DATEV magazin
04/2018

ISSN 2197-2893 FÜR STEUERBERATER, WIRTSCHAFTSPRÜFER, RECHTSANWÄLTE 25. JAHRGANG APRIL 2018

Jetzt wird es ernst

Die EU-Datenschutz-Grundverordnung kommt

Notwendig

Die DATEV braucht eine Satzungsänderung, um die Genossenschaft zukunftsfähig zu machen.

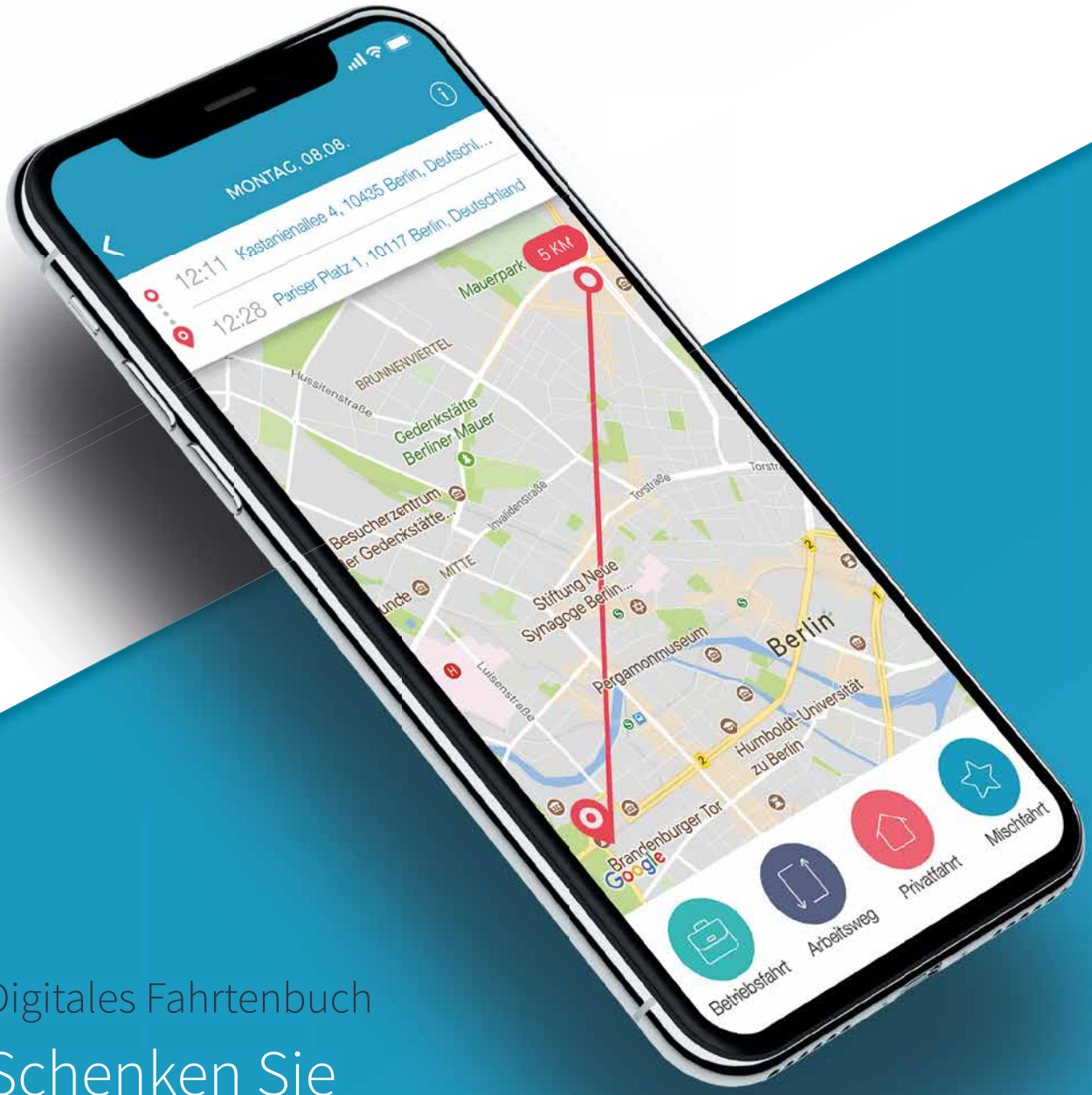
Rechtssicher

Was ist beim Umgang mit Arbeitnehmerdaten künftig zu beachten?

Vorbereitet

Worauf kommt es bei einem effektiven IT-Notfallmanagement an?

VIMCAR



Digitales Fahrtenbuch

Schenken Sie Ihren Mandanten Geld und Zeit!

vimcar.de/datev

Haben Sie noch Fragen? Gerne helfen wir Ihnen weiter! **steuerberater@vimcar.de** und **030 555 732 980**

Wusten Sie schon …

55 Mrd.

… Euro beziffert sich der Schaden, der der deutschen Wirtschaft durch Spionage, Sabotage, Datendiebstahl entsteht.

Quelle: Digitalverband Bitkom

4 von 10

… Unternehmern setzen ihre Mitarbeiter ganz oder teilweise via Homeoffice ein.

Quelle: Digitalverband Bitkom

Nur 27 %

… der deutschen Handwerksbetriebe fühlen sich zum Thema Kassennachschau gut informiert.

Quelle: DATEV

Datenschutz und IT-Sicherheit – zwei Themen, die in den Kanzleien häufig nebenbei laufen müssen, ja manchmal ein Stiefmütterchendasein fristen. Das wird sich mit der Datenschutz-Grundverordnung zwangsläufig ändern – drohen doch hohe Bußgelder. Zudem wirft das neue Recht viele Fragen auf. Ab wann etwa braucht man einen Datenschutzbeauftragten oder was ändert sich beim Beschäftigtendatenschutz gegenüber dem alten Recht? Ein anderer Aspekt ist die IT-Sicherheit. Entsteht doch der deutschen Wirtschaft jährlich ein immenser Schaden, etwa durch Social Engineering.

MARKUS KORHERR
Chefredakteur DATEV magazin

150.000.000

… Lohnabrechnungen wurden 2017 über DATEV-Systeme abgewickelt.

Quelle: DATEV

7 von 10

… Menschen ab 60 Jahren nutzen Facebook.

Quelle: Meedia.de

54 %

… der Geschäftsführer und Vorstände von Unternehmen mit mehr als 20 Beschäftigten geben an, dass sie von Plattformökonomie, Plattformmärkten oder digitalen Plattformen noch nie gehört haben.

Quelle: Digitalverband Bitkom

ERSTE BEHÖRDEN NUTZEN ZENTRALEN DIENST FÜR DIE E-AKTE (QUELLE: VOGEL BUSINESS MEDIA).

Datenschutzrecht

Die DATEV unterstützt Kanzleien und ihre Mandanten dabei, das bestehende Datenschutzniveau zu beurteilen und sich auf die EU-Datenschutzgrundverordnung vorzubereiten.

www.datev.de/dsgvo

ZUM THEMA KASSE BERATEN!

www.datev.de/kasse

HANDELN SIE *jetzt!*

DS-GVO –
neue Vereinbarung zur Auftragsverarbeitung abschließen:

www.datev.de/av

Perspektiven 06

Nachrichten Steuer & Recht 20

Praxis 21

08 Titelthema – Datenschutz und Informationssicherheit

VORSCHAU
AUSGABE
05 / 18

Titelthema

Wissensmanagement
Täglich werden wir mit einer größer werdenden Menge von Informationen konfrontiert, doch es gibt Mittel und Strategien, mit dieser Herausforderung erfolgreich umzugehen.

Eine zukunftsfähige Satzung für die Genossenschaft

Satzungsänderung | Am 19. Februar hat eine außerordentliche Vertreterversammlung der DATEV eG über die Änderung der Satzung abgestimmt. Der Antrag verfehlte mit rund 74 Prozent denkbar knapp die nötige Dreiviertelmehrheit. Das Ergebnis verstehen wir als klaren Auftrag, am Thema weiterzuarbeiten.

Autor: Dr. Robert Mayr

Über die Herausforderungen der digitalen Transformation haben Sie hier im DATEV magazin und an anderer Stelle schon viel gelesen. Genau diese Herausforderungen haben meine Vorstandskollegen und mich auch bewegt, lange bevor klar wurde, dass eine Satzungsänderung ein wichtiger Baustein für die Gestaltung der Zukunft unserer Genossenschaft werden würde.

Am Anfang stand eine Erkenntnis, die heute wohl niemand mehr infrage stellt: Wir befinden uns in einem Zeitalter der Plattformökonomie. Das bedeutet, dass die Anbieter digitaler Portale in allen Bereichen der Wirtschaft wichtiger werden. Sie schieben sich als Makler in die klassische Beziehung zwischen Kunde und Dienstleister, degradieren den Dienstleister zum reinen Produzenten ohne Kontakt zum Kunden und drängen ihn somit in den Hintergrund. Die Hotel- und Taxibranche hat bereits erleben müssen, wie dramatisch Plattformen in ihr Gewerbe eingreifen. Auch im Geschäftsfeld der steuerlichen Berater tauchen mit JustAnswer, Ageras oder yourXpert Portalanbieter am Markt auf. Immer mehr Mitbewerber drängen im Bereich Einkommensteuererklärung auf den Markt. Banken bieten bereits erste Angebote zur Belegablage und sogar zu einer einfachen Steuerdeklaration an. Mit Amazon tritt zudem ein sehr mächtiger Player in Erscheinung, der für E-Commerce-Unternehmen die monatliche Erstellung ihrer Umsatzsteuererklärung möglich macht.

Die Plattformökonomie als Chance

Als Vorsitzender des Vorstands sehe ich es als wichtigste Aufgabe an, mit unserer Genossenschaft die Zukunftsfähigkeit der Mitglieder zu sichern. Dazu gehört, Marktentwicklungen zu beobachten, zu analysieren und hinsichtlich Chancen und Risiken für Sie, unsere Mitglieder, zu bewerten. Die Stärke der Genossenschaft besteht dabei seit ihrer Gründung darin, dass wir gemeinsam Herausforderungen meistern können, die den Einzelnen überfordern würden. Gerade weil wir gemeinsam diese Stärke haben, müssen wir die Plattformökonomie nicht als Bedrohung hinnehmen, sondern können sie uns als Chance zunutze machen. Dies führte zur Plattformstrategie der DATEV, die wir in den letzten Monaten entwickelt haben: Statt zuzusehen, wie sich Dritte mit einer Plattform zwischen Steuerberater und ihre Mandanten schieben und damit die Berater in den Hintergrund drängen, möchte DATEV selbst Plattformen bauen und gestalten, die im Sinne der Genossenschaft den Mitgliedern neue Chancen und Zielgruppen erschließen und sie mithin zu Profiteuren von digitaler Transformation und Plattformökonomie machen.

Vom Steuerbürger zum Mandanten

Basierend auf dieser Strategie haben wir mit dem sogenannten Steuerbürgerszenario eine erste konkrete Lösung konzipiert: Rund 13 Millionen steuerpflichtige Privatpersonen erstellen ihre Steuererklärung bisher selbst. Über eine neue DATEV-Plattform soll diesen Personen eine einfache Möglichkeit zur digitalen Deklaration gegeben werden – verbunden mit dem Angebot, bei komplexeren Fragen Kontakt zu einem DATEV-Mitglied aufzunehmen und sich beraten zu lassen. So wird aus dem Risiko eine Chance: Statt Sie als Berater zu verdrängen, wie andere Plattformen das womöglich machen würden, rücken wir Sie in den Mittelpunkt aller Überlegungen und bauen die Plattform so, dass Sie durch die Anbahnung neuer Mandatsverhältnisse profitieren.

