Praxistipps IT

Datenschutz in der Praxis

Umsetzung der EU-DSGVO für WP und StB

Rouven Friederich / Andreas Schneider

IDW

1 Einleitung

In einer Steuerberatungskanzlei bzw. einer Wirtschaftsprüferpraxis existieren verschiedene Prozesse, bei denen schützenswerte Daten durch die jeweiligen Mitarbeiter bearbeitet werden.

Datenschutz ist heute zunehmend mehr ein Thema für jedermann: Ob Alexa, Google-Standortdienste oder Smartwatches. Daten werden für uns Menschen in einer häufig nicht mehr nach zu vollziehenden Art und Weise gespeichert, verarbeitet und ausgewertet. Wissen Sie, wo genau Ihre Daten gespeichert werden? Die Antwort darauf lautet häufig genug „Im Internet", jedoch auch in einer Vielzahl von Fällen auf den Servern von Unternehmen und Institutionen. Über die Verarbeitung der Daten wissen Endnutzer, wobei dieser Begriff sowohl natürliche Personen als auch Unternehmen umfasst, zumeist noch weniger. Was genau geschieht mit den Daten? Welche Schlüsse und Profile werden daraus gezogen?

Sicherlich ist einer der wesentlichen Ziele der Datenverarbeitung einiger Unternehmen die Personalisierung von Werbeangeboten. Jeder von uns kennt das sicherlich: Nach dem Suchen eines Produkts im Internet werden anschließend auf beliebigen anderen Internetseiten ähnliche oder vergleichbare Produkte angeboten. Der Nutzer wundert sich, woher denn nun diese neu aufgerufene Seite nun „weiß", warum genau das Produkt, welches man Tage zuvor über eine Suchmaschine gesucht und gefunden hatte, nun für Wochen oder sogar Monate auf anderen Internetseiten beworben wird.

Allen Themen ist dabei gemeinsam, dass es den Endnutzern häufig nicht möglich ist, zu erkennen, was genau mit den von Ihnen freiwillig zur Verfügung gestellten Daten gemacht wird. Wobei die Freiwilligkeit in diesem Kontext regelmäßig eher eine Freiwilligkeit der Art „wenn man nicht zustimmt, ist die Funktion nicht möglich" ist.

Ihnen als Leser werden sicherlich gerade weitere Beispiele für die digitale Personalisierung einfallen. Allen gemeinsam ist der überwiegend private Bereich („B2C") der Dateneingabe, Datennutzung und -verarbeitung.

Doch auch im geschäftlichen Umfeld („B2B“) von Kanzleien, Steuerberaterkanzleien wie Wirtschaftsprüfungspraxen, werden Daten ausgewertet und bearbeitet: Bei der Verbuchung von Geschäftsvorfällen mittels OCR-Texterkennung „lernt“ das Programm und erleichtert damit dem Buchhalter die Verarbeitung von Massenbelegen. Es handelt sich hier um einen ausgewählten Bereich der Datensammlung und -verarbeitung innerhalb von Kanzleien, der von vielen als „Digitalisierung“ bezeichnet wird.

Digitalisierung wird heute als Synonym für Effizienzsteigerung, zuhause oder am Arbeitsplatz verwendet und kann unseres Erachtens auch durchaus so betrachtet werden.

Allerdings kommt es wie bei allen Dingen darauf an, wie man sie verwendet. Werkzeuge können als solche, aber auch völlig anders zum Einsatz kommen und nicht alle Erfindungen der Menschheit, welche ursprünglich für mehr für Effizienzsteigerung gedacht waren, werden letztendlich auch so eingesetzt.

Diese Änderung des Einsatzes von Werkzeugen kann versehentlich oder auch absichtlich vorgenommen werden und auch im Zeitablauf werden sich Ansichten über den Einsatzzweck verändern.

Zu einem nicht fehlinterpretierten Einsatz von Werkzeugen bedarf es eines Regelungswerks, welches der Gesetzgeber mit dem neuen Bundesdatenschutzgesetz ins Leben gerufen hat.

