THOMAS MÜTHLEIN UND JÜRGEN HUND

Neues Bundesdatenschutzgesetz

Was muss der Kanzleiinhaber beachten?

Am 23. Mai 2001 ist das neue Bundesdatenschutzgesetz (BDSG) in Kraft getreten. Die Novelle passt das BDSG an die EU-Datenschutzrichtlinie an, um die europäischen Gesetzgebungen zu harmonisieren. Der Beitrag beschreibt die wesentlichen Änderungen und zeigt in Grundzügen zusammenfassend auf, welche Datenschutz-Anforderungen unter Berücksichtigung dieser Änderungen in der Kanzlei zu beachten sind.

Neben der Anpassung des BDSG an die EU-Datenschutzrichtlinie hat der Gesetzgeber in Ansätzen den Forderungen Rechnung getragen, eine Allianz zwischen Datenschutz und Technik - einen unmittelbar an der Technik orientierten Datenschutz - zu schaffen. Die technische Ausgestaltung der Verarbeitungssysteme soll den *Grundsatz der Datenvermeidung* mit den Möglichkeiten *anonymer und pseudonymer Nutzung* berücksichtigen - Datenvermeidung und Datensparsamkeit werden groß geschrieben. Hinzu kommen Regelungen, die den Einsatz von bestimmten Techniken wie Videoüberwachung, Verarbeitung personenbezogener Daten auf Chipkarten oder bei automatisierten Einzelentscheidungen transparenter machen sollen.

Vor allem die Privatwirtschaft treffen die Änderungen, die entsprechende Anpassungs- und Umstellungsmaßnahmen zwingend erforderlich machen. Dies betrifft *Steuerberater, Wirtschaftsprüfer oder Anwälte in ihren* Kanzleien sowohl in der Rolle als Berater im Verhältnis zu den Mandanten als auch in ihrer Funktion als Arbeitgeber beim Umgang mit Personaldaten und den allgemeinen datenschutzrechtlichen Organisationspflichten.

Neuregelungen

Anwendungsbereich

Wesentliches Anliegen der mit der Novelle umgesetzten EU-Datenschutzrichtlinie war, sicherzustellen, dass Datenverarbeitung und Datenaustausch im EU-Raum über die Mitgliedstaaten hinaus nicht auf Grund unterschiedlicher Datenschutzregelungen der einzelnen Mitgliedstaaten behindert werden. Daher ist jetzt der Umgang mit personenbezogenen Daten innerhalb der EU und des Europäischen Wirtschaftsraums – vorbehaltlich des *Sitzlandsprinzips* – einheitlich zu betrachten (§ 1 Abs. 5 BDSG). Das bedeutet, dass Daten grundsätzlich nach dem Datenschutz, des für den Sitz der verantwortlichen Stellen, erhoben, verarbeitet oder genutzt werden müssen. So gilt zum Beispiel deutsches Datenschutzrecht für Erhebungen einer deutschen Kanzlei in Frankreich, soweit die Daten nicht durch die dortige Niederlassung erhoben werden.
Der sachliche Anwendungsbereich des BDSG wurde insbesondere für die Privatwirtschaft erweitert. Jetzt wird jede Verarbeitung personenbezogener Daten (§ 1 Abs. 2 Nr. 3 BDSG) mit *Datenverarbeitungsanlagen* erfasst; bisher bestehende Ausnahmeregelungen für nichtautomatisierte Dateien (für nur intern genutzte Karteien waren lediglich die Vorschriften zur Wahrung des Datengeheimnisses und der Datensicherheit zu beachten) sind weitgehend entfallen. Durch die Neufassung wird auch verdeutlicht, dass zum Beispiel elektronische Akten ebenso in vollem Umfang unter die Regelungen des BDSG fallen wie die auf einem elektronischen Terminkalender gespeicherten dienstlichen „Notizen“.

Einbeziehung der Erhebungsphase

Der dem Verbot mit Erlaubnisvorbehalt unterworfene „Umgang“ mit personenbezogenen Daten wird um die Phase der *Erhebung* erweitert (§ 4 Abs. 1 BDSG). Dabei werden gleichzeitig die Zulässigkeitskriterien für eine Erhebung ohne Mitwirkung des Betroffenen präzisiert (§ 4 Abs. 2 BDSG): Grundsätzlich ist bei Erhebungen der „*Grundsatz der Direkterhebung“* zu beachten. Hieraus können sich im Bereich der Kanzleien von Steuerberatern, Wirtschaftsprüfern, Rechtsanwälten insbesondere im Arbeitsverhältnis der eigenen Mitarbeiter Konsequenzen ergeben. So werden beispielsweise bei so genannten Arbeitgeberauskünften neue Grenzen zu ziehen sein.

