Unternehmen, egal ob klein oder groß, Verstöße gegen die DSGVO vorkommen, müssen diese dem Verdacht nachgehen. Die Behörden sind gesetzlich dazu verpflichtet, jeden Verstoß zu ahnden. Im ersten Jahr nach der Einführung der DSGVO sind die ermittelten Fälle zwar noch in einem überschaubaren Rahmen geblieben, zukünftig wollen die Behörden jedoch weiter Personal aufbauen, um verstärkt gegen Unternehmen bei Nichteinhaltung vorzugehen.

Für jeden Verstoß gegen die DSGVO werden 20 Millionen Euro Strafe oder 4% des Jahresumsatzes fällig

Auch wenn tatsächlich in der DSGVO die Rede von 20 Millionen Euro bzw. 4% des Jahresumsatzes ist, ist hiermit nicht eine generelle Strafe gemeint. Diese beiden Zahlen stellen die Höchststrafen für Vergehen dar. Einfluss auf die Höhe der Strafen haben viele Kriterien, die alle gemeinsam mit in das Strafmaß einfließen, wie beispielsweise Kooperationsbereitschaft, Ausmaß des Schadens, Meldung bei der Behörde etc. Dennoch sollte die Umsetzung der DSGVO nicht auf die leichte Schulter genommen werden, da je nach Faktenlage empfindliche Strafen drohen können.

Rechnungen müssen nach drei Monaten gelöscht werden

Hierbei handelt es sich um einen Irrtum! Selbst wenn die Rechnung personenbezogene Daten enthält, die nach datenschutzrechtlicher Sicht gelöscht werden müssten, besteht für Belege mit steuer- und handelsrechtlichem Charakter die gesetzliche Aufbewahrungsfrist von 10 Jahren. Aufbewahrungsfristen wie diese bleiben von der DSGVO unberührt und stehen im Zweifelsfall immer über den Löschfristen der DSGVO.

Eine Datenübermittlung außerhalb der EU darf nicht stattfinden

Diese Behauptung ist in keiner Weise richtig. Neben der Tatsache, dass in der heutigen, vollvernetzten Welt eine Übertragung in Drittstaaten kaum auszuschließen ist, wird es ausdrücklich auch von der DSGVO erlaubt, Daten in Drittstaaten wie beispielsweise die USA oder Russland zu übertragen. Die DSGVO schreibt lediglich vor, dass die Sicherheitsstandards des Datenschutzes dabei mindestens denen der DSGVO entsprechen müssen.

Eine Datenschutzerklärung berechtigt automatisch zur Datenverarbeitung

Eine Datenschutzerklärung findet sich heute, mehr als ein Jahr nach der Einführung der DSGVO, auf den meisten Webseiten. Dennoch ist eine Datenschutzerklärung nicht gleichzusetzen mit einer Einwilligungserklärung. Während eine Einwilligungserklärung eindeutig eine Zustimmung der betroffenen Person einholt, erfüllt eine Datenschutzerklärung mehr einen informativen Charakter. Die Datenschutzerklärung gibt lediglich Aufschluss darüber, zu welchem Zweck die Daten verarbeitet werden, wer der Ansprechpartner ist und wie lang die Daten aufbewahrt werden.

Auf unserer Website werden keine personenbezogenen Daten verarbeitet

Im höchst seltenen Fall kann dies zwar sein, doch fast immer werden auf Webseiten, selbst ohne Online-Shop oder Kontaktformular, personenbezogene Daten verarbeitet. Die Möglichkeiten, personenbezogene Daten auf der Webseite zu verarbeiten, sind schier unbegrenzt. Google Analytics, der Facebook Like Button, die Einbindung von Xing-Profilen, die Nutzung von Google Maps oder auch ein eingebettetes Video auf YouTube stellen allesamt eine Verarbeitung von personenbezogenen Daten dar. Es ist äußerst schwierig, ohne diese Auswahl von Extras eine ansprechende Webseite zu gestalten. Dennoch reicht hierfür in der Regel ein Hinweis in der Datenschutzerklärung, um die Nutzer darauf aufmerksam zu machen, welche Daten mit welchem Plug-in verarbeitet werden.

