Das Infomagazin Ihres Verbandes

LSWB magazin

JG 71 – B20108 E **Ausgabe 5/2016**

INFO = Vorsprung

Mitarbeiter finden und binden

So gewinnen Sie Talente für Ihre Kanzlei. Seite 8

www.lswb-magazin.bayern

Fit für die EU-Datenschutz-Grundverordnung?

Von Dirk Munker, Munker Privacy Consulting

Ab dem 25. Mai 2018 gelten europaweit neue Datenschutzregelungen. Was ist in der Kanzlei zu tun, um die Prozesse zeitgerecht anzupassen? Zurücklehnen oder durchstarten? Die Antwort gibt Ihnen unsere zweiteilige Artikelserie.

Bevor wir uns mit der konkreten Umsetzung der neuen Anforderungen der EU-Datenschutz-Grundverordnung (EU-DSGVO) in der Kanzlei befassen, werfen wir zunächst einen intensiven Blick auf dieses neue Gesetzeswerk.

Am 14. April 2016 wurde die EU-DSGVO vom EU-Parlament beschlossen und ersetzt damit die aus dem Jahr 1995 stammende Datenschutzrichtlinie der EU. Voraus gingen mehrjährige intensive Verhandlungen und Abstimmungen durch das EU-Parlament, die Europäische Kommission und den Rat der Europäischen Union. Maßgeblichen Anteil an der Entstehung dieser Verordnung hatte nicht zuletzt der parlamentarische Berichterstatter für die Umsetzung der EU-DSGVO, der Deutsche Jan Philipp Albrecht, Grünen-Europaabgeordneter für Hamburg und Schleswig-Holstein und innen- und justizpolitischer Sprecher der Grünen-Europafraktion.

Am 4. Mai 2016 wurde die EU-DSGVO im Amtsblatt der Europäischen Union veröffentlicht und trat 20 Tage später in Kraft, wobei die in ihr enthaltenen gesetzlichen Regelungen erst ab dem 25. Mai 2018 gelten. Allerdings gibt es nach diesem Zeitpunkt keine Übergangsfristen mehr, sodass es bereits jetzt gilt, die bestehenden Prozesse neu zu ordnen und das Datenschutzmanagement der Kanzlei auf die neuen Anforderungen umzustellen. Solange die Grundverordnung noch nicht gilt, muss allerdings auch das Bundesdatenschutzgesetz (BDSG) weiterhin voll beachten werden.

Die EU-DSGVO

Die Ziele der EU-DSGVO sind der Schutz der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf den Schutz personenbezogener Daten. Auch der freie Verkehr personenbezogener Daten hat eine hohe Priorität. Diese Ziele sollen bei der Verarbeitung personenbezogener Daten durch folgende Grundsätze erreicht werden: Rechtmäßigkeit, Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit, Rechenschaftspflicht. Nach wie vor gilt jedoch: Die Verarbeitung personenbezogener Daten ist grundsätzlich verboten, außer es existiert eine gesetzliche Grundlage oder ein Erlaubnistatbestand in Form einer Einwilligung.

Die EU-DSGVO mit ihren 99 Artikeln und 173 Erwägungsgründen, die ebenfalls Bestandteil des Gesetzes sind, ist deutlich umfangreicher als das aktuelle Bundesdatenschutzgesetz. Im Gegensatz zur bisherigen Datenschutzrichtlinie der EU (Richtlinie 95/46/EG), die von den EU-Mitgliedstaaten in nationales Recht umgesetzt werden musste, gilt die EU-DSGVO ohne Umsetzungsakt unmittelbar in allen EU-Mitgliedstaaten. Den Mitgliedstaaten wird es daher nicht möglich sein, den von der Verordnung bereits festgeschriebenen Datenschutz durch nationale Regelungen abzuschwächen oder zu verstärken. Allerdings richtet die EU-DSGVO an den nationalen Gesetzgeber die Aufgabe, auf nationaler Ebene zusätzlich bestimmte Regelungsbereiche auszugestalten und gibt ihm die Möglichkeit zur Gestaltung bestimmter Bereiche an die Hand. Diese Gesetzgebungsverfahren finden ebenfalls in der laufenden Übergangszeit bis Mai 2018 statt, wobei die Bundestagswahl im Herbst 2017 die zur Verfügung stehende Zeit erheblich limitiert.