Zugleich ist mit dem „Grundsatz der Direkterhebung“ eine Vorverlagerung der *Benachrichtigungspflicht* verbunden. Die verantwortliche Stelle muss bei Datenerhebungen beim Betroffenen ihre Identität, Zweck der Erhebung und nachfolgender Verarbeitungen und die Kategorien von nicht „üblichen“ Empfängern nennen (§ 4 Abs. 3 Satz 1 BDSG). Zwar entfällt die Informationspflicht, wenn der Betroffene schon auf andere Weise Kenntnis erlangt hat, was jedoch bei der Erhebung von Mandanten-, Bewerber- oder Arbeitnehmerdaten nicht immer und nicht für alle Aspekte der Information zutreffen muss. Hinsichtlich der Pflicht nach § 4 Abs. 3 Satz 1 Nr. 3 BDSG (sofern der Betroffene im Einzelfall nicht mit der Weitergabe an diese rechnen muss, sind die Kategorien von Empfängern der Daten zu benennen) wird eine Informationspflicht zum Beispiel für die Weitergabe von Daten im Rahmen einer Auftragsdatenverarbeitung an ein Dienstleistungsrechenzentrum - wie es beispielsweise die DATEV betreibt – zu überprüfen sein. Ferner ist unter anderem darauf hinzuweisen, wenn bzw. ob eine Verpflichtung zur Erteilung der Auskunft besteht.
Zudem müssen die *konkreten Verarbeitungszwecke* bereits zum Zeitpunkt der Erhebung festgelegt sein.
Im Hinblick auf diese Informationspflichten sollten in der Kanzlei zu eigenen Zwecken genutzte Erhebungsbögen und Verträge überprüft und angepasst werden.

Übermittlung personenbezogener Daten ins Ausland

Das BDSG enthält detaillierte Regelungen zur Übermittlung personenbezogener Daten ins Ausland.
Dem Ziel der EU-Richtlinie entsprechend sind *Datenübermittlungen in Staaten der Europäischen Union und des Europäischen Wirtschaftsraumes* so zu behandeln wie derartige Verarbeitungsschritte zwischen inländischen Stellen (§ 4 b Abs. 1 BDSG).

In sonstige Staaten - so genannte *Drittländer* - dürfen Daten nur transferiert werden, wenn in dem Drittland ein dem BDSG entsprechendes Datenschutzniveau besteht oder gewährleistet wird oder entsprechende Übermittlungsbefugnisse nach § 4c BDSG vorliegen. Das beurteilt die übermittelnde Stelle zwar selbst, muss sie jedoch gegebenenfalls durch die Aufsichtsbehörden genehmigen lassen. Die EU-Kommission kann die Angemessenheit des Schutzniveaus auch allgemein feststellen, wie sie dies bereits für die Schweiz und Ungarn getan hat.

Allgemeines Widerspruchsrecht

Dem Betroffenen wird erstmals ausdrücklich ein *allgemeines Widerspruchsrecht* gegenüber den ihn betreffenden Datenverarbeitungen eingeräumt (§ 35 Abs. 5 BDSG). Das greift aber nur dann, wenn er darlegen kann, dass auf Grund - der verantwortlichen Stelle bislang nicht bekannter - konkreter persönlicher Umstände seinem Schutzinteresse Vorrang einzuräumen ist und keine Rechtsvorschrift zur Erhebung, Verarbeitung oder Nutzung verpflichtet.

Möglich ist die Berufung auf dieses Widerspruchsrecht theoretisch zwar sowohl im Mandanten- wie auch im Arbeitsverhältnis, allerdings wird diese Regelung auf Grund ihres extremen Ausnahmecharakters in den Kanzleien kaum praktische Bedeutung erlangen.

Beschränkung des Umgangs mit „besonderen Arten personenbezogener Daten“

„Besondere Arten personenbezogener Daten“ (§ 3 Abs. 9 BDSG), wie rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugung, Daten zur Gewerkschaftszugehörigkeit oder zum Sexualleben, dürfen nur noch unter ganz bestimmten Voraussetzungen erhoben und verarbeitet werden: Entweder es gibt eine besondere Gesetzesgrundlage, wie das Sozialgesetzbuch, der Betroffene willigt ein – hier sind die besonderen Formvorschriften des § 4a Abs. 3 BDSG zu beachten - oder es liegt eine besondere Erlaubnis des BDSG vor (§ 28 Abs. 6 bis 9 BDSG).

