Das Infomagazin Ihres Verbandes

LSWB magazin

JG 72 – B20108 E **Ausgabe 1/2017**

INFO = Vorsprung

Abgeschirmt

So schützen Sie die Daten Ihrer Mandanten Seite 10

Die europäische Interessenvertretung der EFAA **Seite 25**

Die Jahrespressekonferenz des Bundesfinanzhofs **Seite 27**

Neue Gestaltungsrisiken bei der Einheitsbewertung **Seite 30**

www.lswb-magazin.bayern

Must-haves im Datenschutz

Von Dirk Munker, Dipl.-Staatsw. (Univ.), Datenschutz-Auditor (TÜV)

Datenschutz ist nicht gleich Datensicherheit: Datenschutz hat Grundrechtsrang.

Für Steuerberater und ihre Mitarbeiter gibt es viele Fallstricke in Sachen Datenschutz. Hierzu gehören die allzu leichtfertige Beantwortung von Anfragen, die Gefahren von Social Engineering[1] oder der fehlerhafte Umgang mit IT und Technik: Oft sind sich die handelnden Personen nicht im Klaren darüber, welche Folgen ein, wenn auch unbeabsichtigtes, Fehlverhalten haben kann. Der folgende Artikel gibt einen Überblick über die komplexe Thematik und zeigt auf, welche Mindestanforderungen Steuerberaterkanzleien einhalten müssen.

Das Thema Datenschutz wird von Kanzleien (zu) oft vernachlässigt. Das Gefährdungspotenzial steigt durch moderne Technik und die jederzeitige Verfügbarkeit von Daten, mit denen ein leichtes Erstellen von Profilen und Querverbindungen möglich ist. Der Schutz personenbezogener Daten ist jedoch gesetzlich im Bundesdatenschutzgesetz (BDSG) und zukünftig in der EU-Datenschutz-Grundverordnung (EU-DSGVO)[2] vorgeschrieben und somit in der Kanzlei entsprechend umzusetzen. Wer diese Vorschriften ignoriert, muss mit einem Bußgeld (aktuell bis zu 300.000 Euro, ab 25. Mai 2018 bis zu 20 Millionen Euro) und je nach Fall mit Schadensersatzforderungen rechnen. Der Imageschaden bei einem bekanntgewordenen Vorfall ist jedoch oft noch viel gravierender.

[1] Als Social Engineering bezeichnet man die psychologische Manipulation von Menschen, um bestimmte Ziele, etwa die Preisgabe vertraulicher Informationen oder den Kauf eines bestimmten Produkts, zu erreichen.
[2] Siehe hierzu auch den Beitrag "Fit für die Europäische Datenschutzgrundverordnung" auf www.lswb-magazin.bayern/DSGVO

Datenschutz ist aber nicht nur lästige Pflicht, es sind auch viele Vorteile damit verbunden. Ein gutes Datenschutzmanagement fördert klare Arbeitsanweisungen, bringt Image- und Vertrauensgewinn nach innen und außen und trägt zur Schadensprävention bei. Auch im Marketing kann das Thema Datenschutz sehr positiv genutzt werden.

Was bedeutet Datenschutz?

Entgegen der Begrifflichkeit geht es hier nicht um den Schutz von Daten, sondern um das Recht einer Person auf informationelle Selbstbestimmung, sprich um den Schutz der Person als Betroffene vor unberechtigtem Umgang mit Informationen über sich selbst, zum Beispiel durch ungewollte Speicherung, Auswertung oder werbliche Nutzung (Stichwort „gläserner Mensch“). Das BDSG gilt allerdings nicht im persönlichen oder familiären Bereich, sondern für den Umgang von Unternehmen und sonstigen nicht-öffentlichen und öffentlichen Stellen mit den Informationen über Personen.

Das Grundgesetz bildet die Basis für den Datenschutz. In Artikel 1 Abs. 1 GG heißt es: „Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist die Verpflichtung aller staatlichen Gewalt.“ Artikel 2 Abs. 1 GG präzisiert weiter: „Jeder hat das Recht auf freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.“ Aus dem späteren sogenannten Volkszählungsurteil vom 15. Dezember 1983 entstand in Deutschland das „Grundrecht auf informationelle Selbstbestimmung“. Hierzu gehört auch der Schutz der Privatsphäre und die Kenntnis darüber, welche Daten wo gespeichert sind. Datenschutz hat in Deutschland somit Verfassungsrang.