3 Einfluss der DSGVO auf die Mandatsbeziehung

Wie in vielen anderen Branchen, hat die DSGVO in der Kanzlei und dementsprechend auch auf die Mandatsbeziehung einen maßgeblichen Einfluss. Noch vor der tatsächlichen Mandatsbeziehung werden bereits einige personenbezogene Daten erhoben, die im späteren Verlauf noch ergänzt werden. Beispiele hierfür sind:

- Anfrage
- Erstberatung
- Telefonkontakt
- E-Mail-Kontakt
- Angebotserstellung

Typischerweise werden an dieser Stelle Daten wie Vor- und Nachname, Anschrift und Kontaktdaten, Telefonnummern und E-Mail-Adressen, Bankverbindungen, Steuernummern, Schriftsätze, Korrespondenz- und Beratungsprotokolle aufgenommen. Während der Ablauf des Prozesses sich für den Mandanten kaum bis gar nicht geändert hat, muss der Prozess seitens der Kanzlei nun deutlich transparenter gestaltet werden.

Gleiches gilt für die weitere Mandatsbeziehung. In den folgenden Unterkapiteln wird aus diesem Grund genau darauf eingegangen, was für Kanzleien im Bereich der Mandantenbeziehung zu beachten ist.

3.1 Auftragsannahme

In einer Kanzlei oder auch im Unternehmen ist die Auftragsannahme der erste Berührungspunkt mit der Datenschutz-Grundverordnung während der gesamten Mandatsbeziehung. Daten werden ausgetauscht, Ansprechpartner festgelegt, Termine vereinbart, Adressen notiert und noch viele weitere Schritte ausgeführt. Diese Flut an Daten ist zum Großteil personenbezogen und unterliegt somit den Regularien der DSGVO.

3.1.1 Rechtmäßigkeit der Verarbeitung

Ein wichtiger Punkt, der zu Beginn festgestellt werden muss, ist die Prüfung auf Rechtmäßigkeit der Verarbeitung. Ist diese Rechtmäßigkeit nicht gegeben, darf eine Datenverarbeitung nicht stattfinden. Artikel 6

(1) a)–f) der DSGVO listet 6 Bedingungen auf, unter denen es der Kanzlei oder dem Unternehmen möglich ist, die Daten des Mandanten zu verarbeiten:

Art. 6 Abs. 1

a. *Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;*
b. *die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;*
c. *die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;*
d. *die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;*
e. *die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;*
f. *die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.*

Wird eine dieser sechs Bedingungen erfüllt, so ist die Verarbeitung laut DSGVO rechtmäßig. Zumeist kommen Absatz a) oder b) in Kanzleien zur Anwendung, da sich diese beiden Punkte auf die Einwilligung bzw. auf die Erfüllung des Vertrages berufen. Bei der Mandantenbeziehung sind dies ebenfalls die beiden führenden Rechtmäßigkeiten. Dass eine Vertragserfüllung gegeben ist, versteht sich im Falle der Mandatsbeziehung von selbst. Schwieriger ist die Frage, wie es mit persönlichen Daten aussieht. Einige Kanzleien führen sogenannte Geburtstagslisten der Ansprechpartner. Mit Glückwünschen zum Geburtstag kann man teilweise dem doch sehr formellen Umgang mit dem Mandanten eine persönliche Note mitgeben. In den letzten Jahren war dies sicherlich kein Problem, aber jetzt nach Einführung der DSGVO ist dies ja schließ-

lich eine Verarbeitung personenbezogener Daten. Grundsätzlich ist diese Liste, soweit sie nur für Geburtstage genutzt wird und keine Einwilligung der Betroffenen eingeholt wurde, nicht erlaubt. Holt man jedoch die Einwilligung ein, ist die Führung der Liste zwar rechtmäßig, jedoch der Charakter der persönlichen Note auch dahin. An solch einem Beispiel zeigt sich schnell, welche Tücken die DSGVO mit sich bringt und an welchen Stellen Probleme auftreten, die vorher nicht denkbar waren.