Meldepflicht, Datenschutzbeauftragter und Vorabkontrolle

Das BDSG legt die grundsätzliche *Meldepflicht* gegenüber der Aufsichtsbehörde fest (§§ 4d, 4e BDSG). In der Praxis allerdings kommt diese Meldepflicht kaum zum Tragen. Denn von einer umfassenden Meldung kann grundsätzlich dann abgesehen werden, wenn ein betrieblicher Datenschutzbeauftragter bestellt ist oder - bei weniger als fünf beschäftigten Mitarbeitern - die Einwilligung des Betroffenen vorliegt oder die Bearbeitung der Daten der Zweckbestimmung eines Vertrages mit dem Betroffenen dient. Ansonsten sind unter anderem meldepflichtig: Zweckbestimmung der Datenerhebung, -verarbeitung und -nutzung, eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien, aber auch Empfänger oder Kategorien von Empfängern, denen Daten mitgeteilt werden können. Ist ein betrieblicher Datenschutzbeauftragter bestellt, ist ihm die Führung des nunmehr von jedermann einsehbaren Verfahrensverzeichnisses zugewiesen. *Ein Datenschutzbeauftragter* kann in kleinen Kanzleien auch auf freiwilliger Basis bestellt werden. Die Bestellung ist obligatorisch bei Vorabkontrolle (siehe unten) oder wenn mindestens fünf Mitarbeiter beim Umgang mit personenbezogenen Daten in automatisierten Verarbeitungen beschäftigt werden.
Das BDSG setzt damit - auch zur Entlastung der staatlichen Aufsichtsbehörden von ansonsten wahrzunehmenden Meldefunktionen - weiterhin auf das Primat der betrieblichen Selbstkontrolle durch interne Datenschutzbeauftragte. Deren Rechtsstellung und Aufgaben sind nunmehr im allgemeinen Teil des Gesetzes dargestellt (§§ 4f und 4g BDSG).
Als neue Aufgabe wurde dem Datenschutzbeauftragten neben der Führung des Verfahrensverzeichnisses die so genannte *Vorabkontrolle* bei besonders risikoreichen Verarbeitungen zugewiesen.
Bei der Vorabkontrolle hat der Datenschutzbeauftragte eine Risikoabwägung vorzunehmen, bevor die Daten verarbeitet werden dürfen. Sie ist insbesondere dann erforderlich, wenn besondere Arten personenbezogener Daten im Sinne des § 3 Abs. 9 BDSG) verarbeitet werden oder die Verarbeitung personenbezogener Daten dazu bestimmt ist, die Persönlichkeit des Betroffenen zu bewerten (Leistungs- und Verhaltensanalysen und -kontrollen, Profilabgleiche). Zu der Vorabkontrolle zählen Planung, Gefahrenanalyse, Risikoanalyse und ein Sicherheitskonzept, die entweder durch die verantwortliche Stelle für den oder durch den Datenschutzbeauftragten zu vollziehen sind.
Die Verpflichtung zur Durchführung einer Vorabkontrolle trifft jedes Unternehmen, damit auch Kanzleien, unabhängig von seiner/ihrer Größe oder Mitarbeiterzahl. Das heißt, auch kleine Kanzleien sind zur Vorabkontrolle verpflichtet, sofern keine gesetzliche Verpflichtung oder die Einwilligung des Betroffenen vorliegt oder die Bearbeitung der Daten der Zweckbestimmung eines Vertrages mit dem Betroffenen dient. Das bedeutet aber auch, dass in diesem Fall unabhängig vom Vorliegen der sonstigen Voraussetzungen immer ein Datenschutzbeauftragter zu bestellen ist. Da ist es hilfreich, dass die Funktion des Datenschutzbeauftragten im Bedarfsfall auch „outgesourct“ und ein *externer Datenschutzbeauftragter* beauftragt werden kann (§ 4 f Abs. 2 BDSG).

Datenschutz-Audit

Mit dem neuen, auf freiwilliger Basis eingeführten *Datenschutz-Audit* für Betreiber und Provider als Daten verarbeitende Stellen sowie für Anbieter und Hersteller von IT-Produkten

verfolgt der Gesetzgeber das Ziel, datenschutz-freundliche Produkte auf dem Markt zu fördern und die Datenschutz-Qualität bei den verantwortlichen Stellen als permanenten Prozess zu stimulieren.
So können zum Beispiel Anbieter von Standardsoftwaresystemen, -Programmen, Provider und externe Dienstleister ihr zertifiziertes Datenschutzkonzept und ihre technische Einrichtung Kunden, Datenschutzverantwortlichen, dem IT- und Personalmanagement anbieten und zu einem Auswahlkriterium werden lassen, wie es beispielsweise bereits von der Systemprüfung zum DEÜV-Meldeverfahren her bekannt ist.
Näheres hierzu soll durch ein besonderes Gesetz geregelt werden.

Datenschutzkontrolle durch Aufsichtsbehörden

Das BDSG erweitert vor allem die Befugnisse der *Aufsichtsbehörden* und stärkt ihre Unabhängigkeit.
Hierzu zählt, dass nunmehr generell von Amts wegen beaufsichtigt wird und Daten verarbeitende Stellen - zu denen auch die Kanzleien zählen – jederzeit kontrolliert werden können. Es bedarf also *keines konkreten Anlasses* mehr, um zu überprüfen, ob eine Kanzlei oder ein Unternehmen mit Daten entsprechend den Vorschriften des BDSG umgeht. Gerade hier haben die Aufsichtsbehörden angekündigt, aktiver zu werden.