Das Bundesdatenschutzgesetz bezweckt den Schutz der Person, deren Daten verarbeitet werden. Damit zielt der Gesetzgeber selbstverständlich nicht darauf ab, die Daten an sich selbst zu schützen, sondern vielmehr den Umgang mit personenbezogenen Daten zu regeln.

Es regelt zusammen mit den Datenschutzgesetzen der Länder und anderen bereichsspezifischen Regelungen den Umgang mit personenbezogenen Daten, die in Informations- und Kommunikationssystemen oder manuell verarbeitet werden.

In Deutschland ist der Datenschutz bereits seit vielen Jahren etabliert und im Grundgesetz auch mit dem Recht auf informelle Selbstbestimmung verankert. Andere europäische Staaten kannten keine vergleichbaren datenschutzrechtlichen Vorschriften und haben auch die

sogenannte EU-Datenschutzgrundverordnung bisher nur in Teilen in nationales Recht umgesetzt.[1]

Während Deutschland die EU-Datenschutzgrundverordnung (DSGVO) mit dem Datenschutz-Anpassungs- und -Umsetzungsgesetz EU v. 30.06.2017 (BGBl. I S. 2097) und das Gesetz zur Änderung des Bundesversorgungsgesetzes und anderer Vorschriften vom 17.07.2017 (BGBl. I S. 2541) in das Bundesdatenschutzgesetz (BDSG) umgesetzt hat, haben andere europäische Länder dies bisher noch nicht getan. Dennoch gilt die neue EU-Datenschutzgrundverordnung unmittelbar in allen Mitgliedsstaaten der Europäischen Union ab dem 25.05.2018.

Hintergrund dafür ist, dass gerade europarechtliche Vorschriften nun einheitlich und allgemein in allen Mitgliedsländern Anwendung finden und ein Anwendungsvorrang des europäischen Rechts vor dem nationalen Recht besteht.

Der deutsche Gesetzgeber stand damit unter anderem vor der Herausforderung gerade im Bereich der berufsrechtlichen Vorschriften für Steuerberater und Wirtschaftsprüfer zur Verschwiegenheit Regelungen zu erarbeiten, die im Rahmen der Mitgliedstaatenwahlrechte Anwendung finden dürfen.

Ihrem Charakter als Grundverordnung folgend, enthält die DSGVO konkrete, an die Mitgliedstaaten gerichtete Regelungsaufträge sowie eine doch gewisse Anzahl Öffnungsklauseln für den nationalen Gesetzgeber. Damit sollen insbesondere die Regelungen des Steuerberatungsgesetzes (StBerG), aber auch der Wirtschaftsprüferordnung (WPO) neben dem BDSG auch weiterhin Bestand besitzen.

Ziel der DSGVO ist ein gleichwertiges Schutzniveau für die Rechte und Freiheiten von natürlichen Personen bei der Verarbeitung von Daten in allen Mitgliedstaaten.

Die DSGVO ist die bedeutendste Datenschutz-Vorschrift in Europa seit dem Jahr 1995. Nach einer zweijährigen Übergangsphase löst die DSGVO nunmehr die veraltete EU-Datenschutz-Richtlinie und in weiten Teilen einzelstaatliche Datenschutzgesetze ab. Im Gegensatz zu einer

[1] Endspurt für Vorbereitung auf neue Datenschutzregeln, NWB Nr. 6 vom 05.02.2018 Seite 323

Richtlinie gilt eine Verordnung in allen Mitgliedsstaaten der EU unmittelbar, ohne dass es nationalstaatlicher Regelungen bedarf. Insofern wurde mit der DSGVO ein EU-weit einheitliches Regelwerk zum Datenschutz geschaffen.

2 Prozesse in Steuerberatungskanzleien und Wirtschaftsprüferpraxen

Wird eine Institution mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beauftragt, ist der Auftraggeber für die Einhaltung der Vorschriften des BDSG verantwortlich (§ 11 Abs. 1 BDSG).

Der Auftraggeber ist verpflichtet, den Auftragnehmer sorgfältig auszuwählen und in der schriftlichen Beauftragung bestimmte Inhalte zu vereinbaren, um den Datenschutz zu genügen.

