Praxistipps IT

Datenschutz in Zeiten digitaler Transformation

Zukunftssicher in der Kanzlei 4.0

Rouven Friederich / Andreas Schneider

IDW VERLAG GMBH

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.