Sanktionen

Die Aufsichtsbehörden können nun *Zwangsgelder* verhängen, *Bußgeldverfahren* einleiten und *Strafantrag* stellen.
Dabei droht das BDSG bei einer erheblichen Erweiterung der Bußgeldtatbestände mit weitaus höheren Strafen als bisher. Das darf bei der Risikoeinschätzung nicht unberücksichtigt bleiben (§ 43 BDSG). Die Aufsichtsbehörden können bei materiellen Rechtsverstöße Geldbußen bis zu 250.000.- € verhängen. Im Bereich der Straftatbestände (§ 44 BDSG) drohen Gefängnisstrafen von bis zu zwei Jahren.
Zu erwähnen ist auch, dass nunmehr auch dem Arbeitgeber das Recht eingeräumt ist, strafbare Datenschutzverstöße von Beschäftigten durch Stellung eines Strafantrags verfolgen zulassen (§ 44 Abs. 2 Satz 2 BDSG).

Wesentliche neue Regelungen

- Datenvermeidung und Datensparsamkeit (§ 3 a)
- Grundsatz der Direkterhebung (§ 4)
- Übermittlung personenbezogener Daten ins Ausland (§§ 4 b und 4 c)
- Meldepflicht (§ 4 d)
- Vorabkontrolle (§ 4 e)
- Erweiterte Informationspflichten (§ 4 Abs. 3, § 33 Abs. 1, § 34)
- Regelungen für den Datenschutzbeauftragten (§ 4 f und § 49)
- Bestimmungen zur automatisierten Einzelentscheidung (§ 6 a)
- Videoüberwachung öffentlich zugänglicher Räume (§ 6b)
- Einsatz mobiler personenbezogener Speicher- und Verarbeitungsmedien (Chipkarten) (§ 6 c)
- Neue Vorgaben für technische und organisatorische Maßnahmen (§ 9)
- Datenschutzaudit (§ 9 a)
- Unterrichtungspflicht bei direkter Werbeansprache über die verantwortliche Stelle und über das Widerspruchsrecht (§ 28 Abs. 4)
- Umgang mit sensitiven Daten (§ 28 Abs. 6-9 i.V.m. § 3 Abs. 9)
- Allgemeines Widerspruchsrecht (§ 35 Abs. 5)
- Kontrolle durch Aufsichtsbehörden generell ohne Anlass möglich (§ 38)

Anforderungen des BDSG an die Kanzleien in der Gesamtbetrachtung

Anwendungsbereich

Das BDSG gilt im Privatbereich für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten unter Einsatz von Datenverarbeitungsanlagen oder mit Hilfe nicht-automatisierter Dateien (herkömmlicher Karteiverarbeitung). Akten und Aktensammlung fallen in der Regel nach wie vor nicht unter das BDSG. Zu den personenbezogenen Daten beim steuerlichen Berater gehören etwa Daten über Lieferanten, Kanzleiangestellte oder Mandanten, insbesondere jedoch auch die zur steuer-, wirtschafts- oder rechtsberatenden Tätigkeit verwendeten Mandantendaten.
Viele der kanzleiüblichen Tätigkeiten, vor allem am oder im Umfeld des PC – darunter nahezu alle DATEV-Anwendungen – fallen daher unter das BDSG oder müssen wegen anderer Rechtsvorschriften zum Datenschutz oder auch aus Eigeninteresse in gleicher Weise geschützt werden.
Zu den „anderen Rechtsvorschriften“ über den Datenschutz gehören etwa die Arbeitnehmerschutzgesetze, HGB, BGB, Betriebsvereinbarungen zum Datenschutz sowie insbesondere auch die einschlägigen berufsrechtlichen Vorschriften (berufliche Verschwiegenheitspflichten der Kanzleiinhaber und ihrer Gehilfen). Derartige datenschutzbezogene Vorschriften in anderen Gesetzen gelten weiterhin und haben gegenüber dem BDSG als so genanntem Auffanggesetz Vorrang.

Hierbei sind insbesondere die Regelungen des Multimedia- und Telekommunikationsbereichs zu nennen. So sind zum Beispiel die Regelungen des Telekommunikationsdatenschutzgesetzes (TDDSG) und der Telekommunikationsdatenschutzverordnung (TDSV) bei der Gestaltung der privaten Telefon-, E-Mail- oder Internetnutzung durch Mitarbeiter zu beachten.
Die einschlägigen Vorschriften des Teledienstegesetzes (TDG) und des Teledienstedatenschutzgesetzes (TDDSG) sind aber auch bei der Gestaltung einer Kanzleihomepage oder bei der Kommunikation mit Mandanten über Internet bindend.
Schließlich besteht auch ein Eigeninteresse der Kanzlei an einer Ausweitung des Schutzbereiches; etwa aus Verlustsicherungsgründen, um teure Wiederbeschaffungskosten für Daten zu vermeiden, oder bei Daten über Betriebs- und Geschäftsgeheimnisse, auch wenn sie nicht nach dem BDSG geschützt sind.