Gelegentlich lese ich in Diskussionen zum Thema, diese Privatpersonen seien als Mandanten nicht interessant. Das mag für diese Veranlagung stimmen, gegebenenfalls aber nicht mehr für dieselbe Person in ein paar Jahren. Vergessen Sie bitte nicht, dass wir über die Zukunft reden und in Zeiten leben, in denen etablierte Geschäftsmodelle viel schneller in Gefahr geraten, als man sich das aus einer Position wirtschaftlicher Stärke heraus vorstellen kann. Und wir leben in Zeiten, in denen sich unsere Kunden verändern: Ganze Generationen junger Menschen sind es inzwischen gewohnt, zuerst bei einer Suchmaschine nach Rat zu suchen, selbst wenn es um so sensible Themen wie Gesundheit und Medizin geht. Die Plattformökonomie macht sich genau diese Entwicklung zunutze: Sie holt die Interessenten dort ab, wo sie sich täglich aufhalten: im Internet. Einen Steuerberater anzurufen oder gar aufzusuchen – auf diese Idee werden plattformkonditionierte Internetnutzer auch dann nicht mehr kommen, wenn Sie zu spannenden potenziellen Mandanten gereift sind, etwa da sich ihre Vermögens- oder Einkommensverhältnisse geändert haben.

Notwendigkeit einer Satzungsänderung

Ausgehend von diesen Überlegungen führte uns der Weg zur außerordentlichen Vertreterversammlung, von der ich oben geschrieben habe. Denn bei unseren Strategieüberlegungen wurde schnell deutlich, dass unsere Satzung aus Zeiten stammt, in denen es noch keine digitale Transformation und Plattformökonomie gab. Eine zentrale genossenschaftliche Plattform aufzubauen und über Suchmaschinen gut auffindbar zu machen, die Privatpersonen bei der Erledigung ihrer einfachen Steuerfälle unterstützt, die also potenzielle Mandanten an die Genossenschaft bindet und den DATEV-Mitgliedern zuführt – das ist mit unserer heutigen Satzung nicht möglich.
Als Konsequenz erarbeitete eine Satzungskommission, die sich aus Mitgliedern aller DATEV-Gremien zusammensetzte, einen Änderungsvorschlag, der die Erweiterung des Geschäftsbetriebs der Genossenschaft mit sonstigen Nichtmitgliedern vorsah. Flankiert wurde der Vorschlag von zusätzlichen Berichtspflichten des Vorstands an den Aufsichtsrat, von einer Zustimmungspflicht durch den Aufsichtsrat und von einer freiwilligen Selbstverpflichtung des Vorstands, die unter anderem garantierte, dass es keinen funktionalen Vorsprung im Nichtmitgliedergeschäft gegenüber dem Mitgliedergeschäft geben wird. Der Vorstand hat sich diesen Vorschlag zu eigen gemacht und einen Antrag auf Satzungsänderung gestellt.

Zukunft gestalten nach der Vertreterversammlung

Auch wenn der Antrag denkbar knapp gescheitert ist, hat die Abstimmung dennoch gezeigt, dass die große Mehrheit in der Vertreterversammlung den vom Vorstand eingeschlagenen Weg gutheißt und mitzugehen bereit ist. Die Bemühungen um die Zukunftsfähigkeit unserer Genossenschaft in Zeiten der digitalen Transformation einfach einzustellen, wäre fahrlässig und würde den Wunsch der Mehrheit der Vertreter ignorieren. Daher verstehe ich das Ergebnis der Abstimmung als klaren Auftrag, am Thema weiterzuarbeiten, die vorgebrachten Bedenken sehr ernst zu nehmen, die Argumente zu schärfen und weiter für die angestrebte Satzungsänderung zu werben, sodass sie vielleicht schon in der kommenden ordentlichen Vertreterversammlung Ende Juni erneut zur Abstimmung gebracht werden kann. Nach intensiven Gesprächen mit dem Aufsichtsrat und den Vorsitzenden des Vertreterrats sehe ich das nicht nur als Möglichkeit, sondern als Aufgabe an. Und auch die intensiven Diskussionen auf den Regional-Info-Tagen bestärken mich darin: Unsere Mitglieder sind höchst interessiert am Thema! Dabei habe ich viel positives Feedback für unsere Plattformstrategie bekommen – und einen starken Rückenwind wahrgenommen, auch das Thema Satzungsänderung weiterzuverfolgen. In den kommenden Wochen und Monaten liegt daher weiterhin viel Arbeit vor uns. Vor allem möchten wir Sie als Mitglied ausführlicher informieren: in unseren Online-Medien, hier im DATEV magazin und im persönlichen Austausch auf unseren Veranstaltungen.

Die Zukunft – das unentdeckte Land

Am Ende des Tages kann keiner von uns sicher sein, wie der nächste Tag und der darauffolgende aussehen werden. Die Zukunft ist ein unentdecktes Land, und wir sind auf dem Weg dorthin, ohne genau zu wissen, was uns dort erwartet. Wir können uns nur so gut und so rechtzeitig wie möglich auf die Reise vorbereiten. Dabei bitte ich Sie herzlich um Ihr Vertrauen! DATEV hat in den über 50 erfolgreichen Jahren ihres Bestehens niemals das Vertrauen der Mitglieder missbraucht und wird das auch in Zukunft nicht tun. Der Vorstand will vielmehr gemeinsam mit Ihnen diese Erfolgsgeschichte fortschreiben. ●

DR. ROBERT MAYR
Vorstandsvorsitzender
der DATEV eG

Datenschutz achten!

Daten der Beschäftigten | Mit Blick auf die Datenschutz-Grundverordnung ist der Umgang mit Arbeitnehmerdaten grundlegend zu überdenken, insbesondere in Bezug auf den einzuhaltenden Grundsatz der Datensparsamkeit.

Autorin: Katharina Haslach

Täglich verarbeiten Personalabteilungen eine Vielzahl von Beschäftigtendaten, von den Personalstamm- inklusive Gehaltsdaten über Daten der Zeiterfassung bis hin zu Gesundheitsdaten, die im Rahmen eines betrieblichen Eingliederungsmanagements erhoben werden. Die Datenverarbeitung ist dabei nicht auf das laufende Arbeitsverhältnis beschränkt; vielmehr beginnt sie bereits mit der Bewerbung und endet auch mit der Beendigung des Arbeitsverhältnisses nicht. Mit Blick auf die hohen Bußgelder, die bis zu 20 Millionen Euro oder vier Prozent des weltweiten Jahresumsatzes betragen können, müssen Personalabteilungen sich dringend fragen, wie sich die Datenschutz-Grundverordnung (DSGVO), ergänzt um das neue Bundesdatenschutzgesetz (BDSG n. F.), die ab dem 25. Mai 2018 gelten, auf die Verarbeitung personenbezogener Daten der Beschäftigten auswirkt. Der schon nach altem Recht maßgebliche Grundsatz, wonach jeglicher Umgang mit personenbezogenen Mitarbeiterdaten grundsätzlich unzulässig ist, es sei denn, ein Gesetz, eine Betriebsvereinbarung beziehungsweise ein Tarifvertrag erlauben es oder der Arbeitnehmer hat in die Datenverarbeitung eingewilligt (Verbot mit Erlaubnisvorbehalt), gilt auch unter der DSGVO und dem BDSG n. F. Die zentrale Regelung im Beschäftigtendatenschutz ist § 26 BDSG n. F. (bislang § 32 BDSG), der bestimmt, dass die Datenverarbeitung zulässig ist, soweit sie zur Entscheidung über die Begründung eines Arbeitsverhältnisses, der Durchführung oder Beendigung eines Arbeitsverhältnisses, der Erfüllung der sich aus einem Tarifvertrag oder einer Betriebsvereinbarung ergebenden Rechte und Pflichten sowie der Aufdeckung von Straftaten bei bestehendem Tatverdacht erforderlich ist.

Bewerbungsverfahren

Dementsprechend darf der Arbeitgeber einen Bewerber weiterhin nach Namen, Anschrift und E-Mail-Adresse sowie den fachlichen Kenntnissen, der Ausbildung und dem beruflichen

Werdegang fragen. Wie bislang ist es auch unter der DSGVO dagegen grundsätzlich nicht zulässig, nach der Schwerbehinderung, der Religions- oder Gewerkschaftszugehörigkeit oder einer Schwangerschaft zu fragen. Der Arbeitgeber darf lediglich fragen, ob der Bewerber an gesundheitlichen, seelischen oder ähnlichen Beeinträchtigungen leidet, durch die er zur Verrichtung der beabsichtigten Tätigkeit ungeeignet ist. Problematisch ist ebenfalls die Erhebung von Daten des Bewerbers über Google oder soziale Netzwerke, wie beispielsweise Xing oder Facebook. Denn soweit hier überhaupt berufsbezogene Daten erhoben werden – das Privatleben des Arbeitnehmers ist für den Arbeitgeber weiterhin tabu –, hätte der Arbeitgeber strenge Informationspflichten gemäß Art. 14 DSGVO gegenüber dem Bewerber zu beachten. So müsste er ihm beispielsweise die Kontaktdaten des Verantwortlichen sowie des Datenschutzbeauftragten ebenso mitteilen wie die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, und auch die Rechtsgrundlage für die Verarbeitung der Daten sowie die Dauer der Speicherung. Daher sollte man Abstand nehmen, auf diese Weise Zusatzinformationen über die Bewerber zu beschaffen. Die aufgezählten Mitteilungspflichten gelten aber auch dann bereits in der Bewerbungsphase, wenn die Daten vom Bewerber selbst erhoben werden (Art. 13 DSGVO), soweit er nicht bereits über die Informationen verfügt. Deshalb ist es zukünftig angeraten, den Bewerbern mit der Eingangsbestätigung ihrer Unterlagen die nach Art. 13 DSGVO erforderlichen Informationen, wie insbesondere die Kontaktdaten des Datenschutzbeauftragten und die Speicherdauer, mitzuteilen. Unter der DSGVO wird es mit Blick auf die drohenden, empfindlichen Bußgelder noch wichtiger als bisher sein, den Grundsatz der Datensparsamkeit einzuhalten. So muss die Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Maß beschränkt werden. Unterlagen abgelehnter Bewerber müssen innerhalb einer angemessenen Frist gelöscht werden. Sollen die Daten in einen Bewerber-Pool für zukünftig zu besetzende Stellen

aufgenommen werden, muss der Bewerber ausdrücklich zustimmen, wobei auch hier keine unbegrenzte Speicherung erfolgen darf und die konkrete Dauer dem Bewerber vor dessen Zustimmung mitzuteilen ist.

