DATEV magazin

PRAXIS

Sensible Daten schützen

DSGVO im Kanzleiumfeld

AUTOR:
DR. MAXIMILIAN GREGER

Auch Steuerberater und Anwälte unterliegen grundsätzlich den neuen Datenschutzvorschriften. Gleichwohl gelten zugunsten der Berufsträger einige Ausnahmen, da sie bei konsequenter Anwendung der neuen Regeln gegen ihre Berufspflichten verstoßen würden.

Seit dem 25. Mai 2018 ist die bereits am 24. Mai 2016 in Kraft getretene europäische Datenschutz-Grundverordnung (DSGVO) zu beachten. Trotz einer zweijährigen Übergangszeit bestehen bei vielen Steuerberatungs- und Rechtsanwaltskanzleien weiterhin Unsicherheiten im Hinblick auf die Anwendbarkeit des Datenschutzes sowie die erforderlichen Maßnahmen zum Schutz personenbezogener Daten.

Was sind überhaupt personenbezogene Daten?

Der Begriff der personenbezogenen Daten wird in Art. 4 Abs. 1 DSGVO definiert. Danach betrifft der Datenschutz überhaupt nur solche Daten, die einen Personenbezug haben, die also Rückschlüsse auf eine bestimmte natürliche Person zulassen. Das ist beispielsweise der Fall, wenn es sich um Informationen über persönliche oder finanzielle Verhältnisse einer Person handelt. Namen, Anschriften, Telefonnummern, E-Mail-Adressen, IP-Adressen, Geburtsdatum und Kontodaten eines Menschen sind hingegen die klassischen personenbezogenen Daten. In einer Steuerberatungs- oder Anwaltskanzlei werden meist zahlreiche weitere personenbezogene Daten, wie etwa Steuerdaten, Gehälter, Vermögen, familiäre Verhältnisse, intime Details, verarbeitet. Um keine personenbezogenen Daten handelt es sich hingegen bei finanziellen Kennzahlen einer Kapitalgesellschaft wie Umsatzzahlen, Lagerbestände oder Inventar.

Anwendung in den Kanzleien

Einige Steuerberater und Rechtsanwälte sind der Ansicht, die DSGVO sei aufgrund der ohnehin bestehenden standesrechtlichen Geheimhaltungspflichten nicht auf sie anwendbar. Doch unabhängig von besonderen Berufspflichten gelten die Datenschutzbestimmungen für jede natürliche oder juristische Person, die eigenverantwortlich oder im Auftrag eines Dritten personenbezogene Daten zumindest teilweise automatisiert verarbeitet, beispielsweise mithilfe von Computern. Das ist schon der Fall, wenn ein Praktikant Daten in den Computer eingibt. Folglich erfasst die DSGVO auch Steuerberater und Anwälte. Für die Frage, ob die Verordnung für Anwälte und

Steuerberater gilt, ist daher auch der Streit nicht weiter relevant, ob der Berufsträger Daten nur im Auftrag verarbeitet oder – so die mittlerweile überwiegende Meinung – eigenverantwortlich.

Die wichtigsten Neuerungen

Zunächst die gute Nachricht: Trotz der Neuregelung durch die DSGVO haben sich die seit über 40 Jahren geltenden Grundprinzipien des Datenschutzes nicht geändert – allen voran das Verbot mit Erlaubnisvorbehalt, wonach die Verarbeitung personenbezogener Daten grundsätzlich verboten ist, wenn sie nicht ausnahmsweise auf eine rechtliche Grundlage gestützt werden kann. An Neuerungen bringt die DSGVO vor allem zahlreiche, auf den ersten Blick nicht so offensichtliche Pflichten mit sich. Der Verantwortliche muss innerhalb seines Betriebs lückenlos dafür sorgen, dass der Datenschutz auf allen Ebenen umgesetzt wird. Seine Maßnahmen muss er nachvollziehbar dokumentieren, indem er über die relevanten datenschutzrechtlichen Vorgänge ein Verzeichnis führt (Verfahrensverzeichnis). Zudem muss er sich regelmäßig fragen, ob seine Maßnahmen zum Datenschutz (noch) wirksam sind, und anhand einer Folgenabschätzung die Risiken von Verstößen abschätzen und seine Maßnahmen laufend anpassen. Datenschutz ist also ein fortdauernder Prozess. Durch die neuen Prinzipien des Privacy by Design und Privacy by Default (Art. 25 DSGVO) ist der Datenschutz bereits bei der Entwicklung von neuen Technologien zu berücksichtigen. Zudem müssen Verantwortliche online sowie offline für datenschutzfreundliche Voreinstellungen sorgen, damit der Betroffene datenschutzfreundliche Einstellungen nicht selbst vornehmen muss. Besonders gravierend sind die hohen Bußgelder von bis zu 20 Millionen Euro oder vier Prozent des weltweiten Jahresumsatzes, je nachdem, welcher Betrag höher ist. Damit gilt mit der DSGVO nun auch für Großkonzerne ein äußerst empfindlicher Bußgeldrahmen.