Einordnung der Kanzlei

Das BDSG unterscheidet für den Bereich der Privatwirtschaft in seinen Auswirkungen zwischen der Erhebung, Verarbeitung und Nutzung personenbezogener Daten für eigene Zwecke einerseits und für Auftragszwecke andererseits. Der Kanzleiinhaber unterliegt sowohl mit seinen eigenen (kanzleiinternen) Daten als auch mit den Mandantendaten den Vorschriften über die Datenverarbeitung für eigene Zwecke, da sich das Mandatsverhältnis auf die Erfüllung der steuer-, wirtschafts- oder rechtsberatenden Tätigkeit als originärem Geschäftszweck (Funktionsübertragung) bezieht, nicht aber auf die in diesem Zusammenhang erforderliche Erhebung, Verarbeitung oder Nutzung der Daten, die lediglich als Hilfsmittel zur Erfüllung der übergeordneten Aufgaben dienen. Der Kanzleiinhaber muss daher – beispielsweise beim Auftrag zur Erstellung einer Finanzbuchführung - die nachstehenden Vorschriften für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten für eigene Zwecke beachten.

Datenvermeidung und Datensparsamkeit

Ziel der gesetzlichen Vorschrift ist es, dass technisch bedingt, möglichst wenig personenbezogene Daten verarbeitet werden. Durch entsprechende Gestaltung der Systemstrukturen sollen Erhebung, Verarbeitung und Nutzung personenbezogener Daten weitgehend vermie-

den werden. Um diesem Grundgedanken Rechnung zu tragen, ist auch anonymen und pseudonymisierten Formen der Datenverarbeitung Vorrang einzuräumen.

Zulässigkeit der Erhebung, Verarbeitung und Nutzung

Die Erhebung, Verarbeitung und Nutzung ist datenschutzrechtlich nur zulässig, wenn das BDSG oder eine andere Rechtsvorschrift sie erlaubt oder der Betroffene ausdrücklich eingewilligt hat. Darüber hinaus müssen bei der Erhebung bestimmte Voraussetzungen – etwa Vorrang der Direkterhebung beim Betroffenen – beachtet werden (siehe Neuregelungen). Soweit es sich um die Mandantendaten handelt, bildet das Vertragsverhältnis zwischen der Kanzlei und dem Mandanten den erforderlichen Zulässigkeitstatbestand. Dies gilt sowohl für den Umgang mit den Daten des Mandanten als auch für den Umgang mit personenbezogenen Daten derjenigen, auf die sich das Mandatsverhältnis bezieht. Das sind beim Steuerberater zum Beispiel Daten der Arbeitnehmer, Kreditoren oder Debitoren des Mandanten. Darüber hinaus kämen teilweise auch einschlägige vorrangige Vorschriften im HGB und in der AO als Zulässigkeitstatbestand in Frage.

Bei kanzleiinternen Daten (z. B. Daten des Kanzleipersonals) sind die Erhebung, Verarbeitung und Nutzung vor allem gestattet, wenn sie der Abwicklung vertraglicher Beziehungen oder der Wahrnehmung überwiegender schutzwürdiger Interessen dienen.

Besondere Restriktionen sind – wie oben beschrieben - beim Umgang mit „besonderen Arten personenbezogener Daten“ (sensitive Daten) sowie beim Datentransfer in so genannte Drittstaaten zu beachten.

Einschaltung eines Service-Rechenzentrums

Bei Einschaltung eines externen Service-Rechenzentrums ist der Kanzleiinhaber verpflichtet, das Rechenzentrum (RZ) unter besonderer Berücksichtigung des dort vorhandenen Datenschutzstandards sorgfältig auszuwählen und sich von der Einhaltung der getroffenen Datenschutz-Maßnahmen zu überzeugen. Dies kann etwa durch Vorlage eines Bestätigungsschreibens, eines Testats durch eine neutrale Prüfinstanz (z.B. Wirtschaftsprüfer, Datenschutz-Audit) oder durch entsprechende Überprüfungen beim Auftragnehmer geschehen. Der Kanzleiinhaber als Auftraggeber bleibt jedoch weiterhin als „Herr der Daten“ für die Daten und somit auch für die Einhaltung der Datenschutzvorschriften verantwortlich (Rechts- und Schadenersatzansprüche der Betroffenen!). Das RZ darf die Daten nur im Rahmen der Weisung des Kanzleiinhabers erheben, verarbeiten oder nutzen. Da ein Service-Rechenzentrum quasi als verlängerter Arm des Auftraggebers handelt, ist hierbei datenschutzrechtlich zwar keine Zustimmung des Mandanten einzuholen, doch ist er gegebenenfalls im Rahmen der Erhebung darüber zu informieren. Aus berufsrechtlichen Gründen ist es nach der einschlägigen Rechtsprechung ferner darüber hinaus zumindest fraglich, ob die Kanzlei ohne Zustimmung des Mandanten Daten an ein gewerbliches Rechenzentrum übermitteln darf, das nicht in gleicher Weise wie DATEV der beruflichen Verschwiegenheit unterliegt. Deshalb enthalten die üblichen Musterverträge auch eine entsprechende Zustimmungsklausel; wo dies nicht der Fall ist, sollte die Zustimmung des Mandanten nachträglich eingeholt werden.