3.1.2 Informations- und Auskunftspflichten der Kanzlei

Im Zuge der Einführung der neuen DSGVO wurden die Informations- und Auskunftspflichten gegenüber den Betroffenen maßgeblich verschärft. Art. 15 Abs. 1 der DSGVO regelt das Auskunftsrecht des Betroffenen. Dieser kann von der Kanzlei Auskunft darüber verlangen, ob und welche Daten von ihm verarbeitet werden. Des Weiteren muss die Kanzlei dem Betroffenen folgende weitere Informationen bereitstellen:

a. über die Verarbeitungszwecke;
b. über die Kategorien personenbezogener Daten, die verarbeitet werden;
c. über die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen;
d. falls möglich über die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, über die Kriterien für die Festlegung dieser Dauer;
e. über das Bestehen eines Rechts auf Berichtigung oder Löschung der ihn betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder auf Widerspruch gegen diese Verarbeitung;
f. über das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
g. wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten;
h. über das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für bzw. auf die betroffene Person.

Die Bereitstellung der Informationen sollte unverzüglich, und spätestens binnen eines Monats erfolgen. Sollte das Konstrukt der Verarbeitung sehr komplex sein, kann eine Fristverlängerung beantragt werden. Diese Verlängerung kann maximal zwei Monate betragen und nur unter Angabe einer Begründung erfolgen. Der Betroffene hat das Recht, eine Kopie der personenbezogenen Daten, die verarbeitet werden, zu erhalten. Die erste Kopie ist für den Betroffenen grundsätzlich kostenlos. Werden mehrere Kopien angefordert, kann ein angemessenes Entgelt für die weiteren Kopien eingefordert werden.

3.2 Mandatsbearbeitung

Die Mandatsbearbeitung beinhaltet die Verarbeitung von personenbezogenen Daten. Je nach Unternehmen, der jeweiligen Unternehmensstruktur oder Rechtsform, fallen unterschiedlich viele personenbezogene Daten an. Eine Verarbeitung ohne diese Daten ist nicht möglich, denn die hierbei anfallenden personenbezogenen Daten sind für Steuerberater und Wirtschaftsprüfer unverzichtbar. Des Weiteren beinhaltet die Mandatsbearbeitung nicht nur die Verarbeitung von personenbezogenen Daten, sondern auch den sicheren Datenaustausch und die elektronische Ablage bzw. Archivierung der Mandantenakte.

3.2.1 Verarbeitung von personenbezogenen Daten

Bei der Verarbeitung von personenbezogenen Daten ist zu beachten, dass eine Kanzlei aus verschiedenen Abteilungen besteht, in denen unterschiedliche Tätigkeiten durch verschiedene Mitarbeiter vorgenommen werden.

Zwischen den jeweiligen Abteilungen sollten Vorkehrungen so getroffen werden, dass datenschutzrechtliche Aspekte im Hinblick auf die Datenminimierung eingehalten werden können. Personenbezogene Daten, die in der Abteilung für Lohn- und Gehaltsabrechnungen den dort tätigen Mitarbeitern bekannt sind, dürfen nicht automatisch allen übrigen Mitarbeitern einer Kanzlei bekannt gegeben werden.

Auch sollte es nicht möglich sein, dass sich Mitarbeiter des Sekretariats oder des Prüfungsbereichs automatisch Zugang zu personenbezogenen Daten der jeweiligen Mandanten verschaffen können.

Im IT-System der Kanzlei sollte hinterlegt sein, welche Mitarbeiter die entsprechenden Mandanten betreuen. Die Zuständigkeiten hierfür werden im System zentral durch die Mitarbeiter des Sekretariats gepflegt. Über die Pflege der Zuständigkeiten verteilt die Software die entsprechenden Berechtigungen. Der Zugriff sollte hier minimal ausgestaltet sein und nicht erlauben, dass Mitarbeiter außerhalb ihres Zuständigkeitsbereichs personenbezogene Daten anderer Mandanten erkennen können.

In der Praxis stellt gerade dies für kleine und mittelständische Kanzleien eine hohe Herausforderung dar. Die IT-Systeme der Kanzlei müssen derart konfiguriert sein, dass zum Beispiel der unmittelbare Zugriff auf die Lohn- und Gehaltsabrechnungsdaten von Mandanten den damit nicht betrauten Mitarbeitern nicht zugänglich ist. Vor dem Hintergrund der notwendigen Flexibilität im Vertretungsfall und auch aus Kostenaspekten (Einrichtung, Überwachung und Dokumentation der Berechtigung) ist dies ein wesentlicher Aspekt für Kanzleien.

Praxistipp:
DATEV bietet an dieser Stelle beispielsweise im Programm Rechteverwaltung die Möglichkeit, Zugriffsrechte zu steuern und zu vergeben. Voraussetzung hierfür ist ein Administratorzugang zum System.