Hinweispflichten gegenüber Mandanten

Gemäß Art. 13 DSGVO ist jeder Mandant beim erstmaligen Erheben seiner personenbezogenen Daten – also bei erstmaliger Mandatsaufnahme – unter anderem darauf hinzuweisen, zu welchem Zweck welche Kategorien personenbezogener Daten erhoben werden, auf welcher Rechtsgrundlage die Datenverarbeitung erfolgt und vor allem, welche Rechte der Mandant im Hinblick auf seine Daten hat. Zu empfehlen ist hier ein sorgfältig erarbeitetes Hinweisblatt, das dem Mandanten bei Unterzeichnung der Mandatsunterlagen zur Kenntnisnahme ausgehändigt wird – selbstverständlich können die Datenschutzhinweise dem Mandanten auch vorab per E-Mail übermittelt werden. Gleiches gilt aber auch für eigene Mitarbeiter und externe Dienstleister, deren personenbezogene Daten die Kanzlei verarbeitet. Auch beim Aufruf der Kanzlei-Webseite – dem Aushängeschild – werden personenbezogene Daten des jeweiligen Besuchs verarbeitet, was zu eben genannten Hinweispflichten führt. Webseiten sind besonders anfällig für Abmahnungen, da sie für jedermann einsehbar sind. Man sollte daher ein besonderes Augenmerk auf die Datenschutzhinweise legen.

Webseiten sind besonders anfällig für Abmahnungen, da sie für jedermann einsehbar sind.

Technisch-organisatorische Maßnahmen

Auch kanzleiintern gilt es, den Datenschutz auf allen Ebenen umzusetzen. Art. 32 DSGVO zwingt jeden Verantwortlichen, den Schutz personenbezogener Daten durch technische und organisatorische Maßnahmen (TOM) sicherzustellen. Daher müssen auch innerhalb der Kanzlei Maßnahmen getroffen werden, die eine unrechtmäßige Datenverarbeitung verhindern. Eine Selbstverständlichkeit ist, dass die Kanzleiräume zu keiner Zeit von Unbefugten betreten werden können. Akten dürfen im Publikumsbereich nicht frei herumliegen. Die Kanzlei hat stets den vollständigen Überblick über sämtliche Schlüssel und Schlüsselkarten zu behalten. Aber auch innerhalb der Räume ist zu gewährleisten, dass nur diejenigen Zutritt zu vertraulichen Daten haben, die dazu befugt sind, zum Beispiel im Server-Raum oder in der Buchhaltung. Um die IT-Sicherheit zu gewährleisten, sind alle Daten nach dem aktuellen Stand der Technik gegen unbefugten Zugriff zu sichern, etwa durch Passwortschutz, Verschlüsselung oder Firewall. Hierbei muss die Kanzlei ihren IT-Dienstleister verpflichten, für die entsprechende Umsetzung der technischen Anforderungen zu sorgen und das auch zu dokumentieren. Damit diese Maßnahmen nicht nur auf dem Papier stehen, müssen alle Angestellten der Kanzlei über die sie betreffende Datenverarbeitung informiert und vertraglich zur

Beachtung der geltenden Datenschutzgesetze verpflichtet werden, etwa im Arbeitsvertrag oder per Dienstanweisung. Kritisch zu bewerten ist insbesondere die Nutzung von privaten Mobiltelefonen zu betrieblichen Zwecken, wenn sich darauf Dienste wie WhatsApp befinden, die auf die Kontaktdaten von Mandanten zugreifen und diese Daten ins Ausland übermitteln.