Zweckbindung der Daten

Nach dem BDSG gilt das Zweckbindungsprinzip. Daher sind bereits bei der Datenerhebung die geplanten Verwendungszwecke konkret festzulegen; bei Datenübermittlungen ist ausdrücklich auf die Einhaltung der Zweckbindung hinzuweisen.
Eine besondere Zweckbindung gilt nach § 39 BDSG bei personenbezogenen Daten, die einem Berufs- oder besonderen Amtsgeheimnis (z. B. Mandantendaten) unterliegen. In diesen Fällen ist die Änderung der Zweckbindung nur auf Grund besonderer Gesetzesbestim-

mungen zulässig; bei Datenübermittlungen ist immer die Zustimmung des jeweiligen Berufsträgers erforderlich.

Rechtsansprüche der Betroffenen

Jeder Betroffene hat einen Rechtsanspruch auf Benachrichtigung, Auskunft sowie gegebenenfalls Berichtigung, Sperrung und Löschung der zu seiner Person gespeicherten Daten. Diese Rechtsansprüche dürfen von der Kanzlei jedoch nur für kanzleiinterne Daten wahrgenommen werden; bei Mandantendaten (Mitarbeiter, Kreditoren, Debitoren des Mandanten) ist aus Gründen der beruflichen Verschwiegenheitspflicht eine unmittelbare Auskunftserteilung an den Betroffenen nicht zulässig, es sei denn, es liegt eine ausdrückliche Weisung des betreffenden Mandanten als legitimiertem Auftraggeber vor.

Datengeheimnis

Die Kanzleiangestellten müssen über die Bestimmungen des BDSG und andere Datenschutzvorschriften belehrt und nach § 5 BDSG schriftlich auf das Datengeheimnis verpflichtet werden. Ob die nach den §§ 62 StBerG, 43 Abs.1 WPO, 43 a Abs. 2 BRAO vorgeschriebene Verschwiegenheitsverpflichtung diesen Ansprüchen genügt, hängt vom jeweiligen Wortlaut der verwendeten Verpflichtungserklärung ab. Die neueren Musterformulare genügen diesen Anforderungen; anderenfalls ist eine entsprechende Ergänzung bzw. ein Nachtrag erforderlich (siehe z.B. Merkblatt der Bundessteuerberaterkammer).

Datensicherheit

Jeder Kanzleiinhaber trägt nicht nur die Verantwortung für die Einhaltung der Grundsätze der Ordnungsmäßigkeit, sondern muss in seiner Kanzlei auch eigenverantwortlich ausreichende Datensicherungsmaßnahmen (Verhältnismäßigkeitsprinzip!) zum Schutz von Daten, Datenträgern und Kommunikationsgeräten vor missbräuchlicher Verwendung, Verlust und Störungen jeder Art treffen.
Die Maßnahmen dienen zur Sicherstellung der

- Vertraulichkeit (Daten/Informationen dürfen nur Berechtigten zur Kenntnis gelangen),
- Verfügbarkeit (Daten/Informationen müssen in vereinbarter Form und Qualität zu jedem vereinbarten Zeitpunkt nutzbar sein),
- Integrität (die Änderungen der Daten/Informationen müssen zugelassen sein),
- Verbindlichkeit (die Urheberschaft ist zweifelsfrei nachzuweisen).