Teilweise nehmen Mitarbeiter auch bereichsübergreifende Tätigkeiten vor. Beispiele dafür sind:

- Derselbe Mitarbeiter erstellt Jahresabschlüsse und wirkt bei einer Jahresabschlussprüfung mit.
- Dieselbe Mitarbeiterin erstellt eine Lohn- oder Gehaltsabrechnung und nimmt monatlich die Finanzbuchführung eines Mandanten vor.
- Das Sekretariat übernimmt Aufgaben im Bereich der Personalverwaltung.

Man erkennt hier ein Spannungsfeld im Bereich des Datenschutzes. Da häufig in kleinen und mittelständischen Kanzleien ein Mitarbeiter für verschiedene bereichsübergreifende Themen zuständig ist, ist hier eine klare Trennung der Berechtigungen nicht oder nicht immer möglich.

Die Anzahl der IT-Systeme ist in kleinen und mittelständischen Kanzleien häufig hoch. Es handelt sich hier um File-Server-Laufwerke, die E-Mail-Software (häufig Outlook) sowie das Kanzleisystem (häufig DATEV), sodass eine Pflege aller Systeme zur Einhaltung der datenschutzrechtlichen Anforderungen erfolgen muss.

3.2.2 Neuanlage von Mandanten

Während an anderer Stelle die technischen und organisatorischen Maßnahmen aus datenschutzrechtlicher Sicht für die jeweilige Dienstleistung beschrieben wird, möchten wir im Folgenden zunächst auf allgemeine Aspekte aus Sicht des Datenschutzes bei der Neuanlage von Mandanten eingehen. Bezüglich der Sicherheitsvorkehrungen und datenschutzrechtlichen Aspekte verweisen wir auf den Abschnitt 6.

Die Auftragsannahme von Mandanten erfolgt in der Regel durch die Kanzleileitung. Abhängig von der Größe der Kanzlei unterscheiden sich die Prozesse bei der Entscheidungsfindung, ob und zu welchem Zeitpunkt ein Auftrag angenommen werden kann, unter anderem werden die Aspekte der Unabhängigkeit oder auch der verfügbaren Mitarbeiter vorweg von der Kanzleileitung dokumentiert.

Bei einem Mandatszugang werden im IT-System der Kanzlei regelmäßig auch personenbezogene Daten erhoben. Es handelt sich dabei entweder um personenbezogene Daten der entsprechenden Mitarbeiter bei einem Auftrag zur externen Lohn- und Gehaltsabrechnung oder auch um personenbezogene Daten von natürlichen Personen bei Aufträgen zur Erstellung der Einkommensteuererklärung oder sonstiger Dienstleistungen.

Diese Daten werden häufig in den Kanzleisystemen als Mandantenstammdaten elektronisch vom bisherigen Berater oder dem Unternehmen übernommen und gegebenenfalls noch einmal ergänzt.

In der Kanzlei können verschiedene Abteilungen bzw. Mitarbeiter auf die personenbezogenen Mandantenstammdaten zugreifen. Diese Daten können beispielsweise Zwecken der Mandatspflege (Geburtstagswünsche oder Firmenjubiläum) oder auch der Rechnungsstellung dienen (Privatanschrift, abweichende Rechnungsanschrift oder sonstige Besonderheiten im Zusammenhang mit der Rechnungsstellung).

Es ist an dieser Stelle darauf hinzuweisen, dass die personenbezogenen Mandantenstammdaten nur insoweit den Mitarbeitern bekannt gegeben werden sollen, als diese auch für die Bearbeitung des jeweiligen Auftrags notwendig sind oder der Mandant hierzu eine Einwilligungserklärung erteilt hat.

Praxistipp:
Bei einem Auftrag zur Erstellung einer Einkommensteuererklärung werden unter anderem Religionszugehörigkeit, die Namen von Kindern, die Geburtsdaten der mit veranlagten Ehegatten und andere personenbezogene Daten aufgenommen.

Es empfiehlt sich hier, bei der Auftragsanlage auch von den Ehegatten ein Einverständnis zur Verarbeitung der personenbezogenen Daten einzuholen. Dieses Einverständnis sollte auch die Verarbeitung der Daten der gemeinsam mit den Eltern veranlagten Kinder berücksichtigen.