Arbeitsverhältnis

Weiterhin zulässig bleibt natürlich die Datenerhebung zur Zeiterfassung und Gehaltsabrechnung. Auch können beispielsweise im Rahmen eines betrieblichen Eingliederungsmanagements gesundheitsbezogene Daten erhoben und – getrennt von der eigentlichen Personalakte und besonders gesichert – aufbewahrt werden. Wichtig ist hier ebenfalls die neue Pflicht zum Hinweis auf die Dauer der Speicherung. Eine Datenverarbeitung liegt zudem auch dann vor, wenn Mitarbeiterdaten, wie beispielsweise Name, Telefonnummer und E-Mail-Adresse, auf der Homepage des Arbeitgebers veröffentlicht werden sollen, um die Kontaktaufnahme durch Kunden und sonstige Geschäftspartner zu erleichtern. Hier ist zwischen sogenannten Funktionsträgern und Nichtfunktionsträgern zu unterscheiden. Die Gruppe der Funktionsträger umfasst dabei alle offiziellen Ansprechpartner eines Unternehmens, zum Beispiel Kundenbetreuer, Geschäftsführer oder Niederlassungsleiter. Daten, die zwingend zur Kontaktaufnahme erforderlich sind, also Name, Tätigkeitsbereich, Telefonnummer und E-Mail-Adresse, dürfen grundsätzlich auch weiterhin ohne ausdrückliche Einwilligung des Arbeitnehmers veröffentlicht werden. Handelt es sich dagegen um Nichtfunktionsträger, wie beispielsweise eine reine Schreibkraft, oder sollen weitere Daten des Funktionsträgers veröffentlicht werden, wie Geburtsdatum, beruflicher Werdegang oder eine Fotografie, bedarf es der ausdrücklichen – vorherigen – Einwilligung des Arbeitnehmers. Die Einwilligung in die Datenverarbeitung, bisher in § 4a BDSG geregelt, ist nun in Art. 7 DSGVO und § 26 Abs. 2 BDSG n. F. normiert. Sie bedarf grundsätzlich der Schriftform - bei Vorliegen besonderer Umstände soll zwar eine weniger strenge Form möglich sein, was sich jedoch schon aus Beweisgründen nicht anbietet. Weiter erfordert eine wirksame Einwilligungserklärung Freiwilligkeit, weshalb die Einwilligung keinesfalls mehr mit dem Arbeitsvertrag verbunden oder gar in diesem enthalten sein darf, denn diese Koppelung hat den Anschein der Unfreiwilligkeit. Freiwillig sind Einwilligungen dagegen insbesondere dann, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und Beschäftigter gleichgelagerte Interessen verfolgen, § 26 Abs. 2 BDSG nF. Daneben muss der Zweck der Verarbeitung und Nutzung konkret benannt werden. Dazu ein Beispiel: Die Fotos werden zum Zweck der Außendarstellung des Unternehmens auf der Website www.unternehmen.de und auf den Social-Media-Kanälen (Facebook, Twitter, Instagram) veröffentlicht. Zudem hat eine Belehrung über ein jederzeitiges Widerrufsrecht zu erfolgen. Abzuwarten bleibt dabei, ob der einzelne Mitarbeiter dieses – wie bisher vom Bundesarbeitsgericht entschieden (BAG, Urteil vom 19.02.2015 – 8 AZR 1011/13) – nur bei Vorliegen eines plausiblen Grundes ausüben kann oder ob sich die Rechtsprechung unter der DSGVO und dem BDSG n. F. ändert. Bereits von den Mitarbeitern eingeholte Einwilligungen sollten ebenfalls auf ihre Vereinbarkeit mit dem neuen Datenschutzrecht überprüft werden. Entsprechen sie den Anforderungen der DSGVO, gelten sie fort. Die Einholung neuer Einwilligungen ist in diesen Fällen also nicht erforderlich.

> Die Speicherfrist für personenbezogene Daten ist nun auf das unbedingt erforderliche Maß zu beschränken.

Neue Betriebsvereinbarungen

Infolge der nun drastisch verschärften Strafen bei Datenschutzverstößen ist es dringend angeraten, die Nutzung der Kommunikationsmittel, wie insbesondere E-Mail, zu privaten Zwecken zu untersagen. Denn datenschutzrechtliche Probleme treten spätestens dann auf, wenn der Mitarbeiter kurzfristig erkrankt und der Arbeitgeber oder Kollegen Zugriff auf E-Mails dieses Mitarbeiters benötigen. Ist die Privatnutzung erlaubt, darf der Arbeitgeber in derartigen Fällen nur dann auf das E-Mail-Postfach des erkrankten Mitarbeiters zugreifen, wenn der Mitarbeiter ausdrücklich darin eingewilligt hat und der Zugriff für betriebliche Zwecke erforderlich ist – so bereits die bisherige Ansicht der Datenschutzaufsichtsbehörden des Bunds und der Länder. Besteht im Unternehmen zur Nutzung firmenbezogener Kommunikationsmittel bereits eine Betriebsvereinbarung, kann diese zwar wirksame datenschutzrechtliche Regelungen enthalten. Ob die getroffenen Vereinbarungen aber auch mit dem neuen Datenschutzrecht vereinbar sind, sollte man vor dem 25. Mai 2018 zwingend prüfen. Gegebenenfalls müssen neue Betriebsvereinbarungen abgeschlossen werden.

Verdacht einer Straftat

Was aber kann konkret unternommen werden, wenn der Mitarbeiter beispielsweise im Verdacht steht, Produktionsmittel zu stehlen oder seine Arbeitszeit mit Surfen im Internet zu verbringen? Nach aktueller Entscheidung des BAG vom 27. Juli 2017 (Az.: 2 AZR 681/16) dürfen jedenfalls keine sogenannten Keylogger – deutsch: Tastenprotokollierer – eingesetzt werden, ohne dass der konkrete Verdacht einer Straftat oder einer schwerwiegenden Pflichtverletzung besteht. Derartige, anlasslose Überwachungen können sogar einen Schmerzensgeldanspruch des unzulässig überwachten Arbeitnehmers begründen (BAG, Urteil vom 19.10.2015 – 8 AZR 1007/13). Die auf diese Weise erlangten Beweise sind zudem – so das BAG –

im Prozess nicht verwertbar. Soll überprüft werden, ob sich die Mitarbeiter tatsächlich an das ausdrückliche Verbot privater Internetnutzung halten, müssen sie nach einer Entscheidung des Europäischen Gerichtshofs für Menschenrechte (Urteil vom 05.09.2017 – 61496/08) vor der Überprüfung zudem über die Möglichkeit, die Art und das Ausmaß der Kontrolle unterrichtet werden. Besteht dagegen der konkrete Verdacht einer Straftat oder einer schwerwiegenden Pflichtverletzung, war die heimliche Mitarbeiterüberwachung bislang sogar in Form eines Detektiveinsatzes oder einer Videoüberwachung grundsätzlich zulässig, soweit keine weniger einschneidenden Mittel zur Verfügung stehen, den Mitarbeiter zu überführen (vgl. BAG, Urteil vom 29.06.2017 – 2 AZR 597/16). Ob diese Vorgehensweise unter der DSGVO weiterhin zulässig bleibt, ist noch unklar, nachdem die strengen Informationspflichten der Art. 13, 14 DSGVO nach ihrem Wortlaut auch hier gelten. Der Arbeitnehmer müsste also vom Arbeitgeber vor der Erhebung von Bilddaten im Rahmen einer verdeckten Videoüberwachung über diese Maßnahme aufgeklärt werden, wodurch natürlich der Sinn der verdeckten Kontrolle ins Leere liefe. Ein Ausschluss heimlicher Datenverarbeitung würde aber unweigerlich zu einem weitestgehenden Verbot verdeckter Arbeitnehmerkontrollen führen, was – so die bislang herrschende Meinung in der Literatur – nicht sein kann. Deshalb soll die Datenerhebung im Rahmen der heimlichen Mitarbeiterüberwachung weiterhin zulässig bleiben. Aufgrund der drohenden enorm hohen Bußgelder sollten Arbeitgeber jedoch bis zu einer gerichtlichen Klärung der Frage mit dem Einsatz heimlicher Kontrollen zurückhaltend umgehen und diesen zuvor sorgfältig prüfen. Anzumerken ist ferner, dass die Pflicht zur Datensparsamkeit auch uneingeschränkt im bestehenden Arbeitsverhältnis gilt. Im Rahmen der Löschung von Daten sind dabei die Fristen, innerhalb derer Ansprüche geltend gemacht werden können beziehungsweise die zur Aufbewahrung für die Kontrolle durch Behörden erforderlich sind, zu beachten. So müssen beispielsweise Entgeltunterlagen mit sozialversicherungsrechtlichen Bezügen fünf Jahre, für den Jahresabschluss relevante Unterlagen sogar zehn Jahre aufbewahrt werden. Nicht vergessen werden darf dabei, dass es auch für bereits erhobene und gespeicherte Daten keine Übergangsregelungen gibt, sodass alle im Sinne der DSGVO und des BDSG n. F. nicht erforderlichen Daten bis zum 25. Mai 2018 gelöscht sein müssen.

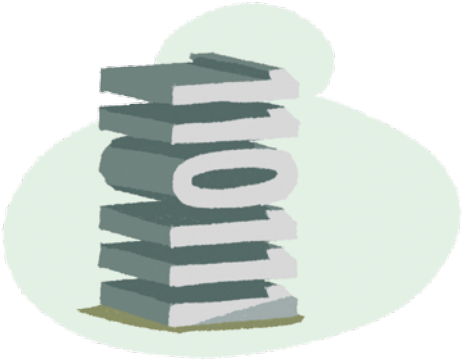
Ende des Arbeitsverhältnisses

Nach Beendigung des Arbeitsverhältnisses werden bestimmte Daten des ehemaligen Mitarbeiters weiterhin benötigt, um nachvertragliche Ansprüche, wie etwa aus einer betrieblichen Altersversorgung, zu erfüllen. Ausschließlich die zur Erfüllung des Anspruchs erforderlichen Daten – also nicht alle in der Personalakte gesammelten Daten – dürfen dafür gespeichert werden, wobei die Verarbeitung eingeschränkt werden sollte. Werden die Daten dagegen weder zur Abwicklung des Arbeitsverhältnisses noch eines nachvertraglichen Anspruchs benötigt, sind sie mit Ablauf der insoweit zu beachtenden Aufbewahrungsfristen zwingend zu löschen. Arbeitnehmer haben also ein Recht auf Vergessenwerden und können die Datenlöschung gemäß Art. 17 DSGVO auch aktiv verlangen. Für das Löschen elektronischer Daten genügt es dabei nicht, die Daten lediglich in den Papierkorb zu schieben und diesen zu leeren; vielmehr müssen die Daten mit Zufallsdaten so überschrieben werden, dass eine Wiederherstellung auch mithilfe von speziellen IT-Kenntnissen nicht oder jedenfalls nur schwer möglich ist. Alle Maßnahmen zur Beachtung des Datenschutzes von der Bewerberphase bis zur Beendigung des Arbeitsverhältnisses sind zudem (datenschutzkonform) zu dokumentieren, da die Einhaltung der datenschutzrechtlichen Vorschriften im Streitfall bewiesen werden muss, eine ebenfalls wesentliche Neuerung, die die DSGVO bereithält.