Spezielle gesetzliche Vorschriften sind bei automatisierter Datenverarbeitung (so genannte acht Gebote der Datensicherheit, Anlage zu § 9 Satz 1 BDSG) sowie bei automatisierten Abrufverfahren (§ 10 BDSG)zu beachten.
Welche Sicherungsmaßnahmen erforderlich sind, hängt vor allem weit gehend davon ab, ob Daten in einem Rechenzentrum oder vor Ort in der Kanzlei verarbeitet werden. Die Datenschutzrisiken sind etwa bei Einschaltung der DATEV sowohl wegen des weitaus größeren Potenzials an wirkungsvollen Datensicherheitseinrichtungen als auch wegen des unterschiedlichen Geheimhaltungsbedürfnisses der Daten wesentlich geringer als in der Kanzlei oder beim Mandanten. Je mehr Datenverarbeitungsaktivitäten in die Kanzlei verlagert werden, umso mehr Sicherungsmaßnahmen sind vor Ort wegen der Eigenverantwortlichkeit des Kanzleiinhabers für den Schutz der Daten seines Verantwortungsbereiches erforderlich. Es bleibt daher grundsätzlich auch dem Kanzleiinhaber überlassen, welche Programme mit welchen Eigenschaften von welchen Herstellern eingesetzt werden. Ein Rechenzentrum hat weder eine datenschutzrechtliche noch eine vertragsrechtliche Verpflichtung, stellvertretend für ihre Auftraggeber deren Datenschutzverpflichtungen sicherzustellen. Andererseits ist etwa die DATEV jedoch bemüht, ihren Anwendern Dienstleistungen anzubieten, die auch die Anforderungen des Datenschutzes möglichst mit abdecken. Hierbei liegt es allerdings auch gerade im Interesse ihrer Mitglieder, andere Aspekte (z. B. Kosten, einfaches Handling, freie Speicherkapazität etc.) hinreichend zu berücksichtigen, um in der Gesamtheit möglichst eine Optimallösung anbieten zu können. Es bleibt jedoch letztlich in der Verant-

wortung des Kanzleiinhabers, solche Datenschutz-Dienstleistungen auch zu nutzen oder – wo die Datenschutzerfordernisse damit nicht hinreichend abgedeckt werden können – zusätzliche Sicherungsmaßnahmen einzuführen. Hierbei wird er in jedem Fall durch entsprechende Hinweise der DATEV auf bestehende Risiken und daraus resultierende Sicherheitserfordernisse unterstützt.

Neue technikorientierte Regelungen

Im Zusammenhang mit der jüngsten Novellierung des Bundesdatenschutzgesetzes wurden unter anderem technikorientierte Regelungen zur automatisierten Einzelentscheidung (§ 6 a BDSG), Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (§ 6 b BDSG Videoüberwachung) sowie mobile personenbezogene Speicher- und Verarbeitungsmedien (§ 6 c BDSG, zum Beispiel Chipkarten) neu eingeführt.
Nach § 6 a BDSG dürfen rechtlich relevante Entscheidungen oder solche, die den Betroffenen erheblich beeinträchtigen, nicht allein auf gespeicherte Bewertung gestützt werden.
Die Videoüberwachung (§ 6 b BDSG) öffentlich zugänglicher Räume ist nur unter spezifischen Voraussetzungen zulässig. Daraus gewonnene Daten dürfen nur in sehr begrenztem Umfang verarbeitet werden. Chipkarten und andere mobile personenbezogene Speicher- und Verarbeitungsmedien (§ 6 c BDSG) müssen bestimmte Anforderungen erfüllen und vor allem für den Betroffenen transparent sein.

Diese Vorschriften gelten zwar grundsätzlich auch für die Kanzlei, dürften in der Praxis jedoch nur sehr eingeschränkt bedeutsam sein. Beispielsweise käme jedoch eine Anwendbarkeit des § 6 b BDSG (Videoüberwachung) bei der Kameraüberwachung des Kanzleigebäudes in Frage, sofern hierbei öffentlich zugängliche Bereiche, zum Beispiel angrenzende öffentliche Straßen und Wege, miterfasst werden.

Datenschutzbeauftragter (DSB)

Ein DSB ist zu bestellen, wenn

- automatisierte Verarbeitung besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, die einer Vorabkontrolle unterliegen;
- eine ansonsten bestehende Meldepflicht an die Datenschutz-Aufsichtsbehörde abgewendet werden soll;
- mindestens fünf Kanzleiangestellte mit der automatisierten oder mindestens 20 Kanzleiangestellte mit der nicht automatisierten Verarbeitung, Nutzung oder Erhebung personenbezogener Daten beschäftigt sind.

Der DSB muss spätestens innerhalb eines Monats nach Eintritt der Bestellpflicht schriftlich bestellt werden.

Grundsätzlich ist zu berücksichtigen, dass die Datenschutzvorschriften auch dann einzuhalten sind, wenn kein DSB zu bestellen ist. In diesem Fall obliegen die Aufgaben des Datenschutzbeauftragten dem Kanzleiinhaber. Deshalb ist im Zweifelsfall zur Entlastung des Kanzleiinhabers immer anzuraten, einen Mitarbeiter zum DSB zu bestellen, der diese Funktion in Personalunion neben seinen bisherigen Tätigkeiten ausübt. Alternativ dazu kommt auch die Bestellung eines externen Datenschutzbeauftragten in Frage.
Nach den BDSG-Vorschriften muss der DSB über die zur Erfüllung seiner Aufgabe erforderliche Fachkunde und Zuverlässigkeit verfügen und ist dem Kanzleiinhaber direkt zu unterstellen. Er ist bei Anwendung seiner Fachkunde weisungsfrei.
Als zentrale Anlaufstelle in Datenschutzfragen ist er zur Verschwiegenheit über die Identität von Betroffenen verpflichtet.
Der DSB hat die Aufgabe, auf die Einhaltung des BDSG und anderer Datenschutzvorschriften in der Kanzlei umfassend hinzuwirken („Sicherstellung“ des Datenschutzes). Schwerpunkte seiner Tätigkeit sind insbesondere:

- Prüfung der Zulässigkeit des Umgangs mit Daten und deren Absicherung,
- Vorabkontrolle bei sensitiven Daten,

- Überwachung der ordnungsgemäßen Programmanwendung,
- Unterrichtung von Mitarbeitern über die Anforderungen des Datenschutzes.