Löschkonzept und Notfallplan

Ferner muss die Kanzlei ein Löschkonzept erarbeiten, das gewährleistet, dass personenbezogene Daten regelmäßig daraufhin überprüft werden, ob sie noch benötigt werden. Ist Letzteres nicht der Fall, fehlt es an einer Rechtsgrundlage und die Daten sind zu löschen. Auch andere im Unternehmen tätige Personen, wie zum Beispiel Hausmeister, Fensterputzer oder Reinigungspersonal, sind vertraglich zur Geheimhaltung zu verpflichten. Zudem ist zu gewährleisten, dass solche Personen keinen Zugriff auf vertrauliche Daten, wie etwa Akten oder Server-Raum haben. Auftragsverarbeiter – etwa IT-Firmen, Webhoster und andere – sind gemäß Art. 28 DSGVO vertraglich zur Einhaltung ihrer datenschutzrechtlichen Pflichten als Auftragsverarbeiter zu verpflichten. Für den Fall, dass trotz Beachtung der eben genannten Ausnahmen Daten unrechtmäßig verarbeitet werden, muss ein Notfallplan existieren, der gewährleistet, dass die Verletzung des Datenschutzes innerhalb von 72 Stunden an die entsprechende Aufsichtsbehörde gemeldet wird, wie es Art. 33 DSGVO vorschreibt.

Verträge mit Auftragsverarbeitern

Wie eingangs bereits erwähnt, betrifft die DSGVO auch Auftragsverarbeiter. Damit die Verantwortlichkeitskette lückenlos ist, muss der Verantwortliche – hier die Kanzlei – auch Dritte, die Daten in seinem Auftrag verarbeiten, vertraglich zur Einhaltung des Datenschutzes verpflichten. Verstößt der Auftragsverarbeiter gegen diese Pflichten, hat der Betroffene Ansprüche sowohl gegen den Verantwortlichen als auch gegen den Auftragsverarbeiter.

Benennung eines Datenschutzbeauftragten

Sofern der Verantwortliche nicht weniger als zehn Personen beschäftigt (dazu zählen auch Teilzeitbeschäftigte, freie Mitarbeiter oder Praktikanten), zwingen Art. 37 DSGVO und § 38 Bundesdatenschutzgesetz (BDSG) den Verantwortlichen regelmäßig zur Bestellung eines Datenschutzbeauftragten, also einer Person, die im Unternehmen weisungsfrei für die Einhaltung des Datenschutzes sorgt und die dafür notwendige Sachkompetenz mitbringt. Die Benennung des Datenschutzbeauftragten ist der Behörde unaufgefordert zu melden.

Verarbeitungsverzeichnis

Damit Aufsichtsbehörden bei Anfragen oder Meldungen schnell und einfach erkennen können, ob ein Steuerberater oder Rechtsanwalt datenschutzkonform agiert, zwingt Art. 30 DSGVO jeden Verantwortlichen, der nicht nur gelegentlich automatisiert personenbezogene Daten verarbeitet, zum Führen eines sogenannten Verarbeitungsverzeichnisses. Mit diesem Verzeichnis beschreibt jeder Verantwortliche tabellarisch, welche Kategorien personenbezogener Daten er verarbeitet, welche Kategorien an Personen von der jeweiligen Datenverarbeitung betroffen sind und welche technisch-organisatorischen Maßnahmen er zum Schutz personenbezogener Daten trifft. Die technischen Maßnahmen werden meist als Anlage beigefügt. Dieses Verzeichnis muss nahezu jeder Verantwortliche führen, weil eine automatisierte Datenverarbeitung bereits vorliegt, wenn manuell Daten in einen Computer eingetippt werden. Ein Muster für ein Verarbeitungsverzeichnis stellt beispielsweise der Deutsche Anwaltverein auf seiner Website zur Verfügung.

Beschränkte Befugnisse der Aufsichtsbehörden

Grundsätzlich haben Aufsichtsbehörden gemäß Art. 58 DSGVO sehr weitgehende Befugnisse, wie etwa Zugriff auf Informationen, Datenschutzprüfungen vor Ort einschließlich Zugang zu allen Informationen und Daten und Zutritt zu den jeweiligen Räumlichkeiten. Da es sich aber bei Rechtsanwälten und Steuerberatern um geheimhaltungspflichtige Personen handelt, die sich bei Verletzung ihrer Geheimhaltungspflichten gemäß § 203 Strafgesetzbuch (StGB) strafbar

machen würden, schränkt § 29 Abs. 3 BDSG die Befugnisse der Aufsichtsbehörden deutlich ein. Rechtsanwälte und Steuerberater müssen Aufsichtsbehörden keinen Zutritt zu den Kanzleiräumen und keinen Zugang zu mandatsbezogenen Daten oder Informationen, wie zum Beispiel Handakten, gewähren.