Ausblick

Die neue DSGVO, ergänzt um das BDSG n. F., wird für Arbeitgeber einen Einschnitt darstellen, denn bei Nichtbeachtung der Vorschriften drohen dann empfindliche Bußgelder. Der bisherige Umgang mit Bewerber- sowie Arbeitnehmerdaten muss daher grundlegend überdacht und überarbeitet werden, insbesondere in Bezug auf den einzuhaltenden Grundsatz der Datensparsamkeit. Das vollständige Ausmaß der Änderungen und der Herausforderungen ist zum jetzigen Zeitpunkt noch nicht absehbar, vielmehr sind die Leitlinien, die von der Rechtsprechung in den nächsten Jahren entwickelt werden, zu beobachten. ●

KATHARINA HASLACH
Rechtsanwältin in der Kanzlei Dr. Seier & Lehmkühler GmbH Rechtsanwaltsgesellschaft in Reutlingen, berät schwerpunktmäßig Unternehmen in arbeitsrechtlichen Fragen



MEHR DAZU

Unterstützungsangebote zur DSGVO finden Sie unter **www.datev.de/dsgvo-weiterbildung**

Neue Pflichten

Datenschutzbeauftragte | Durch die Datenschutz-Grundverordnung und das ergänzende nationale Recht ergeben sich auch Neuerungen für die Personen, die in den Unternehmen auf den Datenschutz zu achten haben.

Autor: Thomas Faas

In diesem Jahr ergeben sich grundlegende Änderungen im Datenschutzrecht. Ab dem 25. Mai 2018 gilt die EU-Datenschutz-Grundverordnung (DSGVO). Damit soll ein einheitlicher Datenschutzstandard in Europa geschaffen werden. Die bislang unterschiedlichen nationalen Bestimmungen werden im Sinne einer Vollharmonisierung abgelöst und in wesentlichen Punkten durch neue Vorschriften ersetzt. Der deutsche Gesetzgeber hat parallel dazu ein neues Datenschutzgesetz (BDSG n. F.) verabschiedet, das ebenfalls zum 25. Mai 2018 in Kraft tritt und an die Stelle des aktuell noch gültigen Datenschutzgesetzes (BDSG) tritt. Der wesentliche strukturelle Unterschied zur bisherigen Rechtslage besteht darin, dass die DSGVO unmittelbare Wirkung in allen EU-Mitgliedstaaten entfaltet und nationale Datenschutzbestimmungen nur noch dann zulässig sind, wenn die DSGVO ausdrücklich eine entsprechende Öffnungsklausel enthält. Neben zahlreichen bislang unbekannten Informations- und Dokumentationspflichten sowie einer drastischen Erhöhung des Bußgeldrahmens bei Verstößen ergeben sich durch das Zusammenspiel von DSGVO und BDSG n. F. auch Neuerungen hinsichtlich des Datenschutzbeauftragten. Die maßgeblichen Bestimmungen sind Art. 37–39 DSGVO und § 38 in Verbindung mit §§ 5–7 BDSG n. F.

> Der primäre Geschäftszweck des Unternehmens muss in der Verarbeitung personenbezogener Daten bestehen.

Benennung eines Datenschutzbeauftragten

Während das deutsche Datenschutzrecht für Unternehmen schon seit Langem die Bestellung eines Datenschutzbeauftragten vorsieht, war bei den Verhandlungen über die DSGVO umstritten, ob eine solche Verpflichtung auch auf europäischer Ebene normiert werden sollte. Letztlich wurde eine europaweit einheitliche Verpflichtung zur Benennung (nach bisherigem Recht: Bestellung) eines Datenschutzbeauftragten in die DSGVO aufgenommen. Bislang unterliegen Unternehmen in Deutschland einer Verpflichtung zur Bestellung eines Datenschutzbeauftragten, wenn sie

- in der Regel zehn oder mehr Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen oder
- in der Regel mindestens 20 Personen mit der nicht automatisierten Verarbeitung personenbezogener Daten beschäftigen (§ 4f BDSG).

Nach der DSGVO trifft Unternehmen künftig vor allem dann eine Verpflichtung zur Benennung eines Datenschutzbeauftragten, wenn die Kerntätigkeit des Unternehmens in der Durchführung von Verarbeitungsvorgängen besteht, die aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen (Art. 37 Abs. 1 lit. b) DSGVO). Die DSGVO knüpft damit im Unterschied zum bisherigen deutschen Recht nicht an ein konkret messbares quantitatives, sondern an ein risikobasiertes Kriterium an. Dementsprechend ist umstritten, was unter dem Begriff der Kerntätigkeit des Unternehmens zu verstehen ist. Nach wohl überwiegender Auffassung muss der primäre Geschäftszweck des Unternehmens in der Verarbeitung personenbezogener Daten bestehen. Da auch in der Arbeitswelt 4.0 die meisten Unternehmen einen anderen primären Geschäftszweck, etwa die Herstellung und den Vertrieb von Waren oder die Erbringung von Dienstleistungen, verfolgen und die Verarbeitung personenbezogener Daten nur als Nebentätigkeit anfällt, trifft die europaweite Verpflichtung zur Benennung eines Datenschutzbeauftragten nach der DSGVO derzeit nur einen geringen Anteil der Unternehmen. Der deutsche Gesetzgeber hat jedoch von der Öffnungsklausel der DSGVO (Art. 37 Abs. 4 Satz 1 DSGVO) Gebrauch gemacht. Unternehmen in Deutschland müssen künftig stets dann einen Datenschutzbeauftragten benennen, wenn sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen (§ 38 Abs. 1 BDSG n. F.). Die bisherige Regelung zur Bestellpflicht bei nicht automatisierter Verarbeitung personenbezogener Daten entfällt. Für Unternehmen, die den vorerwähnten Schwellenwert nicht überschreiten, ist damit die Benennung eines Datenschutzbeauftragten auch künftig freiwillig, es sei denn, ihr primärer Geschäftszweck besteht in der Verarbeitung personenbezogener Daten. Unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen ist ein Datenschutzbeauftragter ferner bei solchen Verarbeitungen zu benennen, die einer Datenschutz-Folgenabschätzung (Art. 35 DSGVO) unterliegen oder geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder der Markt- oder Meinungsforschung erfolgen (§ 38 Abs. 1 S. 2 BDSG n. F.).

Anforderungsprofil des Datenschutzbeauftragten

Nach dem bisherigen BDSG muss der Datenschutzbeauftragte die zur Erfüllung seiner Aufgaben erforderliche Fachkunde und Zuverlässigkeit besitzen (§ 4f Abs. 2 BDSG). Zur persönlichen Eignung gehört auch, dass die Tätigkeit als Datenschutzbeauftragter nicht durch andere Aufgaben und Tätigkeiten beeinträchtigt wird. Personalleiter, Mitglieder der Unternehmensleitung oder Leiter der IT-Abteilung dürfen wegen der insoweit üblicherweise bestehenden Interessenskollision nicht zum Datenschutzbeauftragten bestellt werden. Das Unternehmen hat ein Wahlrecht, ob es einen eigenen Arbeitnehmer (interner Datenschutzbeauftragter) oder einen außenstehenden Auftragnehmer (externer Datenschutzbeauftragter) bestellt. Nach der DSGVO und dem BDSG n. F. ergeben sich hinsichtlich

des Anforderungsprofils keine wesentlichen Änderungen. Die DSGVO betont jedoch die Erforderlichkeit des Fachwissens auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis (Art. 37 Abs. 5 DSGVO), was sich aber im Ergebnis mit den bisherigen Anforderungen decken wird. Auch die Wahlmöglichkeit zwischen internem und externem Datenschutzbeauftragten bleibt erhalten (Art. 37 Abs. 6 DSGVO). Es wurde zudem erstmals ausdrücklich normiert, dass eine Unternehmensgruppe einen gemeinsamen Datenschutzbeauftragten ernennen darf, sofern dieser von jeder Niederlassung aus leicht erreicht werden kann (Art. 37 Abs. 2 DSGVO).

Pflichten und Kompetenzen

Der Datenschutzbeauftragte hat nach dem bisherigen deutschen Datenschutzrecht vor allem die Aufgabe, auf die Einhaltung des BDSG und anderer Vorschriften über den Datenschutz hinzuwirken. Dazu gehören die Überwachung der ordnungsgemäßen Anwendung von Datenverarbeitungsprogrammen sowie die Schulung der mit der Verarbeitung betrauten Personen. Darüber hinaus kann sich der Datenschutzbeauftragte in Zweifelsfällen an die Aufsichtsbehörde wenden (§ 4g Abs. 1 BDSG n. F.). Er ist in seiner Amtsführung weisungsfrei und unmittelbar dem Leiter des Unternehmens unterstellt, hat aber keine eigenen Durchsetzungskompetenzen. Nach der DSGVO, deren Vorschriften im BDSG n. F. inhaltsgleich übernommen wurden, treffen den Datenschutzbeauftragten demgegenüber zusätzliche Pflichten. Neben der Unterrichtung und Beratung des Unternehmens sowie der Beschäftigten gehört zu den Aufgaben des Datenschutzbeauftragten insbesondere die Überwachung der Einhaltung der DSGVO und anderer Datenschutzvorschriften sowie der im Unternehmen eingerichteten Strategien für den Schutz personenbezogener Daten (Art. 39 Abs. 1 DSGVO, § 38 Abs. 2 in Verbindung mit § 6 BDSG n. F.). Darüber hinaus fungiert er künftig als Anlaufstelle für die Aufsichtsbehörden. Insgesamt ergibt sich ein deutlich umfangreicheres Aufgabenspektrum. Das hat nach umstrittener Ansicht auch Verschärfungen hinsichtlich einer möglichen Haftung des Datenschutzbeauftragten bei Datenschutzverstößen zur Folge.

Schutz des Datenschutzbeauftragten

Der (interne wie externe) Datenschutzbeauftragte darf nach dem bisherigen deutschen Recht wegen der Erfüllung seiner Aufgaben nicht diskriminiert werden. Die Bestellung zum Datenschutzbeauftragten darf nur aus wichtigem Grund widerrufen werden. Der interne Datenschutzbeauftragte genießt darüber hinaus zusätzlich besonderen Schutz gegen die Kündigung seines Arbeitsverhältnisses. Eine Kündigung ist während der Bestellung und innerhalb eines Jahrs nach der Beendigung der Bestellung nur möglich, wenn Tatsachen vorliegen, die zu einer Kündigung aus wichtigem Grund ohne Einhaltung einer Kündigungsfrist, § 626 Bürgerliches Gesetzbuch (BGB), berechtigen (§ 4f Abs. 3 BDSG n. F.). Die DSGVO sieht lediglich ein Diskriminierungs- und Abberufungsverbot vor, enthält jedoch keine Regelung zum besonderen Kündigungsschutz (Art. 38 Abs. 3 DSGVO). Der deutsche Gesetzgeber hat jedoch die bisherigen Bestimmungen über den Sonderkündigungsschutz des internen Datenschutzbeauftragten in das BDSG nF aufgenommen. Für Unternehmen in Deutschland ändert sich damit am Schutzniveau des Datenschutzbeauftragten letztlich nichts.