Herausforderungen für die Kanzlei

Die Herausforderung für die Kanzlei liegt nun darin, die bestehenden Prozesse fit für die EU-DSGVO zu machen, hierbei jedoch die laufende Gesetzgebung zum Datenschutz auf nationaler Ebene nicht unberücksichtigt zu lassen.

Im Rahmen der EU-DSGVO werden zahlreiche Neuerungen auf die Kanzleien zukommen. Die konkrete Umsetzung der oben genannten Ziele finden ihren Niederschlag in Forderungen wie Risikoanalyse und Datenschutz-Folgeabschätzung sämtlicher Verfahren und Prozesse in der Kanzlei, einer Rechenschaftspflicht hinsichtlich der Datenschutz-, Datensicherheits- und IT-Sicherheitsmaßnahmen, strengeren Regelungen bezüglich der Meldung von Datenschutzpannen und damit einhergehend verschärften Bußgeldhöhen mit Bußgeldsummen bis 20 Millionen Euro.

Um auf die sichere Seite zu kommen, sollten Steuerberater die bestehenden Prozesse überprüfen, Schwachstellen zeitnah abstellen und eine aktuelle Dokumentation über alle Prozesse vorhalten. Das sogenannte Verzeichnis von Verarbeitungstätigkeit, bislang als „Verfahrensverzeichnis“ bekannt, gewinnt somit eine völlig neue Qualität. Dieses Verzeichnis ist die Grundlage für die Durchführung von Risikobewertungen und Datenschutz-Folgeabschätzungen. Letztere sind immer dann durchzuführen, wenn die Form der Verarbeitung wahrscheinlich ein hohes Risiko verursacht, insbesondere bei neuen Technologien oder komplexen Anwendungen.

Europaweite Gültigkeit: Im Gegensatz zur bisherigen EU-Datenschutzrichtlinie gilt die EU-DSGVO in allen EU-Mitgliedstaaten.

Die Meldung von Datenschutzpannen an die zuständige Aufsichtsbehörde, in der Regel der Landesbeauftragte für den Datenschutz (in Bayern das Bayerische Landesamt für Datenschutzaufsicht, www.lda.bayern.de) hat zukünftig innerhalb von 72 Stunden zu erfolgen. Falls aufgrund einer Datenschutzpanne ein hohes Risiko für den Betroffenen besteht, ist dieser ebenfalls zu informieren. Da sämtliche Mandantendaten in der Steuerkanzlei der Verschwiegenheit nach § 203 Strafgesetzbuch unterliegen, liegt ein solches Risiko bei einem Verlust stets nahe. Dafür kann es ausreichen, dass diese Daten beispielsweise bei der Übermittlung per E-Mail oder bei der Fernwartung durch Dienstleister unbefugten Personen zur Kenntnis gelangt sind. Zur Vermeidung von Straftatbeständen empfiehlt sich gerade auf Prozesse unter Beteiligung „Dritter“ ein besonderes Augenmerk zu richten!

Die Position der Aufsichtsbehörden, welche zukünftig europaweit zusammenarbeiten werden, wird durch die EU-DSGVO gestärkt. Es ist damit zu rechnen, dass die Aufsichtsbehörden zukünftig ihr Personal aufstocken und intensiver kontrollieren werden, zumal der Datenschutz im Augenblick auch einen hohen politischen Stellenwert hat.

Auch die Anforderungen an die Dienstleister der Kanzlei ändern sich. Während bei einer Auftragsverarbeitung (bislang Datenverarbeitung im Auftrag) die Haftung beim Auftraggeber, sprich in der Kanzlei, verblieb, werden zukünftig Auftraggeber und Auftragsverarbeiter gemeinsam für Datenschutzpannen haften.