Der Auftraggeber besitzt drüber hinaus Kontrollpflichten und Rechte, die beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überprüfen.

Zur Sicherstellung der Einhaltung der Rechte und Pflichten des DSGVO bzw. des BDSG ist eine persönliche Inaugenscheinnahme nicht erforderlich, sofern die Überzeugung auf andere Weise gebildet werden kann, zum Beispiel durch Vorlage eines Testats oder einer Zertifizierung. Häufig wird dies in der Praxis mit sogenannte Auftragsverarbeitungsverträgen umgesetzt.

Steuerberater und Wirtschaftsprüfer werden aktuell zunehmend auch mit Auftragsverarbeitungsverträgen konfrontiert: Dienstleister, z.B. auch die DATEV, oder Mandanten verlangen von der Kanzlei diese schriftlichen Vereinbarungen.

Während Dienstleister der Kanzlei grundsätzlich Auftragsverarbeiter im Sinne der DSGVO bzw. des BDSG sein können, hatte sich in der Vergangenheit noch eine Unsicherheit dahingehend ergeben, ob die Kanzlei, beispielsweise im Rahmen der Erbringung von Dienstleistungen in Form von Lohn- und Gehaltsabrechnungen selbst Auftragsverarbeiter sein kann.

Ob ein solches Vertragsverhältnis zwischen Mandant und Steuerberater eine Auftragsverarbeitung darstellt, hat die Bundessteuerberaterkammer mittlerweile beantwortet.

Sie hat klargestellt, dass die Kanzlei kein Auftragsdatenverarbeiter sein kann, da dies die freiberufliche, eigenverantwortliche Tätigkeit nicht zulässt.

§ 11 BDSG in der Fassung bis zum 25.05.2018 schrieb für die Auftragsdatenverarbeitung eine Weisungsgebundenheit vor. Auch die neuen Regelungen sehen dies unverändert vor. In dem am 16.01.2018 Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) werden ebenso die Eigenverantwortlichkeit und Weisungsgebundenheit als Entscheidungskriterium herangezogen.[2]

Die berufsrechtlichen Vorschriften lassen allerdings eine Weisungsgebundenheit des Steuerberaters bzw. Wirtschaftsprüfers nicht zu, da beide Berufsgruppen eigenverantwortlich und selbständige ihre Tätigkeiten ausführen müssen.

Praxistipp:
Während die Kanzlei selbst kein Auftragsverarbeiter im Sinne des Datenschutzes sein kann, da dies den berufsrechtlichen Vorschriften wiedersprechen würde, sind z.B. IT-Dienstleister (DATEV eG, u.a.) stets Auftragsverarbeiter der Kanzlei.

Unabhängig davon finden die Regelungen des BDSG jedoch auch für eine Steuerberatungskanzlei oder eine Wirtschaftsprüferpraxis Anwendung. Damit sind einerseits die Unterstützungsprozesse der Kanzleiorganisation, andererseits die Leistungsprozesse zur Erbringung der steuerberatenden oder wirtschaftsprüfenden Tätigkeiten zu betrachten.

Die Unterstützungsprozesse stellen diejenigen Tätigkeiten dar, welche für die Praxisorganisation notwendig sind, u.a. handelt es sich dabei um die kanzleiinternen Prozesse zum Umgang mit Dienstleistern, Mitarbeitern, der internen Buchhaltung oder der Rechnungsschreibung.

Die Leistungsprozesse umfassen alle Tätigkeiten im Zusammenhang mit den Mandatsbeziehungen, u.a. die Lohn- und Gehaltsabrechnung, die Finanzbuchhaltung oder die Erstellung und Prüfung von Jahresabschlüssen.

[2] vgl. https://www.lda.bayern.de/media/dsk_kpnr_13_auftragsverarbeitung.pdf (zuletzt abgerufen am 28.05.18)

2.1 Dienstleister der Kanzlei

Die Steuerberatungskanzlei bzw. die Wirtschaftsprüferpraxis sind häufig nicht nur Verantwortlicher für die Datenverarbeitung, sondern lagern auch Leistungen an andere Dienstleister aus. Hier handelt es sich auf fachlicher Ebene um andere Steuerberater/Wirtschaftsprüfer oder freiberuflich tätige Mitarbeiter.