Haftung des Datenschutzbeauftragten

Zu den umstrittensten Fragen im Zusammenhang mit den Neuregelungen gehört eine mögliche Haftung des Datenschutzbeauftragten. Zentraler Anknüpfungspunkt für eine denkbare straf- oder ordnungswidrigkeitsrechtliche Haftung des Datenschutzbeauftragten ist die Frage, ob ihn aufgrund seiner Benennung eine sogenannte Garantenpflicht (§ 13 Strafgesetzbuch – StGB), trifft, also eine rechtliche Verpflichtung, aktiv gegen Rechtsverstöße im Unternehmen vorzugehen und diese zu verhindern. Nach bislang ganz herrschender Auffassung zum noch aktuellen BDSG aF besteht eine solche Garantenpflicht für den Datenschutzbeauftragten in der Regel nicht, sodass er bei unterlassenem Einschreiten gegen Rechtsverstöße Dritter bislang grundsätzlich keine straf- oder ordnungswidrigkeitsrechtliche Verfolgung zu befürchten hat bzw. hatte. Nachdem die bisher bestehende Verpflichtung des Datenschutzbeauftragten zum bloßen Hinwirken auf die Einhaltung der Datenschutzbestimmungen durch die DSGVO nun zu einer ausdrücklichen Überwachungsverpflichtung aufgewertet wird, spricht aus rechtlicher Sicht viel dafür, dass den Datenschutzbeauftragten künftig eine Garantenpflicht mit entsprechenden straf- und ordnungswidrigkeitsrechtlichen Haftungsrisiken trifft. Zu beachten ist allerdings, dass die europäischen Datenschutzaufsichtsbehörden eine persönliche Haftung des Datenschutzbeauftragten im Fall der Nichteinhaltung von Datenschutzanforderungen bislang pauschal ablehnen.

Ausblick

Bis zur Klärung der geschilderten Fragestellungen durch die Rechtsprechung ist jedenfalls zu erwarten, dass Datenschutzbeauftragte künftig mehr denn je darauf bedacht sein werden, Unregelmäßigkeiten und Verstöße gegen datenschutzrechtliche Bestimmungen im Unternehmen bereits im Vorfeld zu verhindern und ihre Rolle insgesamt aktiver als bislang interpretieren. Alles in allem werden die Bedeutung des Datenschutzes sowie die Sensibilisierung für die diesbezüglichen Gefahren durch die DSGVO und das BDSG n. F. erheblich verstärkt. ●

THOMAS FAAS

Rechtsanwalt und Fachanwalt für Arbeitsrecht, Partner der auf Arbeitsrecht spezialisierten Sozietät Küttner Rechtsanwälte in Köln, berät nationale und internationale Unternehmen insbesondere zu Fragen des Arbeitnehmerdatenschutzes.

Angriff auf allen Ebenen

Informationssicherheit | Nach einer Studie des Bitkom entstand 2017 der deutschen Wirtschaft durch Spionage, Sabotage und Datendiebstahl ein Schaden von 55 Milliarden Euro. Ein Anteil dessen geht auf sogenanntes Social Engineering zurück, das gezielte Ausspähen und Aushorchen von Menschen.

Autoren: Jennifer Zahl, Stefan Hager, Martina Mendel

Der Mensch ist ein soziales Wesen, deshalb kann jeder zum Ziel eines Social-Engineering-Angriffs werden, im Beruf oder im privaten Bereich. Warum sollte ein Hacker gegen eine starke IT-Schutzmauer anrennen, wenn er an anderer Stelle viel schneller Erfolg hat? Stattdessen kann er sich eine falsche Identität zulegen und zum Beispiel Firmenmitarbeiter aushorchen. Der Angreifer besorgt sich Informationen über Freunde, Bekannte und Arbeitgeber aus sozialen Netzwerken und kombiniert sie dann mit öffentlich zugänglichen Informationen über das genannte Unternehmen. Er belauscht Telefonate im öffentlichen Raum, Unterhaltungen im Taxi, beim privaten Kneipentreffen mit Kollegen, Gespräche auf Messen oder offen zugänglichen Firmenveranstaltungen. Ein starkes Argument dafür, sich hier sehr zurückzunehmen, wenn Unbekannte dabeistehen. Denn viele Gesprächsthemen lassen sich wieder bei einem anderen dazu verwenden, einen vertrauenserweckenden Eindruck zu machen, weil man Insider-Informationen hat. Auch das Mitlesen von E-Mails zählt dazu.

Angriffe dieser Art sind häufig sehr spezialisiert, können sich über lange Zeiträume erstrecken und nutzen menschliche Verhaltensprägungen aus. Dass es sozial erwünscht ist, kooperativ und in Notlagen hilfsbereit zu sein, spielt den Angreifern sehr in die Karten. Auch Stolz auf die eigene Arbeit, Vertrauen in Vorgesetzte oder großer Respekt können eine Motivation sein.

Schwachstelle: autoritäre Chefs, ängstliche Mitarbeiter

Auch Angst ist ein starker Impuls für unüberlegte Handlungen. Sehr gefährdet sind daher Mitarbeiter mit Chefs oder Vorgesetzten, die einen autoritären Führungsstil haben oder oft Druck ausüben. Denn dann neigen Mitarbeiter dazu, nicht kritisch zu hinterfragen, um nicht negativ aufzufallen. Sie sind auch eher bereit zu unüblichen Handlungen, wenn der Angreifer Dringlichkeit im Interesse ihres Chefs vortäuscht. Beim CEO-Fraud wird sogar im Namen des Vorstandsvorsitzenden der Auftrag für eine hohe Geldüberweisung gegeben und auch nachgehakt, ob das erledigt wurde. Wenn ja, wird schnell noch ein weiterer Auftrag nachgeschoben.

USB-Sticks als Köder

Mobile Datenträger wie USB-Sticks scheinen eine unwiderstehliche Anziehungskraft zu haben. In einem Test der Universität Illinois wurden sie auf einen Firmenparkplatz platziert. Es dauerte nur wenige Minuten, bis der erste Stick am System des Finders angesteckt wurde. „Unglaubliche 69 Prozent der Versuchsteilnehmer unternahmen keinerlei Vorkehrungen vor dem Öffnen der Geräte und deren Inhalten“, schreibt das Magazin CIO. „Die Erfolgsrate […] lag erschreckenderweise zwischen 45 und 98 Prozent. […] Lediglich 16 Prozent der unfreiwilligen Probanden sahen es als erforderlich an, den USB-Stick mittels Antivirus-Software zu prüfen. Wäre auf diesen schadhafter Code gewesen, hätte der Cyberangriff in kürzester Zeit zum Erfolg geführt.“

Um die Wahrscheinlichkeit zu erhöhen, dass gefundene USB-Sticks auch eingesteckt werden, bedienen die Angreifer verschiedene Emotionen: Ein USB-Stick mit Plüschtierchen und Schlüsselbund appelliert an die Hilfsbereitschaft. Neugier oder sogar Gier ist schnell geweckt mit dem Aufkleber Vorstandsbudget. Inzwischen ist auch der Aufkleber Bitcoins bei den Kriminellen sehr beliebt.

> Warum sollte ein Hacker gegen eine starke IT-Schutzmauer anrennen, wenn er an anderer Stelle viel schneller Erfolg hat?

E-Zigaretten

Kritisch kann es auch sein, eine E-Zigarette mit dem USB-Anschluss eines Computers zu verbinden, um sie aufzuladen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) warnt davor, dass präparierte Verdampfer auf diesem Weg Malware einschleusen könnten.

Elektronische Karten

Zu Weihnachten oder anderen Anlässen werden gern elektronische Karten mit lieben Grüßen verschickt. Eine gute Gelegenheit für Angreifer, denn die Karten haben verhältnismäßig hohe Klickraten. Die Empfänger klicken die in der Mail angegebenen Links, um die Karte lesen zu können, und der Weg in ihren Computer ist offen. Nächster Termin dafür ist Ostern.

So schützen Sie sich

- Geben Sie keine sensiblen Daten über soziale Netzwerke oder Messenger-Dienste weiter.
- Fordern Sie auch von Mitarbeitern ein striktes Einhalten vereinbarter Regeln zur Datenweitergabe.
- Akzeptieren Sie keine Freundschaftsanfragen, ohne die Person zu prüfen.
- Besprechen Sie keine Firmeninterna oder streng Vertrauliches an einem öffentlichen Ort.
- Verwenden Sie einen Sichtschutz für Ihr Notebook, sobald Sie in einer unsicheren Umgebung vertrauliche Dokumente bearbeiten. Durch das sogenannte Shoulder Surfing gelangen andere sonst leicht an sensible Daten oder Passwörter.
- Jeder einzelne Mitarbeiter kann zum Schutz im sozialen Bereich beitragen, dort, wo keine Firewall und kein Virenschutz helfen. Schulen Sie also Ihre Mitarbeiter, damit sie ein gesundes Misstrauen entwickeln.
- Ermutigen Sie Ihre Mitarbeiter dazu, kritisch zu sein und nachzufragen, wenn ihnen etwas seltsam erscheint – selbst dann, wenn es um einen Auftrag in Ihrem Namen als Chef gehen sollte.
- Klicken Sie nicht auf jeden zugesendeten Link. Bei einem unbekannten Absender sollte man per se vorsichtig sein.

Dubiose Links erkennen

Das eine Merkmal für einen verdächtigen Link gibt es leider nicht. Aber manches kann ein Hinweis sein: Ist der geschriebene Link derselbe wie beim Mouse-over? Wenn nicht, ist das ein Warnsignal. Ist der Link prägnant, wie etwa www.firmenname.de/praesentationen/titel.php, spricht es für einen unverdächtigen Link. Dubios ist dagegen eher ein langer Link mit merkwürdiger Syntax wie www.amazon.kundenservice-fbblgruhgrubrftskdjjfhg.ru/blaarbradhig/nfdhhuerf.html. Aber auch echte Links können lang und komplex aussehen. Wenn man unsicher ist, empfiehlt es sich, beim Absender anzurufen – wenn es ein Kollege, Partner, Bekannter ist – und zu fragen, ob er die Mail geschickt hat. ●

JENNIFER ZAHL, STEFAN HAGER, MARTINA MENDEL
DATEV eG

Quellen: www.bitkom.org (Spionage, Sabotage), www.golem.de (E-Zigaretten), www.cio.de (USB-Sticks)

Sind Sie sicher?

Informationssicherheitsmanagement | Mit einer ISO-27001-Zertifizierung lassen sich zwei Fliegen mit einer Klappe schlagen. Die eigene Organisation und die verwendeten Daten werden geschützt. Gleichzeitig kann die Kanzlei Mandanten und Geschäftspartnern zeigen, dass sie verantwortungsvoll und sicher mit den anvertrauten Daten umgeht.

Autor: Reinhard Muth

Informationssicherheit ist weltweit ein sehr wichtiges Thema, das aufgrund der vielen Angriffe auf die Sicherheitsinfrastruktur und entdeckten Sicherheitslücken in Hardware und Software immer mehr in den Fokus rückt (vgl. Die Lage der IT-Sicherheit in Deutschland 2017, Bundesamt für Sicherheit in der Informationstechnik, BSI). In jüngster Zeit wurde die CPU-Sicherheitslücke von Spectre und Meltdown entdeckt. Die Schwachstellen können unter anderem dazu benutzt werden, sensible Daten aus dem Speicher zu lesen, zum Beispiel private Zertifikatsschlüssel oder Passwörter. Doch muss sich auch eine Durchschnittskanzlei intensiv damit befassen? Eindeutig ja.

Auch bei Kanzleien wurden schon Cyberangriffe festgestellt. Ein Beispiel sind die sehr erfolgreichen Social-Engineering-Angriffe, bei denen Kriminelle viele verschiedene Methoden wie Belauschen, Telefonieren und E-Mails nutzen, um ihre Opfer zu manipulieren und dadurch vertrauliche Informationen zu

erhalten. Die Angreifer versuchen, entweder die Daten der Mandanten zu stehlen, um dann die Kanzlei zu erpressen, oder sie versuchen – angeblich im Auftrag des Chefs –, einen Mitarbeiter zu einer Geldüberweisung zu veranlassen. (Mehr zum Social Engineering lesen Sie im Beitrag Angriff auf allen Ebenen auf Seite 15.)