Die Rolle des Datenschutzbeauftragten

Die Verantwortung für die Umsetzung all dieser Themen liegt nicht etwa beim Datenschutzbeauftragten, sondern bei der Kanzleileitung. Allerdings tritt der Datenschutzbeauftragte in manchen Fällen beratend beziehungsweise unterstützend hinzu. Nach wie vor hat er allerdings die Aufgabe, die Geschäftsleitung und die Mitarbeiter mit den datenschutzrechtlichen Anforderungen vertraut zu machen (Mitarbeiterschulung) und den Datenschutz in der Kanzlei zu überwachen. In der Praxis wird es vermutlich auch zukünftig so sein, dass der Datenschutzbeauftragte die Themen in der Kanzlei abarbeitet. Nur wird er hierfür zukünftig mehr Zeit einplanen müssen als bisher.

Lesen Sie in der nächsten Ausgabe, welcher konkrete Handlungsbedarf für Steuerkanzleien auf dem Weg zur EU-DSGVO besteht und wie Sie die Anforderungen umsetzen können. ■

Munker Privacy Consulting

Munker Privacy Consulting besteht seit März 2012 und berät Firmen aus verschiedensten Branchen und unterschiedlicher Größenordnung im Bereich Datenschutz. Besonders wohl fühlen sich die Experten des Unternehmens nicht nur in ihrem Spezialgebiet – Datenschutz in Steuerkanzleien – sondern auch als Datenschutzbeauftragte und in der Beratung von Freiberuflern, Dienstleistern und Unternehmen mit hohem Dienstleistungsanteil, sowie Kliniken, medizinischen Versorgungszentren und Arztpraxen.

Machen Sie Ihre Kanzlei fit für die EU-Datenschutz-Grundverordnung!

LSWB kanzleiplus

Teil 2 *unserer Serie*

Von Dirk Munker, Munker Privacy Consulting GmbH

Ab dem 25. Mai 2018 gelten europaweit neue Datenschutzregelungen. Was ist in der Kanzlei zu tun, um die Prozesse zeitgerecht anzupassen? Zurücklehnen oder durchstarten? Die Antwort gibt Ihnen der zweite und abschließende Teil unserer Artikelserie.

In der letzten Ausgabe haben wir einen intensiven Blick auf die EU-Datenschutz-Grundverordnung (EU-DSGVO) geworfen. Heute wollen wir uns mit der Frage beschäftigen, welche Konsequenzen sich für die Kanzlei daraus ergeben.

Als erstes werfen wir einen kurzen Blick auf das, was auch nach dem Inkrafttreten der neuen Gesetzesgrundlagen bestehen bleibt. Es ist beispielsweise davon auszugehen, dass Kanzleien mit mehr als neun Mitarbeitern wie bisher einen Datenschutzbeauftragten bestellen müssen. Auch für den Internetauftritt der Kanzlei bleibt es dabei, dass Impressum, Datenschutzhinweise und Seitenverschlüsselung zu beachten sind. Die Verträge mit Dienstleistern (Stichwort Auftragsdatenverarbeitung) sind weiterhin erforderlich. Einer der wichtigsten Grundsätze im Datenschutz bleibt ebenfalls erhalten: Das sogenannte „Verbot mit Erlaubnisvorbehalt", das nur dann eine Verarbeitung von Daten erlaubt, wenn eine konkrete Einwilligung vorliegt, eine vertragliche Regelung oder eine entsprechende Gesetzesgrundlage.

Informationspflichten

Mit der EU-DSGVO hält die Pflicht zur Information der Betroffenen in wesentlich größerem Umfang als bisher Einzug in die Kanzleien. Zukünftig müssen Mandanten ausführlich über die Datenverarbeitung in der Kanzlei unterrichtet werden. Hierzu gehört neben Zweck und Rechtsgrundlage der Verarbeitung und Angaben zur verantwortlichen Stelle auch die Information über die Person des Datenschutzbeauftragten, sofern die Kanzlei aufgrund ihrer Größe zur Bestellung eines Datenschutzbeauftragten verpflichtet ist. Kanzleien müssen sich außerdem darauf vorbereiten, ihren Mandanten Angaben über Dienstleister, an die personenbezogene Daten der Mandanten oder ihrer Beschäftigten übertragen werden, zukommen zu lassen. Weitere Informationspflichten beziehen sich auf Aufbewahrungs- und Löschfristen, Auskunftsrechte und einen Verweis auf das Beschwerderecht bei der zuständigen Datenschutzaufsichtsbehörde. All diese Angaben sollen eine faire und transparente Verarbeitung der personenbezogenen Daten ermöglichen. Zwar gab es auch bislang Unterrichtungspflichten, es ist jedoch davon auszugehen, dass die bestehenden Datenschutzerklärungen den neuen Anforderungen nicht gerecht werden und entsprechend erweitert werden müssen.