Ab 25. Mai 2018 ändert sich die Gesetzeslandschaft zum Datenschutz in Europa komplett. Seit 25. Mai 2016 ist die EU-Datenschutz-Grundverordnung in Kraft und gilt nach einer zweijährigen Übergangsfrist – mit Ausnahme der wenigen nationalen Ausgestaltungsspielräume – unmittelbar in allen Mitgliedsstaaten.

Alle Daten in Steuerkanzleien unterliegen grundsätzlich der bekannten standesrechtlichen Verschwiegenheitspflicht aus § 203 StGB sowie §§ 57 und 62 StBerG. Darüber hinaus sind im BDSG konkrete Maßnahmen zum Schutz der personenbezogenen Daten von Mandaten, aber auch Mitarbeitern und Geschäftspartnern vorgesehen, um die erforderlichen personellen und organisatorischen Voraussetzungen für eine gewissenhafte Berufsausübung in der Kanzlei zu gewährleisten.

Welche Must-haves im Datenschutz sind in der Steuerkanzlei nun umzusetzen?

Die Bestellung eines Datenschutzbeauftragten, intern oder extern, ist für alle Kanzleien verpflichtend, in denen mehr als neun Mitarbeiter ständig personenbezogene Daten verarbeiten. Hierbei sind alle Köpfe zu zählen, einschließlich der Geschäftsleitung. In Kanzleien mit weniger Mitarbeitern entfällt lediglich die Bestellpflicht für den Datenschutzbeauftragten, die Umsetzung der Vorschriften liegt dann allein bei der Kanzleileitung.

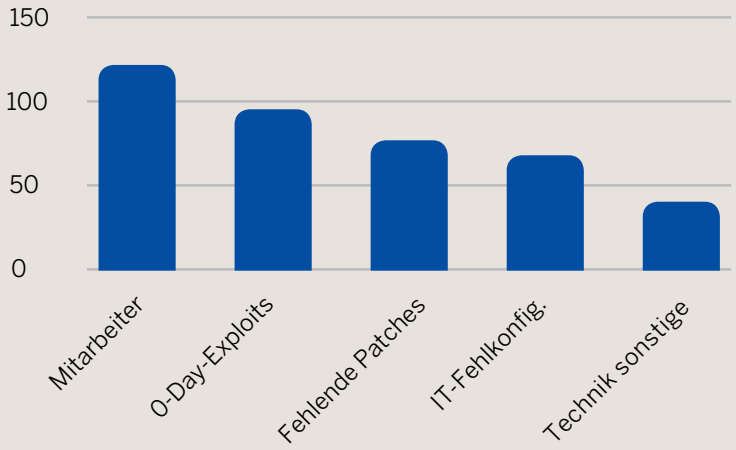
Ganz grundlegend muss die Geschäftsführung zunächst definieren, welche Ziele im Datenschutz erreicht werden sollen, denn die Umsetzung der rechtlichen Vorgaben lässt Anpassungsspielraum. Bei der Umsetzung sollte der Datenschutzbeauftragte mit den notwendigen Umsetzungskompetenzen ausgestattet sein. Die Kanzleileitung sollte sich deutlich zum Thema Datenschutz positionieren, um ein klares Signal für den Umgang mit den entsprechenden Regelungen zu setzen.

Datenschutz und die Mitarbeiter

Den Mitarbeitern kommt eine wichtige Rolle bei der Umsetzung der Datenschutzregelungen zu. Im Alltag kann Datenschutz nur funktionieren, wenn alle Mitarbeiter sich aktiv an die Vorschriften und Regelungen halten. Die Schulung und Sensibilisierung aller Mitarbeiter ist daher nicht nur verpflichtend, sondern unumgänglich, wenn die Kanzlei ein sinnvolles Datenschutzniveau erreichen will. Auch die Schulung im Umgang mit EDV und Technik spielt eine große Rolle, denn schon ein unbedachter Mausklick kann schwerwiegende Folgen haben. Die Schulung ist außerdem notwendig, damit die Mitarbeiter die Inhalte der anschließenden Verpflichtung zur Verschwiegenheit nach § 5 BDSG verstehen. Mitarbeiter im Personal- beziehungsweise Administrationsbereich sind gegebenenfalls auch nach § 88 Telekommunikationsgesetz und § 35 Sozialgesetzbuch I zu verpflichten. Die Auskunftsfähigkeit bei datenschutzrechtlichen Anfragen und Auskunftsersuchen von Mandanten und sonstigen Betroffenen ist ebenfalls sicherzustellen. Hier gilt es eine Ansprechstelle zu benennen und den Mitarbeitern Handlungssicherheit zu vermitteln.