Geschäftsführer einer Steuerberatungskanzlei sind verantwortlich für die Aufbau- und Ablauforganisation und die strategischen Fragen. In Zeiten zunehmender Cyberangriffe (vgl. BSI-Lagebericht 2017) gehört dazu auch, eine Arbeitsumgebung zu schaffen, die ein hohes Maß an Informationssicherheit garantiert.

Sicherheitsexperten finden

Dazu empfiehlt es sich, Sicherheitsberater oder Experten zurate zu ziehen, um mit ihnen gemeinsam die eigene Organisation zu analysieren, Risiken zu erkennen und zu bewerten, um schließlich ein Sicherheitskonzept zu erstellen und wirkungsvolle Maßnahmen zu planen und umzusetzen. Gute Sicherheitsberater findet man unter anderem über den zentralen IT-Sicherheitsdienstleister des Bunds, dem BSI. Hier kann man Kontakt zu Sicherheitsberatern aufnehmen, die ihre Qualifikation durch eine BSI-Zertifizierung erworben haben und damit ihr Fachwissen nachweisen. Eine andere Option sind zertifizierte Sicherheitsberatungsfirmen. Auch hier haben sich die Berater einer Fachprüfung unterzogen, zum Beispiel als ISO-27001-Auditor.

> Die Informationssicherheit soll zu einem integrierten Bestandteil der täglichen Arbeit werden.

ISO-Norm als Basis

Eine gute Basis für die Analyse der eigenen Aufbau- und Ablauforganisation ist die Norm EN ISO/IEC 27001. Diese internationale Norm für Informationssicherheit beschreibt die Anforderungen für das Einrichten und Realisieren eines dokumentierten Informationssicherheits-Managementsystems ebenso wie die Handhabung und Verbesserung. Sie besteht aus einem Managementteil (Kapitel 4 bis 10) und dem Anhang (A 5 bis A 18).

Im Managementteil sind die Anforderungen an ein Informationssicherheits-Managementsystem beschrieben. Beispielsweise soll der Anwendungsbereich (Scope) definiert werden. Soll sich das Managementsystem auf die gesamte Kanzlei beziehen oder nur auf einen Teilbereich (vgl. Kapitel 4.3 – Festlegen des Anwendungsbereichs des Informationssicherheits-Managementsystems)?

Vertraulichkeit, Verfügbarkeit, Integrität

Welche Ziele verfolgt der Kanzleiinhaber bei der Informationssicherheit? (vgl. Kapitel 6.2 – Informationssicherheitsziele und Planung für deren Erreichung). Meist ist es die Gewährleistung von Vertraulichkeit, Verfügbarkeit und Integrität. Diese Ziele müssen operationalisiert werden: Welche Vertraulichkeitsstufen soll es geben und mit welchen Maßnahmen setzt man die jeweiligen Vertraulichkeitsklassen um (vgl. A 8.2 – Informationsklassifizierung)? Soll es Zutritts- und/oder Zugangsbeschränkungen geben (vgl. A 9.4 – Zugangssteuerung für Systeme und Anwendungen)? Welche Daten dürfen nur verschlüsselt an Dritte weitergegeben werden (vgl. A 10 – Kryptographie)?

Die Forderung nach Verfügbarkeit bezieht sich darauf, wie lange zum Beispiel Server und Clients ausfallen dürfen. Meist sind es nur wenige Stunden täglich. Das muss eine Backup-Strategie berücksichtigen. (Mehr zum Thema Notfallkonzept lesen Sie auf Seite 30.)

Um Integrität zu gewährleisten, spielt die kanzleiinterne Patch- und Zugriffs-Policy eine wichtige Rolle. Welche Patches muss man sofort installieren? Dürfen alle Mitarbeiter auf alle Mandantendaten zugreifen oder welche Daten müssen besonders geschützt werden?

Welche Rollen und Verantwortlichkeiten soll es geben (vgl. Kapitel 5.3 – Rollen, Verantwortlichkeiten und Befugnisse der Organisation)? Bei der Analyse der einzelnen Prozesse sollte man alle Tätigkeiten beschreiben und auf den Wertschöpfungsbeitrag hin untersuchen. Lassen sich Genehmigungsschritte, Kontrollen, Bearbeiterwechsel oder redundante Prozessschritte reduzieren? Oft fällt erst bei der Beschreibung der einzelnen Prozesse auf, dass sich einige Schritte ohne Qualitätsverlust verkürzen ließen. Dass beispielsweise ein elektronischer Prozess nicht mehr ausgedruckt werden muss, um ihn später wieder manuell einzuscannen, wie die Unterschrift des Chefs oder manuelle Dateneingaben.

Umgang mit Risiken und Chancen

Die Norm beschreibt auch, wie man mit Risiken und Chancen umgehen soll (vgl. Kapitel 6 – Maßnahmen zum Umgang mit Risiken und Chancen). Bei der Analyse der kanzleiinternen Prozesse findet man in der Regel auch einige Risiken, die die Zielerreichung der Prozesse verhindern könnten. Die Risiken werden nach Eintrittswahrscheinlichkeit und Schadenshöhe klassifiziert. Das BSI hat 47 elementare Gefährdungen beschrieben, die auf ihr Risiko untersucht werden sollen. Beispiel Feuer (G 01): Es kommt häufig vor, dass elektrische Kleingeräte, wie Kaffeemaschinen oder Tischleuchten, unsachgemäß installiert oder aufgestellt sind und dadurch Brände verursachen. Beispiel Verschmutzung, Staub, Korrosion (G 04): Handwerkliche Tätigkeiten können viel Staub verursachen, der bei fehlendem Schutz durch die Lüftungsschlitze in ein

PC-Gehäuse eindringen kann und das Netzteil unbrauchbar macht.
Mit der Umsetzung der Sicherheitsanforderungen (den sogenannten Controls) in Anhang A ist jedes Unternehmen, egal welcher Größe, gegen mögliche Angriffe gut geschützt.
Anhand der Ergebnisse der Risikoanalyse lässt sich ein Sicherheits- oder Notfallkonzept erarbeiten, das die gefundenen Risiken auf ein für die jeweilige Kanzlei akzeptables Maß reduzieren lässt sowie Kosten und Nutzen abwägt. Ein solches Konzept fordert auch die Norm im Control A 5-Informationssicherheitsrichtlinien (mehr dazu auch im Beitrag Nummer sicher auf Seite 30.)
Ebenso wichtig wie die technische Seite ist die menschliche. Die Informationssicherheit soll zu einem integrierten Bestandteil der täglichen Arbeit werden. Daher ist die Schulung und Sensibilisierung der Mitarbeiter ein zentrales und wichtiges Ziel. Hierfür eignen sich jährlich stattfindende Präsenzschulungen und auch Wirksamkeitstests im Alltag.

Jährlich oder anlassbezogen überprüfen

Haben sich in letzter Zeit die IT-Systemlandschaft oder wesentliche Teile der Organisation geändert oder ist die Eintrittswahrscheinlichkeit eines Risikos gestiegen oder gesunken, so sind das Sicherheitskonzept und die damit verbundenen Sicherheitsmaßnahmen an die neue Situation anzupassen. Hilfestellung bietet hier der Anhang der ISO 27001 mit Themen wie:

- Personalsicherheit (zum Beispiel Informationssicherheitsbewusstsein, -ausbildung und -schulung)
- Zugangssteuerung (zum Beispiel Verschlüsselung, Zugangssteuerung für Systeme und Anwendungen)
- Betriebssicherheit (zum Beispiel Schutz vor Schad-Software oder Datensicherung)
- Kommunikationssicherheit (zum Beispiel Netzwerksicherheit)

Für die Zertifizierung der Kanzlei nach ISO 27001 ist es notwendig, alle Sicherheitsanforderungen der Norm umzusetzen. Viele wichtige Punkte wurden hier genannt, es fehlen jedoch insbesondere noch die internen Audits und die Managementbewertung (vgl. Kapitel 9.2 – Internes Audit). Die regelmäßigen internen Audits sollen prüfen, ob alle Maßnahmen des Sicherheitskonzepts umgesetzt sind und auch gelebt werden. Das Ergebnis dieser Audits ist dann Bestandteil der Managementbewertung (vgl. Kapitel 9.3 – Managementbewertung). Dabei bewertet die Kanzleileitung alle Aspekte der Informationssicherheit, um ihre Eignung, Angemessenheit und Wirksamkeit sicherzustellen. Mit der Umsetzung aller empfohlenen und selbst definierten Sicherheitsanforderungen steht einer Zertifizierung nach ISO 27001 nichts mehr im Wege. ●

REINHARD MUTH
DATEV eG, Bereich Managementsysteme und Rechteprüfung

MEHR DAZU

finden Sie auf der Internet-Seite des Bundesamts für Sicherheit in der Informationstechnik: **www.bsi.bund.de**

ISO 27001-Zertifikate auf der Basis von IT-Grundschutz

Die Lage der IT-Sicherheit in Deutschland 2017

Berufsständische Versorgungseinrichtungen

Steuerfreie Beitragserstattung

Die Erstattung von Pflichtbeiträgen zu einer berufsständischen Versorgungseinrichtung ist unabhängig von einer Wartefrist nach dem Ende der Beitragspflicht steuerfrei. Das hat der Bundesfinanzhof zu § 3 Nr. 3 Buchst. c des Einkommensteuergesetzes (EStG) entgegen der Auffassung des Bundesministeriums der Finanzen entschieden. (BFH, X R 3/17, www.datev.de/lexinform/0447856).

Da sich der Rechtsstreit nur auf den Veranlagungszeitraum 2013 bezog, musste der BFH die Frage offenlassen, ob die Beitragsrückerstattung zu einer Kürzung des Sonderausgabenabzugs in den Jahren führt, in denen der Kläger Pflichtbeiträge zum berufsständischen Versorgungswerk geleistet hat.

Steuerhinterziehung

Verlängerte Festsetzungsfrist

Bundesfinanzhof, VIII-R-32/15

Die Festsetzungsfrist aufgrund einer Steuerhinterziehung verlängert sich bei einem Erbfall auch dann, wenn der demenzerkrankte Erblasser ausländische Kapitaleinkünfte nicht erklärt, jedoch ein Miterbe von der Verkürzung der Einkommensteuer wusste und selbst eine Steuerhinterziehung begeht.

Die Verlängerung der Festsetzungsfrist auf zehn Jahre wirkt dabei auch zu Lasten des Miterben, der von der Steuerhinterziehung keine Kenntnis hat, so der Bundesfinanzhof (BFH, VIII R 32/15, www.datev.de/lexinform/0447795).

Umsatzsteuer

Erstattungsbetrag bei Änderung einer rechtswidrigen Umsatzsteuerfestsetzung

Ändert das Finanzamt zugunsten des Steuerpflichtigen eine von Anfang an rechtswidrige Umsatzsteuerfestsetzung und führt dies zu einem Erstattungsbetrag, so sind Erstattungszinsen festzusetzen.