Das „Recht auf Vergessenwerden"

Neben dem Anspruch auf Transparenz in der Datenverarbeitung spielt das „Recht auf Vergessenwerden" eine große Rolle in der EU-Datenschutz-Grundverordnung. Ein Beispiel hierfür ist das Recht von Bewerbern, bei denen es nicht zu einer Anstellung gekommen ist, auf Löschung aller Daten, die im Zusammenhang mit der Bewerbung in der Kanzlei vorhanden waren. Mandantenakten mit steuerrelevanten Daten sind zehn Jahre nach Ende des Mandatsverhältnisses zu vernichten, Aufzeichnungen im Rahmen einer Videoüberwachung jedoch in der Regel spätestens nach 72 Stunden. Letztendlich müssen Speicherdauer beziehungsweise Aufbewahrungsfristen für alle Kanzleiprozesse dokumentiert werden. Außerdem muss sichergestellt sein, dass die Daten nach Ablauf dieser Fristen zu löschen sind. Für uns Deutsche ist das nicht grundsätzlich neu, lediglich die Wertigkeit eines Löschkonzepts für personenbezogene Daten hat zukünftig eine Qualität.

Die Datenschutz-Folgeabschätzung

Wie bereits in unserem ersten Artikel angesprochen, ist für jeden Prozess in der Kanzlei eine sogenannte Datenschutz-Folgeabschätzung vorzunehmen. Dabei ist es nicht mehr ausreichend, die Datensicherheitsmaßnahmen der Kanzlei (technisch-organisatorische Maßnahmen) allgemein zu beschreiben. Vielmehr sollte bei jedem Prozess untersucht werden, zu welchem Zweck die Daten verarbeitet werden, ob die Notwendigkeit für die Datenverarbeitung gegeben ist und welche Risiken mit der Datenverarbeitung verbunden sind. Auf dieser Grundlage sind anschließend die entsprechenden Datensicherheitsmaßnahmen zu planen. Bei webbasierten Anwendungen empfiehlt es sich deshalb zwingend, beim jeweiligen Dienstleister eine detaillierte Beschreibung der technischen Abläufe anzufordern. Es ist außerdem ratsam, die Datenbestände der Kanzlei nach ihrer Sensibilität zu kategorisieren. Wir empfehlen hierzu eine Einteilung in drei Schutzklassen, wobei Daten, die einem Berufsgeheimnis unterliegen, grundsätzlich der höchsten Schutzklasse zuzuordnen sind.

Neben dem Anspruch auf Transparenz in der Datenverarbeitung spielt das „Recht auf Vergessenwerden" eine große Rolle in der EU-Datenschutz-Grundverordnung.

Schutzmaßnahmen

Auch die Datensicherheitsmaßnahmen werden zukünftig eine neue Qualität erlangen. Wie oben bereits aufgezeigt, sind diese Maßnahmen für jeden Prozess gesondert zu beschreiben. Darüber hinaus unterliegt die Kanzlei jedoch zukünftig einer Nachweispflicht über diese Maßnahmen. Der Berater muss darlegen können, dass die Verarbeitung personenbezogener Daten nach „Treu und Glauben" und zum festgelegten Zweck erfolgt, auf das notwendige Maß beschränkt ist, dass alle Daten sachlich richtig und auf dem neuesten Stand sind und durch geeignete technische und organisatorische Maßnahmen geschützt werden. Diese Aufgabe kann nicht durch den Datenschutzbeauftragten und seine regelmäßigen und stichprobenartigen Prüfungen alleine abgedeckt werden. Vielmehr muss der EDV-Beauftragte der Kanzlei oder der IT-Dienstleister regelmäßig die Aktualität und die Wirksamkeit des Schutzes gegen Daten- und IT-Sicherheitspannen auf den Prüfstand stellen und das Ergebnis seiner Überprüfungen dokumentieren.