Auch in diesem Bereich ist wiederum ersichtlich, dass die Trennung der Funktionen und das Vorhandensein eines ausführlichen Berechtigungskonzepts für die Einhaltung der datenschutzrechtlichen Aspekte unabdingbar ist.

Hierbei müssen ebenfalls die organisatorischen Regelungen berücksichtigt werden. Konkret bedeutet dies für den Prozess der Auftragsanlage im IT-System der Kanzlei, dass Aufträge nur dann angelegt werden können, wenn eine Freigabe durch die Kanzleileitung erfolgt ist. Die zur Auftragsanlage befugten Mitarbeiter sollten klar definiert sein. Gleichzeitig mit der Anlage des Auftrags sind die jeweiligen Berechtigungen im IT-System der Kanzlei zu hinterlegen.

Hinweis:
Personenbezogene Daten sind bei der Auftragsanlage regelmäßig nicht auf den File-Servern oder im E-Mail-System vorhanden. Vielmehr muss sich die Ausgestaltung des Berechtigungskonzepts auf das „Warenwirtschaftssystem“ der Kanzlei beziehen.

3.2.3 Gewährleistung eines sicheren Datenaustauschs

Die Gewährleistung eines sicheren Datenaustauschs ist ein unverzichtbarer Bestandteil eines aktiven, vollumfänglichen Datenschutzes in der Kanzlei. In der Steuerberater- und Wirtschaftsprüferbranche muss Datenschutz an oberster Stelle stehen, was neben einer lückenlosen Dokumentation auch den sicheren Datenaustausch inkludiert. Während in früheren Jahrzehnten ein sicherer Datenaustausch noch durch Wachs und Siegel gewährleistet wurde, ist die Komplexität des Datenaustauschs im Jahr 2019 deutlich gestiegen. Obwohl der Versand einer E-Mail mit wenigen Klicks geschehen ist, bedarf es einiger Mehreinstellungen und eines großen Maßes an Erfahrung, um den E-Mail-Versand auch so sicher wie möglich zu gestalten.

E-Mails jeglicher Art und Priorität überfluten täglich die Postfächer der Kanzleien. Sowohl E-Mails interner als auch externer Absender finden sich in rauen Mengen in den Postfächern der Mitarbeiter. Trotz der Mahnung zur Datenminimierung im Rahmen der DSGVO, versenden Mitarbeiter E-Mails an unnötig große Verteilergruppen, leiten E-Mails samt Anhang bedenkenlos weiter und teilen große Dateien direkt per E-Mail. Diese Flut an E-Mails und Daten steht nun der DSGVO gegenüber.

In der digitalen Kanzlei geschieht der Datenaustausch zwischen den Mitarbeitern und mit den Mandanten hauptsächlich über E-Mails. Da es sich größtenteils um schützenswerte Daten handelt, muss eine sichere E-Mail-Kommunikation gewährleistet sein. Diese lässt sich auf mehrere Ebenen herunterbrechen. Sie beinhaltet sowohl die Transportverschlüsselung als auch die Inhaltsverschlüsselung und die Verschlüsselung des Anhangs. Nur wenn alle drei Ebenen verschlüsselt sind, kann ein sicherer, DSGVO-konformer Versand sichergestellt werden. Ergänzend kann zusätzlich zum sicheren Versand eine eindeutige E-Mail-Signatur erstellt werden.

Transportverschlüsselung vs. Ende-zu-Ende-Verschlüsselung

Die Transportverschlüsselung SSL bzw. TLS ist in den meisten gängigen E-Mail-Programmen wie beispielsweise Outlook, Web.de, GMX oder T-Online bereits integriert. Ein Versand ohne Transportverschlüsselung ist bei diesen Anbietern beispielsweise nicht mehr möglich. Während SSL, das Secure Socket Layer, vielen technisch versierten Nutzern noch