Die private Nutzung von EDV und Telekommunikationseinrichtungen (TK) durch die Mitarbeiter sollte schriftlich geregelt werden, denn die Zulassung der privaten Nutzung von EDV und TK setzt eine vertragliche Vereinbarung mit jedem einzelnen Mitarbeiter voraus. Ansonsten stellt jegliche Überwachung der Kanzlei-IT, Protokollierung, Anti-Spam-Automatik etc. einen Eingriff in die Rechte des Mitarbeiters dar. Der Kanzlei wird damit die Kontrolle über die eigenen EDV- und Systemlandschaft zu einem großen Teil entzogen. Ein Verbot dieser privaten Nutzung, insbesondere von E-Mail und Internet, ist zu empfehlen, muss aber sauber geregelt und auch kontrolliert werden. Ohne Kontrolle schleicht sich innerhalb kürzester Zeit die „betriebliche Übung“ ein, und die Nutzung ist wieder erlaubt.

Gründe für den Erfolg von Cyber-Angriffen



Quelle: Cyber-Sicherheits-Umfrage 2015, Allianz für Cybersicherheit

Auf die Frage „Falls eine Institution schon einmal Ziel eines erfolgreichen Cyber-Angriffs war, worauf war der Erfolg zurückzuführen?“ antworteten die Teilnehmer einer Umfrage der Allianz für Cybersicherheit wie nebenstehend abgebildet.

Der wesentliche Grund dafür, dass Cyber-Angriffe erfolgreich sein konnten, war demnach ungewolltes Fehlverhalten von Mitarbeitern.

Weitere Must-haves für die Kanzlei
Als Grundlage für die Umsetzung des Datenschutzes ist ein Verfahrensverzeichnis zu erstellen. Darin wird jedes einzelne Verfahren in der Kanzlei erfasst, in dem personenbezogene Daten verarbeitet werden. Dieses Verzeichnis ist nicht nur Grundlage für die Arbeit des Datenschutzbeauftragten, sondern ist auch auf Anfrage „Jedermann" (jeder natürlichen Person) in geeigneter Art und Weise zur Verfügung zu stellen. Mit der EU-Datenschutzgrundverordnung (EU-DSGVO) entsteht ab 25. Mai 2018 die zusätzliche Verpflichtung, für die einzelnen Verfahren eine Risikobewertung und ggf. eine Datenschutz-Folgenabschätzung vorzunehmen.

Ein weiteres wichtiges Thema ist der Abschluss aller erforderlichen Verträge zur Auftragsdatenverarbeitung nach § 11 BDSG, nicht nur weil fehlende Verträge regelmäßig mit empfindlichen Bußgeldern geahndet werden, sondern weil dies vor dem Hintergrund der berufsrechtlichen Verschwiegenheit unumgänglich ist. Siehe hierzu unseren Fachartikel „Wenn Dienstleister auf Ihre Daten schauen" (Seite 13).

Mit der EU-DSGVO kommen noch weitere Verpflichtungen auf die Kanzleileitung zu wie die Rechenschaftsplicht über alle Maßnahmen zum Datenschutz, zur Datensicherheit und zur IT-Sicherheit. Auf dieses Thema wird im Artikel „Datenschutz, Datensicherheit und IT-Security" genauer eingegangen (Seite 14). Daneben wird als neues Schutzziel im Datenschutz die „Belastbarkeit" der Systeme und Dienste erwähnt. Das heißt, die Systeme der Kanzlei müssen zukünftig einer gewissen Beanspruchung standhalten. Um dies sicherzustellen, ist ein Notfallhandbuch beziehungsweise ein Notfallmanagement in der Kanzlei unumgänglich.

Da die Datenschutzkonformität der Kanzleiwebsite nach außen sofort sichtbar ist, gab es in letzter Zeit zahlreiche Abmahnungen dazu zu verzeichnen. Aus diesem Grund wollen wir hierauf etwas detaillierter eingehen.