FG BW, 12-K-2324/17, www.datev.de/lexinform/0447845

Einkommensteuer/Lohnsteuer

Beachtung des Internationalen Privatrechts auch im Steuerrecht

Gerichte dürfen Verträge, die ausländischem Recht unterliegen, nicht nach deutschem Recht auslegen. Sie müssen daher nicht nur die ausländischen Rechtsnormen, sondern auch deren Anwendung in der Rechtspraxis ermitteln und haben hierfür ggf. einen Sachverständigen hinzuzuziehen.

BFH, IV-R-23/14, www.datev.de/lexinform/0447857

Kosten eines privaten Sicherheitsdienstes

Die Kosten für die Beauftragung eines privaten Sicherheitsdienstes führen zu außergewöhnlichen Belastungen, wenn die Aufwendungen notwendig und angemessen sind, um eine Gefahr für Leib und Leben abzuwehren.

FG Münster, 13-K-1045/15-E, www.datev.de/lexinform/0447829

Kein Werbungskostenabzug bei Auslandsstudium

Eine an einer deutschen Hochschule eingeschriebene Studentin kann für Zeiträume von Auslandssemestern und Auslandspraktika keine Aufwendungen für die dortige Unterkunft und Verpflegung geltend machen kann, wenn sie im Inland keinen eigenen Hausstand unterhält.

FG Münster, 7-K-1007/17-E, www.datev.de/lexinform/0447828

Keine Tarifbegünstigung für nicht entnommene Verschmelzungsgewinne

Bei nicht entnommenen Gewinnen nach § 34a EStG für außerbilanziell hinzuzurechnende Ergebnisse aus der Verschmelzung einer GmbH auf eine KG gilt keine Tarifbegünstigung.

FG Münster, 3-K-1256/15-F, www.datev.de/lexinform/0447830

Arbeitsrecht

Altersabstandsklausel bei der Hinterbliebenenversorgung

Erhalten Ehegatten nur dann eine Hinterbliebenenversorgung, wenn sie nicht mehr als 15 Jahre jünger sind als der Versorgungsberechtigte, liegt darin keine gegen das Allgemeine Gleichbehandlungsgesetz (AGG) verstoßende Diskriminierung aufgrund des Alters.

BAG, 3-AZR-43/17, www.datev.de/lexinform/0447853

Kündigung wegen des Antritts einer Freiheitsstrafe

Arbeitgeber können das Beschäftigungsverhältnis mit einem Arbeitnehmer kündigen, wenn dieser eine Freiheitsstrafe von mehr als zwei Jahren zu verbüßen hat und eine vorzeitige Entlassung nicht sicher erwartet werden kann.

LAG Hessen, 8-Sa-146/17, www.datev.de/lexinform/0447812

Erbrecht

Pflichtteilsansprüche des Enkels nach Enterbung des Sohns

Enterbt der Großvater nur seinen Sohn und vererbt er sein Vermögen anderen Erben, kann dem Enkel ein Pflichtteils- und Pflichtteilsergänzungsanspruch zustehen.

OLG Hamm, 10-U-31/17, www.datev.de/lexinform/0447783

Sonstiges Recht

Grundstückseigentümer für beauftragte Handwerker voll verantwortlich

Grundstückseigentümer, die einen Handwerker Reparaturarbeiten am Haus vornehmen lassen, sind gegenüber Nachbarn verantwortlich, wenn das Haus infolge der Arbeiten in Brand gerät und das Nachbargrundstück dabei beschädigt wird. Auch dass der Handwerker sorgfältig ausgesucht wurde, ändert daran nichts.

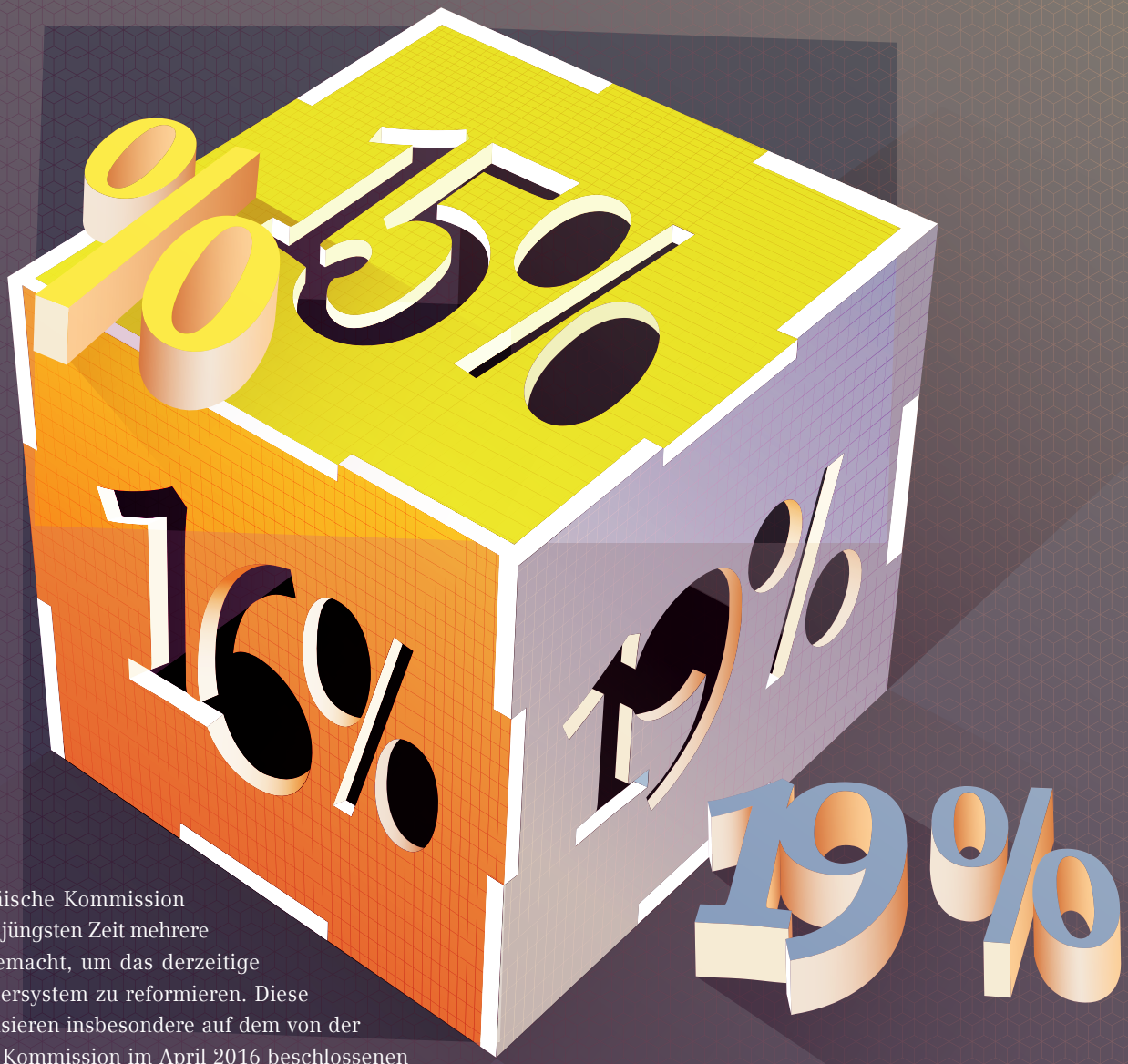
BGH, V-ZR-311/16, www.datev.de/lexinform/0447814

Fotos: alashi, RedlineVector/Getty Images

Es muss passen

Gesetzesinitiative | Die Europäische Kommission hat dem Mehrwertsteuerbetrug den Kampf angesagt und will zudem die Regelungen für grenzüberschreitend tätige Unternehmen vereinfachen.

Autor: Christian Mozelewski



Die Europäische Kommission hat in der jüngsten Zeit mehrere Vorschläge gemacht, um das derzeitige Mehrwertsteuersystem zu reformieren. Diese Vorschläge basieren insbesondere auf dem von der Europäischen Kommission im April 2016 beschlossenen sogenannten Mehrwertsteueraktionsplan – Auf dem Weg zu einem einheitlichen europäischen Mehrwertsteuerraum: Zeit für Reformen. Vier grundlegende Prinzipien sollen als Eckpfeiler eines neuen endgültigen und gemeinsamen EU-Mehrwertsteuerraums vereinbart werden. Im Dezember letzten Jahrs hat der EU-Ministerrat bereits erste Vereinfachungen der Mehrwertsteuerregelungen für grenzüberschreitend tätige Online-Unternehmen beschlossen, die schrittweise bis 2021 in Kraft treten sollen.

Hintergrund

Seit Langem setzt sich die Europäische Kommission für eine Reform des Mehrwertsteuersystems ein. Das ist auch dringend erforderlich, da die letzte Novellierung im Jahr 1993 bereits mehr als ein Vierteljahrhundert zurückliegt. Durch die geplanten

Neuregelungen soll das Mehrwertsteuersystem für die Regierungen und Unternehmer nicht nur verbessert, sondern auch modernisiert werden. Den Mitgliedstaaten gehen allein durch den grenzüberschreitenden Mehrwertsteuerbetrug jährlich Einnahmen in Höhe von 50 Milliarden Euro verloren; Einnahmen, die für den Bau und die Modernisierung von Schulen, Straßen und Krankenhäusern genutzt werden könnten. Des Weiteren stellen die derzeitigen Mehrwertsteuerregelungen vor allem ein Hemmnis für den grenzüberschreitenden Handel insbesondere von kleineren und mittleren Unternehmen dar. Die EU-Kommission hat hierzu berechnet, dass Unternehmen, die grenzüberschreitenden Handel treiben, derzeit rund elf Prozent höhere Kosten für die Einhaltung der Vorschriften haben als Unternehmen, die nur im Inland tätig sind.

Inhalte der Reform

Zunächst einmal geht es um die Bekämpfung des Mehrwertsteuerbetrugs als eines der zu vereinbarenden vier Grundprinzipien. Künftig soll die Mehrwertsteuer beim grenzüberschreitenden Handel zwischen Unternehmen erhoben werden. Derzeit ist dieser Handel unter gewissen Voraussetzungen von der Mehrwertsteuer befreit, was jedoch dazu führt, dass kriminelle Unternehmen die Umsatzsteuer vereinnahmen, jedoch nicht abführen. Die Einführung einer zentralen Anlaufstelle soll dazu dienen, dass Unternehmer bei einem einzigen Online-Portal in der eigenen Sprache Erklärungen abgeben und Zahlungen durchführen können. Die Mehrwertsteuer wird dann an die jeweiligen Mitgliedstaaten weitergeleitet, wie das bereits bei den elektronischen Dienstleistungen (sogenannten Mini-One-Stop-Shop-Verfahren) der Fall ist. Geplant ist auch die Umstellung auf das sogenannte Bestimmungslandprinzip, wonach die Mehrwertsteuer stets an den Mitgliedstaat des Endverbrauchers entrichtet wird, und zwar mit dem Mehrwertsteuersatz, der in diesem Mitgliedstaat gilt. Die derzeitigen Mehrwertsteuervorschriften sollen zudem vereinfacht werden und damit zu einem Abbau der Bürokratie führen. Beabsichtigt ist, dass der Verkäufer beim grenzüberschreitenden Handel die Rechnung nach den Vorschriften seines Heimatlandes erstellen kann sowie keine zusammenfassende Meldung an sein Finanzamt mehr abgeben muss.

> Künftig soll die Mehrwertsteuer beim grenzüberschreitenden Handel zwischen Unternehmen erhoben werden.