Es handelt sich hierbei aus berufsrechtlicher Perspektive um eine Auslagerung im Sinne des Standards des IDW PS 951 „Die Prüfung des internen Kontrollsystems bei Dienstleistungsunternehmen". Nach IDW PS 951 n.F. müssen Dienstleistungsunternehmen, welche Teile der Prozesse und Funktionen an Subdienstleister auslagern, dies in der Beschreibung des dienstleistungsbezogenen internen Kontrollsystems transparent darstellen.

In jedem Fall hat das auslagernde Unternehmen im Hinblick auf den Datenschutz sicher zu stellen, dass auch der Dienstleister seinen datenschutzrechtlichen Vorschriften nachkommt und muss dies damit in seiner eigenen Dokumentation berücksichtigen.

Damit sind insbesondere im Hinblick auf die berufsrechtlichen Vorschriften im Rahmen der prozessunabhängigen und prozessintegrierten Überwachungsmaßnahmen des Dienstleisters jedoch die Einhaltung der datenschutzrechtlichen Vorschriften zu kontrollieren.

Praxistipp:
Umgangssprachlich sind die Kontrollen die einzelnen Bestandteile des internen Kontrollsystems. Dieser Begriff ist jedoch nicht mit einer ausgefüllten Checkliste oder einem Papier gleichzusetzen. Vielmehr kann man hierunter auch eine „Maßnahme" verstehen. Diese soll die Frage beantworten: „Wie ist es sicher zu stellen, dass etwas eingehalten wird bzw. nicht passiert"?[3]

Verarbeitet der Dienstleister, sofern er kein Steuerberater ist, personenbezogene Daten im Sinne von § 62 BDSG, ist eine Vereinbarung zur Auftragsverarbeitung abzuschließen.

[3] Vgl. Tritschler/Lamm, Jahresabschlussprüfung bei Outsourcing und Cloud-Computing, S. 58

Da eine Steuerberatungskanzlei bzw. die Wirtschaftsprüferpraxis *kein* Auftragsverarbeiter sein kann, ist hier für Subdienstleister, welche ebenso Steuerberater/Steuerberatungskanzleien bzw. die Wirtschaftsprüferpraxen sind, eine solche Vereinbarung nicht notwendig.

Hinweis:
Im Ergebnis sind somit bei der der Auslagerung von Dienstleistungen „auf fachlicher Ebene" sowohl die Vorgaben des IDW PS 951 n.F. als auch die datenschutzrechtlichen Aspekte zu berücksichtigen. Zwar liegt bei einer solchen Auslagerung keine Auftragsdatenverarbeitung vor, weil der Dienstleister ein Berufsangehöriger der steuerberatenden oder wirtschaftsprüfenden Berufe ist, jedoch gelten alle übrigen Vorschriften des BDSG sowie auch die Verlautbarungen des IDW im Hinblick auf Auslagerungen von Dienstleistungen.

2.2 BDSG oder DSGVO – Was gilt denn nun?

Offen ist damit die Frage, ob und welche Daten unter die Neuregelungen des BDSG fallen und wie bzw. ob diese Daten verarbeitet werden dürfen?

Natürlich stellt sich auch die Frage, welche Rolle die DSGVO spielt, welche nicht in allen Bereichen inhaltsgleich mit den neuen Vorschriften des BDSG ist.

Bisher regelte das deutsche Bundesdatenschutzgesetz („BDSG alt") die Rechte und Pflichten der Verantwortlichen bei sowie die Zulässigkeit der Erhebung, Verarbeitung, Nutzung und Speicherung personenbezogener Daten weitgehend abschließend.

Als Verordnung gilt die DSGVO in den EU-Staaten unmittelbar. Der Bundesgesetzgeber hat darüber hinaus das Bundesdatenschutzgesetz (BDSG) überarbeitet, um die Rechtslage in Deutschland, wo nötig, den Vorgaben der DSGVO anzupassen und um Freiräume zu nutzen, die die EU den Mitgliedstaaten in der DSGVO gelassen hat.