Der DSB ist rechtzeitig über neue Vorhaben automatisierter Datenverarbeitung zu unterrichten. Als wichtiges Hilfsmittel muss ihm von der Kanzlei ferner eine Übersicht über die automatisierten Verarbeitungsverfahren mit zugriffsberechtigten Personen zur Verfügung gestellt werden.
Der DSB ist bei der Erfüllung seiner Aufgaben zu unterstützen. Er darf nicht benachteiligt werden und kann nur unter erschwerten Bedingungen (§ 626 BGB) oder auf Verlangen der Aufsichtsbehörde abberufen werden.

Datenschutz-Audit

Wie bereits oben dargestellt, können Anbieter von Datenverarbeitungssystemen und -programmen, aber auch andere Daten verarbeitende Stellen ihr Datenschutzkonzept zur Verbesserung des Datenschutzes und der Datensicherheit durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen. Diese Bestimmung richtet sich zwar vorrangig nicht an die Kanzlei. Gleichwohl kann bei Einschaltung eines Service-Rechenzentrums die Vorlage eines entsprechenden Zertifikates durch den Auftragnehmer dazu beitragen, seine gesetzlich auferlegte Sorgfaltspflicht bei der Auswahl eines geeigneten Service-Rechenzentrums sicherzustellen und zu dokumentieren.

Aufsichtsbehörde

Die Ausführung der Datenschutzvorschriften wird extern durch eine Datenschutz-Aufsichtsbehörde überwacht. Sie hat das Recht, sowohl bei begründeten Anlässen als auch ohne Anlass die Kanzleiräume zu betreten und auch in Daten Einsicht zu nehmen oder darüber Auskunft verlangen zu dürfen, die dem Berufsgeheimnis unterliegen. Stellt die Aufsichtsbehörde technische oder organisatorische Mängel fest, kann sie Maßnahmen zur Abhilfe anordnen oder – bei schwerwiegenden Mängeln – den Einsatz einzelner DV-Verfahren untersagen. Bei Datenschutzverstößen hat sie darüber hinaus das Recht, Strafantrag zu stellen und den Betroffenen sowie die zuständige Behörde zu unterrichten.

Straf- und Bußgeldvorschriften

Bei Verstößen gegen das Bundesdatenschutzgesetz sind Gefängnisstrafen bis zu zwei Jahren oder Geldstrafen (Straftat) bzw. Geldbußen bis zu 250.000.- € (Ordnungswidrigkeit) vorgesehen. Die Straf- und Bußgeldvorschriften betreffen nicht nur den Kanzleiinhaber, sondern darüber hinaus auch den jeweiligen Kanzleiangestellten, falls er unberechtigt mit personenbezogenen Daten umgeht.

Fazit

Das neue Datenschutzgesetz bedeutet erst einmal eines: mehr Arbeit.
Über Sinn oder Unsinn mancher neuer Regelung im BDSG lässt sich streiten - aber das Gesetz ist umzusetzen. Dies erfordert eine Sichtung, Bewertung und Risikoabwägung in den Kanzleien. Dazu gehört eine detaillierte Auseinandersetzung mit den Neuregelungen des BDSG, eine Bestandsaufnahme (Inventur) der automatisierten Verfahren mit personenbezogenen Daten, die Ist-Aufnahme der technischen und organisatorischen Maßnahmen, eine Bewertung des Sicherungskonzepts und Entscheidung über Vorabkontrolle und Datenschutzaudit.

Als Hilfestellung wird von DATEV derzeit ein Handbuch (Artikel-Nummer 11761) entwickelt, das auf die Bedeutung und Umsetzung der einzelnen Regelungen im Alltag der Kanzleien im Einzelnen eingeht.
Das Handbuch enthält unter anderem eine Gesamtdarstellung des Themenkreises „Datenschutz und Datensicherheit in der Kanzlei“, Hilfestellungen der DATEV bei der Festlegung

technischer und organisatorischer Maßnahmen zum Datenschutz, Muster und Richtlinien für die Datenschutzorganisation und Hinweise zu ausgewählten Themen der Datensicherheit (z. B. digitale Signatur, Internet, Computerviren, Fernbetreuung).

Die Autoren

Thomas Müthlein, DMC Datenschutz Management & Consulting GmbH & Co.KG, Köln, und *Jürgen Hund*, DATEV eG.