ein Begriff war, ist der Nachfolger TLS noch weitgehend unbekannt. TLS steht für Transport Layer Security und ist ein hybrides Verschlüsselungsprotokoll, welches zur sicheren Datenübertragung im Internet dient. TLS ist eine Punkt-zu-Punkt-Verschlüsselung. Wie bereits der Name sagt, verschlüsselt das TLS den Inhalt bei der Übermittlung zwischen Versender und E-Mail-Provider (Absender), dem E-Mail-Provider (Absender) und dem E-Mail-Provider (Empfänger) sowie dem E-Mail-Provider (Empfänger) und dem tatsächlichen Empfänger. Auch wenn das Risiko eines Abfangens einer E-Mail mit dieser Maßnahme zwar schon drastisch gesenkt wurde, birgt diese Verschlüsselung dennoch ein Risiko. Bei genauerer Betrachtung fällt auf, dass die E-Mail nicht von Absender bis Empfänger verschlüsselt ist, sondern vielmehr von Übertragungspunkt zu Übertragungspunkt. Die E-Mail selbst wird beispielsweise auf dem Server des Providers entschlüsselt, um sie auf Viren oder Spam zu durchsuchen. Vorteil dieser Methode ist, dass dies ohne Zutun des Empfängers geschieht, sodass keine weitere Einrichtung durch den Nutzer erforderlich ist.

Anders als bei der gängigen TLS-Verschlüsselung, muss bei der Ende-zu-Ende-Verschlüsselung zusätzliche Software installiert werden. Mit Hilfe eines Austauschs von privaten und öffentlichen Schlüsseln können die E-Mails während der Übertragung vollständig verschlüsselt bleiben. Eine Vorabsortierung bzw. -durchsuchung auf Viren oder Spam kann zwar nicht erfolgen, angesichts der Tatsache, dass sowohl der Absender als auch der Empfänger sich untereinander „kennen“, ist dies jedoch auch nicht notwendig. Eine Möglichkeit der Ende-zu-Ende-Verschlüsselung bietet hier beispielsweise die DE-Mail.

E-Mail-zu-PDF-Verschlüsselung

Eine weitere Option der E-Mail-Verschlüsselung ist die E-Mail-zu-PDF-Verschlüsselung. Namhafte Softwarehersteller bieten mit Hilfe eines Outlook-Plug-ins die Möglichkeit, E-Mails in das PDF-Format zu verschlüsseln.

Entscheidender Vorteil dieser Option ist, dass nahezu jeder Rechner und jedes mobile Endgerät PDFs öffnen kann. Sicherheitstechnisch bietet die PDF-Verschlüsselung zwei große Vorteile. Einerseits kann sowohl die E-Mail als auch ihr Inhalt nach Versand nicht verändert werden. Der zweite Vorteil ist, dass die E-Mail mit einem Passwort geschützt werden kann, sodass niemand Unberechtigtes auf die E-Mail oder ihren Anhang Zugriff hat.

Praxistipp:
Grundsätzlich sollten Passwörter, egal in welchem Bereich sie angewendet werden, auf jeden Fall den Mindestanforderungen des BSI entsprechen.

Das Prinzip der E-Mail-zu-PDF-Verschlüsselung ist denkbar einfach. Die Software wird als Plug-in entweder auf dem PC des Absenders oder auf dem Server der Kanzlei installiert.

Möchte der User nun eine E-Mail versenden, kann er dies wie gewohnt mit seinem Outlook-Programm machen. Die Erstellung der E-Mail findet wie gewohnt im Outlook-E-Mail-Fenster statt. Anhänge werden wie gewohnt eingefügt und der Text standardmäßig geschrieben. Nach Beendigung der Erstellung, wird das Plug-in der Verschlüsselungssoftware ausgewählt. Anschließend wählt der User ein Passwort, dass entweder 128-bit- oder 256-bit-verschlüsselt wird.

Nach Bestätigung des Passworts öffnet das E-Mail-Programm eine Transport-E-Mail, die darauf hinweist, dass die E-Mail verschlüsselt ist und der Inhalt sich als passwortgeschütztes PDF im Anhang befindet. Das Layout und der Text dieser E-Mail lassen sich individuell anpassen.

Das Programm selbst hat im Moment der Passworteingabe beim Versenden einen PDF-Container erstellt. Dieser enthält alle Anhänge im Originalformat und den Text der E-Mail als PDF. Die Transport-E-Mail enthält lediglich ihren individuellen Text. Der geschützte Text der E-Mail kann erst durch Eingabe des Passworts aufgerufen werden.

Der Empfänger selbst benötigt keine Zusatzsoftware, außer einen PDF-Reader. Das Passwort zur E-Mail sollte im besten Fall telefonisch oder per SMS ausgetauscht werden.