Im Zuge der Anpassung Rechts zum Datenschutz an die DSGVO wurde zunächst das BDSG nahezu vollständig gefasst.

Beide Regelungen, also das „BDSG neu" und die DSGVO sind am 25. Mai 2018 in Kraft getreten. Hier gilt, dass das BDSG selbstverständlich nur in Deutschland Anwendung findet, während die räumliche Geltung der DSGVO durch Artikel 3 DSGVO definiert wurde:

Artikel 3 DSGVO *Räumlicher Anwendungsbereich*

1. Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet.
2. Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht
   a. betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;
   b. das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.
3. Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen Verantwortlichen an einem Ort, der aufgrund Völkerrechts dem Recht eines Mitgliedstaats unterliegt.

Der räumliche Geltungsbereich ist damit im weitesten Sinne auf die Staaten der Europäischen Union beschränkt. Die aktuellen Mitglieder der EU sind auf der Internetseite der EU veröffentlicht.[4] Das Vereinigte Königreich bleibt rechtlich gesehen bis zum Abschluss der Austrittsverhandlungen Mitglied der Europäischen Union und zwar mit allen Rechten und Pflichten, die sich daraus ableiten. Damit gilt die DSGVO bis zu diesem Zeitpunkt auch dort.

Zwar gilt eine EU-Verordnung ab ihrer Wirksamkeit unmittelbar, in der DSGVO hat der europäische Gesetzgeber allerdings einige sogenannte Öffnungsklauseln vorgesehen. Damit sollen die einzelnen EU-Mitgliedsstaaten die Möglichkeit erhalten, bestimmte Bereiche abweichend von der DSGVO oder ergänzend dazu zu regeln. Diese ergänzenden Regelungen dürfen aber wiederum nicht im Widerspruch zur DSGVO (und anderen EU-Vorschriften) stehen.

[4] Vgl. https://europa.eu/european-union/about-eu/countries_de (zuletzt abgerufen am 28.05.18)

Weil die DSGVO innerhalb ihres Geltungsbereichs Anwendungsvorrang genießt, ist anzunehmen, dass maßgebliche Abschnitte des BDSG ihren Geltungsanspruch zugunsten der reformierten Bestimmungen aufgeben müssen. Auf dem Gebiet des BDSG wird in Zukunft also grundsätzlich von einer vorrangigen Geltung der neuen Grundverordnung auszugehen sein.

Hinweis:
Sofern eine Regelung in dem BDSG nicht oder nicht in vollem Umfang vorhanden ist, greift die DSGVO.

Die DSGVO stellt das Rahmenwerk dar. Die nationalen Regelungen des BDSG dürfen hierzu nicht im Widerspruch stehen.

Im Hinblick auf die Konkurrenz der Regelungen des BDSG zu anderen gesetzlichen Vorschriften regelt das BDSG grundsätzlich, dass andere spezialgesetzliche Vorschriften dem BDSG vorgehen, allerdings dann das BDSG Anwendung findet, wenn diese Gesetze Sachverhalte nicht oder nicht vollständig regeln.

§ 1 Abs. 2 BDSG

Andere Rechtsvorschriften des Bundes über den Datenschutz gehen den Vorschriften dieses Gesetzes vor. Regeln sie einen Sachverhalt, für den dieses Gesetz gilt, nicht oder nicht abschließend, finden die Vorschriften dieses Gesetzes Anwendung. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

2.3 Auftragsannahme

2.3.1 Rechtmäßigkeit der Verarbeitung

Die Auftragsannahme bei Steuerberatungskanzleien orientiert sich an den Vorschriften der BStBK[5] und soll grundsätzlich schriftlich erfolgen. Vergleichbare Regelungen finden sich für Wirtschaftsprüfer im Gesetz sowie den berufsständischen Vorschriften (u.a. des IDW[6]).

[5] Vgl. www.bstbk.de (zuletzt abgerufen am 28.05.18)
[6] Vgl. www.idw.de (zuletzt abgerufen am 28.05.18)