In diesem Zusammenhang kann auch eine Zertifizierung oder die Einhaltung genehmigter Verhaltensregeln von Vereinigungen oder Verbänden als ein Faktor für die Erfüllung dieser Pflichten herangezogen werden.

Vorgehen bei Datenpannen

Auf die Meldung von Datenschutzpannen an die zuständige Aufsichtsbehörde innerhalb von 72 Stunden haben wir bereits im ersten Teil des Artikels hingewiesen. Woher aber weiß die Kanzlei, welche Daten bei einer Datenpanne gegebenenfalls „verloren" gegangen sind, beziehungsweise Unbefugten zur Kenntnis gelangt sind? Unser Lösungsvorschlag lautet, sich gründlich mit den Prozessen in der Kanzlei auseinander zu setzen und diese im „Verzeichnis der Verarbeitungstätigkeiten" zu dokumentieren. Die EU-Datenschutz-Grundverordnung sieht dieses Verzeichnis, bislang als „Verfahrensverzeichnis" bekannt, verpflichtend zwar nur noch bei Unternehmen ab 250 Mitarbeitern vor. Wir empfehlen jedoch dringend, das Verzeichnis nach wie vor zu führen oder zu erstellen. Nur auf diese Weise erlangt die Kanzlei eine Übersicht über alle datenverarbeitenden Prozesse, die davon betroffenen Daten und Personen sowie die beteiligten Dienstleister. Es bildet die Grundlage für die Datenschutz-Folgenabschätzung und die Risikobewertung der Prozesse und ist daher eine unerlässliche Basis. In diesem Verzeichnis wird jedes Verfahren einer Schutzklasse zugeordnet, die Speicher- und Löschvorgaben werden dokumentiert und die Datensicherheitsmaßnahmen beschrieben.

Kommt es zu einer Panne in Zusammenhang mit einem bestimmten Verfahren oder einer Softwareanwendung in der Kanzlei, kann über dieses Verzeichnis schnell ermittelt werden, welche Datenbestände betroffen sind und ob ein Risiko für die betroffenen Personen besteht.

Was ist konkret zu tun?

Unser erster Appell an die Kanzleien ist daher, das bereits vorhandene Verfahrensverzeichnis unbedingt zu aktualisieren. Sollte die Übersicht über die Verfahren noch nicht existieren, wäre es spätestens jetzt an der Zeit, diese zu erstellen. Sofern vorhanden, bietet das Qualitätsmanagement-Handbuch der Kanzlei eine erste gute Grundlage dafür, die es um weitere Prozesse zu ergänzen gilt.

Zusätzlich dazu sind detaillierte Informationen über die Abläufe bei Dienstleistern einzuholen. Dabei sollten auch die Subunternehmer nicht vergessen werden. Wenn mit den Dienstleistern der Kanzlei noch keine datenschutzrechtlichen Vereinbarungen geschlossen wurden, sollte das möglichst schnell nachgeholt werden.

Auf der Grundlage dieser Unterlagen – dem Verfahrensverzeichnis und den Informationen der Dienstleister – kann im nächsten Schritt die Datenschutzerklärung für die Kanzlei erstellt beziehungsweise aktualisiert werden, die künftig zur Erfüllung der Informationspflichten an die Mandanten gegeben werden muss.

Wer diese Vorgaben beachtet, außerdem den Internetauftritt und Präsenzen in sozialen Netzwerken datenschutzkonform gestaltet, die Mitarbeiter regelmäßig durch seinen Datenschutzbeauftragten schulen lässt und außerdem die Fachkunde des Datenschutzbeauftragten durch regelmäßige Fortbildung sicherstellt, kann dem Start der EU-Datenschutz-Grundverordnung im Mai 2018 gelassen entgegensehen. ■

Seminar des Autors

Datenschutzbeauftragter in der Steuerkanzlei
Referent: Dirk Munker
16.–18.01.2017, München
LSWB-Forum, Implerstraße 11