Beschränkung des Informationsanspruchs

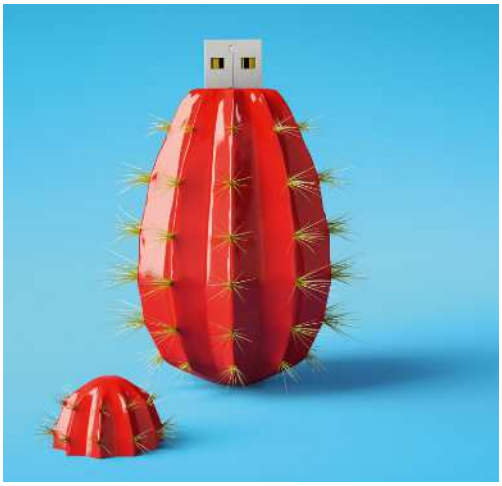
Zudem enthält Art. 14 Abs. 5d DSGVO für alle Berufsträger eine Ausnahme von der allgemeinen Pflicht, den Betroffenen vor Erhebung seiner personenbezogenen Daten auf die Datenverarbeitung hinzuweisen. Geheimhaltungspflichtige Berufsträger müssen einen Betroffenen, zum Beispiel einen Gegner, nicht darüber informieren, dass sie ihn betreffende personenbezogene Daten übermittelt bekommen haben. Das ist logisch, denn der Rechtsanwalt oder Steuerberater würde gegen seine Geheimhaltungspflichten verstoßen und sich gemäß § 203 StGB strafbar machen, wenn er den Dritten über die Aufnahme des Mandatsverhältnisses informiert, ohne dass der Mandant dem zustimmt. Aber auch der Mandant muss vor der Übermittlung personenbezogener Daten, die einen Dritten betreffen, zum Beispiel den Gegner oder Beteiligten eines Rechtsstreits, gemäß § 29 Abs. 2 BDSG nicht informieren. Denn die Erfüllung der Hinweispflichten könnte das Mandatsverhältnis sowie eine effektive Rechts- beziehungsweise Steuerberatung gefährden – der Mandant ist nicht verpflichtet, sein Mandatsverhältnis offenzulegen.

Beschränkung weiterer Betroffenenrechte

Auch weitere Rechte des Betroffenen sind eingeschränkt. Steuerberater und Rechtsanwälte sind gemäß § 29 Abs. 1 BDSG nicht verpflichtet, einer von der Datenverarbeitung betroffenen Person Auskunft gemäß Art. 15 DSGVO darüber zu erteilen, ob und gegebenenfalls welche personenbezogenen Daten sie im Rahmen des Mandatsverhältnisses zu dessen Person erhoben haben. Beschränkt wird ferner das Benachrichtigungsrecht nach Art. 34 DSGVO. Kommt es zu Datenschutzverstößen, müssen Betroffene wegen § 29 Abs. 1 Satz 3 DSGVO ausnahmsweise nicht darüber benachrichtigt werden, wie es an sich Art. 34 DSGVO vorsieht.

Wer hilft bei der Umsetzung in der Kanzlei?

Wichtige Schritte können Steuerberater und Rechtsanwälte –vor allem im Fall von kleineren Kanzleien – zunächst selbst erledigen. So können sie selbstständig ihren Datenschutzbeauftragten benennen und die ihnen obliegenden Hinweispflichten gegenüber den Betroffenen erfüllen. Muster finden sich im Netz zuhauf. Das Anlegen des Verarbeitungsverzeichnisses ist schon etwas aufwendiger, aber unerlässlich. Bei den technisch-organisatorischen Maßnahmen hilft zumeist der IT-Dienstleister. Externe Dienstleister stellen in der Regel selbst Verträge zur Auftragsverarbeitung bereit. Größere Unternehmen tun gut daran, einen externen Datenschutzbeauftragten zu verpflichten, der die notwendige Expertise hat, ein unternehmensinternes Audit durchzuführen, um die Schwachstellen (Gap) festzustellen und diese zu schließen. Ebenso können auf Datenschutz spezialisierte Rechtsanwälte weiterhelfen.



Fotos: Marcin Jastrzebski / Getty Images

MEHR DAZU

Alle Wissensangebote zur DSGVO finden Sie unter www.datev.de/dsgvo-weiterbildung