Der Einsatz von sogenannten Tracking-Tools wie Google Analytics oder Piwik ist nur erlaubt, wenn die Verarbeitung der Daten den Vorschriften des BDSG und des Telemediengesetzes (TMG) entsprechend abgebildet werden kann. Zum einen muss die Kanzlei einen Vertrag zur Auftragsdatenverarbeitung mit Google schließen. Zusätzlich dazu müssen die IP-Adressen der Besucher der Homepage anonymisiert verarbeitet werden, das Widerspruchsrecht der Betroffenen ist zu beachten (Hinweis in der Datenschutzerklärung) und gegebenenfalls ist die Löschung von Altdaten zu veranlassen, die noch nicht datenschutzkonform erfasst wurden. Als Alternative zur Überwachung des Verkehrs auf der Internetseite der Kanzlei bieten sich Lösungen wie Piwik an, bei denen (zumindest in der Self-Hosted-Variante) die Daten „im Haus" beziehungsweise auf dem Server der Kanzlei bleiben.

Die Kanzlei sollte überprüfen, ob sich auf der Webseite entsprechende Formulare befinden, mit deren Hilfe Daten in die Kanzlei übertragen werden können (Kontaktformular etc.). Dann ist darauf zu achten, dass die Pflichtangaben sich auf das tatsächlich Notwendige beschränken (Grundsatz der Datensparsamkeit) sowie dass ein Hinweis auf die Datenverarbeitung im Datenschutzhinweis erfolgt. Außerdem muss die Übertragung der Daten über ein solches Formular auf der Homepage nach dem Stand der Technik verschlüsselt erfolgen. Falls die Kanzlei einen Newsletter eingebunden hat, muss die Anmeldung im sogenannten Double-Opt-In-Verfahren abgebildet werden (doppelte Bestätigung einer Anmeldung über Online-Formulare und E-Mails).

Alle Internetauftritte müssen über einen Datenschutzhinweis und ein Impressum verfügen, die, neben den Pflichtangaben aus § 13 Telemediengesetz (TMG), § 5 TMG und gegebenenfalls § 55 Abs. 2 Rundfunkstaatsvertrag (RStV), auf die individuellen Gegebenheiten der Kanzlei-Website anzupassen sind. Sowohl der Datenschutzhinweis als auch das Impressum müssen von jeder Seite des Internetauftritts aus leicht zu erreichen sein.

Wer diese Punkte umgesetzt hat, ist in Sachen Datenschutz auf dem richtigen Weg und muss sich auch vor den neuen Anforderungen durch die EU-DSGVO nicht verstecken. ■

Seminare des Autors

Datenschutz in der Steuerkanzlei

Referent: Dirk Munker, Dipl.-Staatsw. (Univ.), Datenschutz-Auditor (TÜV)

15.05.2017, 13:00–17:00 Uhr, Nürnberg
Ramada Parkhotel, Münchener Straße 25

16.05.2017, 09:00–13:00 Uhr, München
LSWB-Forum, Implerstraße 11

Über den Autor

Diplom-Staatswissenschaftler (Univ.) Dirk Munker ist Datenschutz-Auditor (TÜV), Geschäftsführer der Munker Privacy Consulting GmbH und Datenschutzbeauftragter des LSWB. Als Datenschutzberater und externer Datenschutzbeauftragter betreut er mit seinen Mitarbeitern bundesweit Steuerkanzleien und Unternehmen sowie den LSWB.

Seit Januar 2017 ist Munker Privacy Consulting LSWB-KanzleiPlus-Partner. Mitglieder bekommen daher zahlreiche Dienstleistungen des Unternehmens zu Sonderkonditionen.

Ihre Ansprechpartnerin bei Munker Privacy Consulting:
Christine Munker
E-Mail: c.munker@munker.info
Web: www.munker.info

Vorsicht Falle: Wenn Dienstleister auf Ihre Daten schauen

Von Dirk Munker, Dipl.-Staatsw. (Univ.), Datenschutz-Auditor (TÜV)

Daten sind in Ihrer Kanzlei sicher: Wie sieht es bei Ihren Partnern und Dienstleistern aus?