Anhangsverschlüsselung

Die Unterscheidung zwischen nicht schützenswerten Daten und schützenswerten Daten ist nicht trivial. Das Postulat der Datenminimierung ist an dieser Stelle ein guter Grundsatz, um einen sicheren Datenaustausch zu konzipieren und umzusetzen.

Grundsätzlich beginnt ein sicherer Datenaustausch beim Verständnis der Mitarbeiter. Tatsache ist, dass der sichere Datenaustausch meist mehr Aufwand verursacht als der gewöhnliche, ungeschützte E-Mail-Versand. Dennoch sollten bei dem Versand und Austausch von sensiblen Daten Vorkehrungen getroffen werden, wie beispielsweise eine Verschlüsselung.

Empfehlenswert ist neben der Verschlüsselung der E-Mail grundsätzlich die Verschlüsselung des Anhangs. Mit kostenlosen Packprogrammen wie beispielsweise 7-Zip lassen sich Ordner mit wenigen Klicks in Zip-Dateien umwandeln. Zip-Dateien sind komprimierte Ordner, die während des Zip-Vorgangs mit einem Passwort geschützt werden können.

Der sicherheitstechnische Vorteil liegt darin, dass die Datei in verschlüsseltem Zustand versendet wird und anschließend vom Absender durch das vorher festgelegte Passwort entschlüsselt werden kann. Um die Sicherheit weiter zu erhöhen, sollte das Passwort entweder vorher mit dem Empfänger ausgetauscht werden, oder es wird ihm über einen anderen Kommunikationsweg, wie beispielsweise eine SMS, übermittelt. Das Passwort selbst sollte mindestens den BSI-Richtlinien entsprechen, d. h. es sollte aus mindestens acht Buchstaben bestehen, Klein- und Großschreibung beinhalten, ein oder mehrere Sonderzeichen und eine oder mehrere Zahlen beinhalten.

Hinweis:

Jedes von Ihnen gewählte Passwort sollte den BSI-Kennwort-Richtlinien entsprechen.[3] Ein sicheres Passwort sollte folgende Kriterien erfüllen:

- mindestens acht Zeichen
- Groß- und Kleinbuchstaben
- Ziffern
- Sonderzeichen

Je mehr der oben genannten Kriterien erfüllt sind, desto sicherer ist Ihr Passwort.

[3] Quelle: BSI Grundschutzkatalog, Umsetzungshinweise zum Baustein APP.2.2 Active Directory, online abrufbar unter https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/APP/Umsetzungshinweise_zum_Baustein_APP_2_2_Active_Directory.html (zuletzt abgerufen am: 20.11.2019)

Prozess- und Arbeitsschritte werden vermehrt digital abgebildet. Wirtschaftsprüfungs- und Steuerberatungspraxen sind von diesen Veränderungen und den neuen Herausforderungen genauso betroffen wie die Industrie.

Datenschutzrechtlich sind dabei einige Fallstricke zu beachten, insbesondere vor dem Hintergrund der Datenschutzgrundverordnung (DSGVO). Dieser Praxisleitfaden legt den Fokus auf die wesentlichen Handlungsnotwendigkeiten im Bereich des Datenschutzes in der Praxis:

- Einrichtung von organisatorischen Maßnahmen zur Sicherstellung des Datenschutzes
- Umgang mit personenbezogenen Daten von Mandanten, Mitarbeitern und Dienstleistern
- Darstellung der notwendigen TOMs (technische und organisatorische Maßnahmen) auf Ebene der IT-Systeme, z.B. im Mailverkehr, den Mandantenstammdaten oder auf Ebene der Netzwerklaufwerke

Das Buch enthält viele Beispiele, Tipps und praktische Handlungsempfehlungen und bietet so einen schnellen Überblick über die Thematik und die erforderlichen Maßnahmen in Wirtschaftsprüfungs- und Steuerberatungspraxen. Die datenschutzrechtlichen Aspekte, die sich aus der (häufig in kleineren und mittelständischen Kanzleien anzutreffenden) bereichsübergreifenden Tätigkeit der Mitarbeiter ergeben, werden gesondert hervorgehoben.

IDW VERLAG GMBH

ISBN 978-3-8021-2467-9
Preis: 49,00 € (D)
www.idw-verlag.de