Bei der Erbringung bestimmter Leistungen können Dienstleister auf die Daten einer Steuerkanzlei schauen. Das ist zum Beispiel bei der Fernwartung von Software oder der Telefonanlage der Fall, aber auch beim IT-Monitoring, bei der Auslagerung der Lohnbuchhaltung oder bei der Nutzung eines Rechenzentrums oder von Cloud-Diensten. Man spricht dann von einer sogenannten Datenverarbeitung im Auftrag oder Auftragsdatenverarbeitung (ADV) im Sinne des § 11 BDSG. Anders gesagt ist das immer dann der Fall, wenn sich die Kanzlei einer Stelle bedient, die für sie im Auftrag und weisungsabhängig personenbezogene Daten erhebt, verarbeitet oder nutzt. Die Kanzlei als Auftraggeber haftet hierbei weiterhin dem Dateneigentümer (Betroffenen) gegenüber für die Einhaltung der datenschutzrechtlichen Vorschriften.

Eine Funktionsübertragung hingegen liegt vor, wenn der Auftragnehmer nicht nur weisungsabhängig datenverarbeitende Hilfsfunktionen durchführt, sondern die übergebenen Daten zur nicht weisungsgebundenen Erfüllung von Aufgaben oder Funktionen benötigt. Dies ist zum Beispiel der Fall, wenn die Daten zur weiteren Beratung eines Mandanten an einen Rechtsanwalt weitergegeben werden. Damit handelt es sich um eine Übermittlung personenbezogener Daten an „Dritte“. Die Haftung gegenüber dem Dateneigentümer geht, anders als bei der Datenverarbeitung im Auftrag, an den Funktionsnehmer über. Für die Übermittlung ist auch diesem Fall eine Rechtsgrundlage, in der Regel eine Einwilligung des Mandanten, erforderlich.

Im Falle einer ADV ist die Kanzlei verantwortlich für die sorgfältige Auswahl des Dienstleisters unter Berücksichtigung dessen Datenschutz- und Datensicherheitsniveaus sowie der technisch-organisatorischen Maßnahmen. Bei der Beauftragung ist in jedem Fall ein schriftlicher Auftrag zur Festlegung detaillierter Vorgaben (siehe § 11 Abs. 2 BDSG) wie die Kontrolle des angemessenen Niveaus der beim Auftragnehmer getroffenen technisch-organisatorischen Maßnahmen notwendig. Die Ergebnisse solcher Kontrollen müssen in der Kanzlei dokumentiert werden. Außerdem verpflichtet sich der Dienstleister, ausschließlich weisungsgebunden zu arbeiten und seine Mitarbeiter auf das Datengeheimnis nach § 5 BDSG zu verpflichten.

Wichtig ist, dass all diese Punkte geklärt sind, bevor der erste Datensatz an den Auftragnehmer übermittelt wird. Die Kontrolle des Dienstleisters muss dabei nicht zwingend vor Ort auditiert werden, es reicht auch die Vorlage von Zertifikaten, Auditberichten oder Selbstauskünften. Die technischen und organisatorischen Maßnahmen müssen jedoch konkret aufgelistet und nicht nur beispielhaft benannt werden. Das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) hat im Fall einer unzureichenden Auftragserteilung bereits in 2015 eine Geldbuße in fünfstelliger Höhe festgesetzt.

Steuerkanzleien unterscheiden sich bei der organisatorischen Regelung der Zusammenarbeit mit Dienstleistern von anderen Unternehmen durch den § 203 Strafgesetzbuch (StGB). Dieser besagt, dass die Offenbarung von Mandantendaten nur mit Einwilligung der Mandanten erlaubt ist. Diese ist in allen Fällen, in denen Kanzleien Dienstleister hinzuziehen, die auf die mandantenbezogenen Daten der Kanzlei schauen können, erforderlich. Bisher sind kaum Verfahren zu § 203 StGB bekannt, da diese Verstöße ein Antragsdelikt darstellen und einen Strafantrag des Betroffenen voraussetzen. Es bleibt jedoch ein Risiko, das gegebenenfalls mit einem finanziellen Schaden und einem Imageschaden für die Kanzlei sowie mit persönlichem Haftungsrisiko für den Berater einhergeht, wenn der Verstoß gegen das Berufsgeheimnis offenkundig wird, zum Beispiel durch eine Datenschutzpanne. Mit entsprechenden Einwilligungen durch die Mandanten kann sich die Kanzlei jedoch gegen dieses Risiko wappnen. ■

Datenschutz, Datensicherheit und IT-Sicherheit

Von Dirk Munker, Dipl.-Staatsw. (Univ.), Datenschutz-Auditor (TÜV)

Mit der Definition von Datenschutz haben wir uns bereits im Artikel „Must-haves im Datenschutz“ befasst. Datensicherheit („Safety”) hingegen ist der Schutz vor ungewolltem Datenverlust, zum Beispiel durch Feuer im Serverraum, Festplattendefekt, Hochwasser etc. Hierzu zählen auch menschliches Versagen beziehungsweise Mitarbeiterfehler. IT-Sicherheit („Security”) ist der Schutz vor gewolltem Datenverlust, vor gewollten Angriffen auf die Vertraulichkeit, Integrität und Verfügbarkeit von Daten. Beste Beispiele hierfür sind die Angriffe auf Kanzleien mit sogenannten Erpressungstrojanern in der letzten Zeit.[1]

IT-Sicherheit und Datensicherheit befassen sich auch mit dem Schutz von Daten ohne Personenbezug. Es geht um die Frage, welche Maßnahmen zum Schutz der Daten vor Verlust getroffen werden müssen. Noch bis zum In-Kraft-Treten der EU-DSGVO finden sich die gesetzlichen Vorgaben dazu im § 9 BDSG beziehungsweise dessen Anlage, der die geeigneten technisch-organisatorischen Maßnahmen vorgibt, die in der Kanzlei umzusetzen sind. Der entsprechende Umgang mit EDV und IT kann beispielsweise in einer IT-Richtlinie für die Mitarbeiter verbindlich geregelt werden, die unter anderem die Nutzung privater Hard- und Software, eine Passwortregelung, die Weitergabe vertraulicher Informationen, Regelungen für die Heimarbeit und einige weitere Vorgaben enthalten sollte.

Im Wesentlichen geht es um vier Schutzziele: Vertraulichkeit, Integrität, Verfügbarkeit und Resilienz (Belastbarkeit).

Die Vertraulichkeit beschreibt die Tatsache, dass die Daten der Kanzlei nicht in unbefugte Hände geraten dürfen. Hierzu können entsprechende Hardware wie zum Beispiel Firewalls, Programme wie Virenschutzsoftware oder Systemkonfigurationen wie eine Benutzerkontrolle eingesetzt werden.

Beim Thema Integrität geht es um die Verlässlichkeit von Daten und die zuverlässige Funktionsweise von Programmen und Hardware. Es gilt, eine Veränderung der Daten und Fehler in Programmen zu verhindern.

Ein besonderes Augenmerk sollte der Verfügbarkeit der Daten, insbesondere der Datensicherung gelten. Damit die Sicherung im Ernstfall zur Verfügung steht, sollte auf eine externe Lagerung beziehungsweise eine Lagerung in einem anderen Brandabschnitt als der/die Server beziehungsweise außerhalb der Kanzlei (zum Beispiel Bankschließfach oder Online-Sicherung) geachtet werden. Eine Sicherung sollte verschlüsselt erfolgen und vor unbefugtem

Foto: imacture/fotolia

Angriff aus dem Internet: Wie schützen Kanzleien ihre Daten?

Zugriff geschützt werden. Die Sicherungsdatenträger sollten nicht ständig mit dem Server verbunden sein, es sei denn es ist sichergestellt, dass Schadsoftware sich nicht auf diese ausbreiten kann.

Die Datensicherungen und das Datensicherungskonzept müssen regelmäßig überprüft werden, damit die relevanten Datenbestände komplett, lesbar und wiederherstellbar gesichert werden. Leider mussten etliche Kanzleien nach einem Befall mit Schadsoftware feststellen, dass entweder die Sicherungsdatenträger auch von der Schadsoftware befallen waren oder die vorhandenen Datensicherungen für eine Wiederherstellung des Systems ungeeignet waren.

Die Belastbarkeit (Cyber-Resilienz) als neues Schutzziel der EU-Datenschutz-Grundverordnung geht die IT-Sicherheit auf verschiedenen Ebenen an und bezieht Personen, Prozesse und Technologie mit ein, um Störungen und Fehler durch möglichst vorausschauendes Handeln zu vermeiden. Dies findet seinen Niederschlag in einer vorausschauenden IT-Strategie.

Die Einhaltung der wichtigsten Aspekte zu Datensicherheit und IT-Security sind wichtige Bausteine, um ein zielführendes Datenschutzkonzept in der Kanzlei umsetzen zu können. ■

[1] Siehe dazu „Locky und Co“ in LSWB-Magazin 3/2016, S. 28 oder auf www.lswb-magazin.bayern.