Bekämpfung des Mehrwertsteuerbetrugs

Darüber hinaus hat die Europäische Kommission Instrumente zur Bekämpfung des Mehrwertsteuerbetrugs vorgeschlagen. Als wichtigste Maßnahmen sind die Stärkung der Zusammenarbeit zwischen den Mitgliedstaaten, die Zusammenarbeit mit den Strafverfolgungsbehörden, der Austausch wichtiger Informationen über die Einfuhren in die Europäische Union sowie der Austausch von Informationen über Fahrzeuge zu nennen. Nach Aussage des EU-Kommissars für Wirtschafts- und Finanzangelegenheiten, Steuern und Zoll, Pierre Moscovici, „wird beispielsweise Eurofisc, das EU-Expertennetzwerk für die Betrugsbekämpfung, Zugang zu den Fahrzeugzulassungsdaten anderer Mitgliedstaaten erhalten. Dadurch wird dem Mehrwertsteuerbetrug im Zusammenhang mit Gebrauchtwagen – einer der am weitesten verbreiteten Betrugsarten – ein Ende gesetzt."

Flexiblere Mehrwertsteuersätze

Mit den am 18. Januar 2018 vorgelegten Vorschlägen will die Europäische Kommission den Mitgliedstaaten mehr Flexibilität bei der Festlegung der Mehrwertsteuersätze einräumen. Nach Ansicht der Europäischen Kommission sind die derzeitigen Mehrwertsteuervorschriften nicht nur nicht mehr zeitgemäß, sondern auch zu unflexibel. Mit ihren Vorschlägen kommt die Europäische Kommission daher ihrer Zusage gegenüber den Mitgliedstaaten nach, ihnen mehr Spielraum bei den Mehrwertsteuersätzen zuzugestehen. Diese Vorschläge lassen sich wie folgt zusammenfassen: Neben einem weiterhin geltenden Mehrwertsteuermindestsatz in Höhe von 15 Prozent könnten die Mitgliedstaaten dann

- zwei ermäßigte Steuersätze zwischen fünf Prozent und dem vom Mitgliedstaat gewählten Normalsatz,
- eine Mehrwertsteuerbefreiung (Nullsatz) sowie
- einen ermäßigten Mehrwertsteuersatz zwischen null Prozent und dem ermäßigten Satz festlegen.

Die derzeitige Liste von Gegenständen und Dienstleistungen, bei denen die Anwendung ermäßigter Steuersätze infrage kommt, soll durch eine Liste von Gütern, wie zum Beispiel Waffen, alkoholische Getränke, Glücksspiele und Tabak, ersetzt werden, auf die stets der Normalsatz von 15 Prozent oder ein höherer Satz angewendet werden müsste.

Vereinfachungen für Kleinunternehmen

Ebenfalls am 18. Januar 2018 hat die Europäische Kommission Vorschläge zur Verbesserung der steuerlichen Bedingungen für Kleinunternehmen vorgelegt. Nach den derzeitigen Regelungen der jeweiligen Mitgliedstaaten können von Kleinunternehmen getätigte Verkäufe von der Mehrwertsteuer befreit beziehungsweise nicht erhoben werden, wenn diese einen bestimmten Jahresumsatz nicht übersteigen. Problematisch ist, dass die jeweiligen nationalen Regelungen für eine Steuerbefreiung nur den inländischen Unternehmen zur Verfügung stehen. Hierdurch bestehen keine einheitlichen Wettbewerbsbedingungen innerhalb der Europäischen Union für Kleinunternehmen. Die dazu ergan-

genen Vorschläge der Europäischen Kommission zur Vereinfachung für Kleinunternehmen sehen neben der Beibehaltung der derzeitigen Schwellenwerte für Steuerbefreiungen Folgendes vor:

- einen EU-weiten Umsatzschwellenwert von zwei Millionen Euro, der bis zu dem Vereinfachungsmaßnahmen für alle – steuerbefreiten und nicht steuerbefreiten – Kleinunternehmen anwendbar ist
- die Möglichkeit, dass die Mitgliedstaaten alle Kleinunternehmen, die für eine Mehrwertsteuerbefreiung infrage kommen, von ihren Pflichten im Hinblick auf Registrierung, Rechnungstellung, Aufzeichnung und Mitteilung befreien
- einen Umsatzschwellenwert von 100.000 Euro, der Unternehmen, die in mehr als einem Mitgliedstaat tätig sind, ermöglichen würde, die Mehrwertsteuerbefreiung in Anspruch zu nehmen

Weiteres Vorgehen

Die Vorschläge der Europäischen Kommission werden nun den Mitgliedstaaten im Rat der Europäischen Union (EU-Ministerrat) zur Zustimmung sowie dem Europäischen Parlament zur Stellungnahme vorgelegt. Zudem will die Europäische Kommission noch in diesem Jahr einen detaillierten Vorschlag zu Änderung der Mehrwertsteuerrichtlinie auf technischer Ebene vorlegen, sodass die vorgeschlagenen Regelungen auch reibungslos umgesetzt werden können.

Beschlossene Regelungen für Online-Unternehmen

Der EU-Ministerrat hat bereits im Dezember vergangenen Jahrs Regelungen beschlossen, die das Mehrwertsteuersystem für grenzüberschreitend tätige Online-Unternehmen in der Europäischen Union vereinfachen sollen. Die Regelungen sollen schrittweise bis 2021 in Kraft treten. Bereits ab 1. Januar 2019 gelten Regelungen, die bestimmte Unternehmen, die online Waren in andere EU-Mitgliedstaaten verkaufen, entlasten sollen. Für Kleinstunternehmen mit einem grenzüberschreitenden Umsatz unter 10.000 Euro richtet sich dann die Mehrwertsteuer nach deren Ansässigkeitsstaat. Für kleinere und mittlere Unternehmen, die grenzüberschreitende Verkäufe im Wert von bis zu 100.000 Euro pro Jahr erbringen, werden einfachere Verfahren gelten. Zudem sollen künftig alle Unternehmen, die grenzüberschreitend Waren an Kunden verkaufen, ihren EU-Mehrwertsteuerpflichten über ein einheitliches nutzerfreundliches Online-Portal in ihrer Landessprache nachkommen können. Eine komplizierte Registrierung in dem jeweiligen EU-Mitgliedstaat soll damit entfallen. Die einzige Anlaufstelle für Online-Verkäufe von Waren soll 2021 einsatzbereit sein. Die Mitgliedstaaten haben bis dahin Zeit, die hierfür erforderlichen technischen Voraussetzungen zu schaffen beziehungsweise zu aktualisieren.

Fazit

Die von der Europäischen Kommission vorgelegten Vorschläge sowie die bereits im Dezember vergangenen Jahrs vom EU-Ministerrat beschlossenen Mehrwertsteuerregelungen sind wichtige Schritte in die richtige Richtung. Neben der Bekämpfung des Mehrwertsteuerbetrugs muss es vor allem um die Vereinfachung von Regelungen insbesondere für grenzüberschreitend tätige Unternehmen gehen. Das ist enorm wichtig, um das Ziel eines gemeinsamen, einheitlichen EU-Mehrwertsteuerraums zu erreichen, in dem es keinen Unterschied macht, ob die Waren im Inland oder über die nationalen Grenzen verkauft werden. ●

CHRISTIAN MOZELEWSKI

Steuerberater und Rechtsanwalt bei der Berliner Wirtschaftsprüfungs- und Steuerberatungsgesellschaft Crowe Horwath Trinavis, berät regelmäßig Unternehmen in internationalen Steuerfragen

Schritte mit Bedacht

Steuerliche Beratung | Die Grenze zwischen erlaubter Gestaltung und strafbarem Verhalten ist häufig fließend – mit der Folge, dass der Steuerberater leicht zum Täter oder Teilnehmer einer Steuerstraftat werden kann.

Autoren: Thorsten Stielow und Anja Reichling

Jeder, der steuerlich beratend tätig ist, kennt die Situation, dass die Vorstellungen des Mandanten zur Senkung von Steuern mit den steuerrechtlich zur Verfügung stehenden Möglichkeiten nicht in Übereinstimmung zu bringen sind. In dieser Situation gilt es für den Berater im Interesse des Mandanten, die Grenzen des Möglichen klar aufzuzeigen. Das liegt aus straf-, berufs- und haftungsrechtlichen Gründen auch im ureigenen Interesse des Beraters. Steuerberater haben die Pflicht, ihre Mandanten umfassend zu beraten und ungefragt über alle bedeutsamen steuerlichen Einzelheiten und deren Folgen zu unterrichten (vgl. BGH, Urteil vom 20.02.2003 – IX ZR 384/99).

Ausgangssituation

Grundlage der steuerlichen Beratung und damit die Begrenzung des Umfangs der steuerlichen Beratungspflichten bildet der jeweilige Beratungsvertrag. Der Steuerberater kann sich jedoch nicht allein auf die Beschränkung seines Auftrags berufen, da er im Rahmen des Mandatsverhältnisses auch Hinweispflichten zur eventuellen Gefahr der Entstehung von Steuern und anderen Abgaben sowie den damit verbundenen Rechtsfolgen unterliegt (vgl. OLG Köln, Urteil vom 16.01.2014 – 8 U 7/13, rechtskräftig). Zunächst ist der sicherste Weg zum erstrebten steuerlichen Ziel aufzuzeigen und mittels sachgerechter Vorschläge dessen Verwirklichung darzustellen. Sind verschiedene steuerrechtliche Wege mit unterschiedlichen Vor- und Nachteilen gangbar, sind dem Auftraggeber für dessen Entscheidungsfindung auch die mit ihnen verbundenen Rechtsfolgen aufzuzeigen (vgl. BGH, Urteil vom 16.10.2003 – IX ZR 167/02; Urteil vom 09.01.1996 – IX ZR 103/95). Gefälligkeitsgestaltungen verbieten sich generell, da der Steuerberater verpflichtet ist, seinen Mandanten davor zu bewahren, sich durch Überschrei-

Fotos: mediaphotos/ Getty Images

tung des zulässigen Rahmens der steuerstrafrechtlichen Verfolgung auszusetzen (vgl. BGH, Urteil vom 14.11.1996 – IX ZR 215/95). Wann die Grenze der Tätigkeit des Steuerberaters zu strafbarem Verhalten für seinen Mandanten oder ihn selbst überschritten ist, kann selbst im Einzelfall nicht immer klar bestimmt werden (Sieja, DStR 2012, S. 991ff.). Sicher ist nur, dass der Berater im Spagat zwischen Berufspflichten und Mandanteninteressen gelegentlich an seine Grenzen kommt.

Neue Transparenzvorschriften

Das kann künftig noch mehr an Bedeutung gewinnen. So kommen die am 21. Juni 2017 veröffentlichten Pläne der Europäischen Kommission zu neuen Transparenzvorschriften für Intermediäre, die potenziell schädliche steuerliche Gestaltungen entwickeln oder vermarkten, und ein durch den damaligen Bundesfinanzminister im Juli 2015 in Auftrag gegebenes Gutachten des Max-Planck-Instituts für Steuerrecht und Öffentliche Finanzen zu dem Schluss, dass eine Anzeigepflicht von Steuergestaltungen sowohl mit dem Grundgesetz als auch mit dem EU-Recht vereinbar wäre und auch ein taugliches Mittel zur Förderung steuerlicher Belastungsgleichheit darstelle. Wie sich entsprechende Gesetzesänderungen auf das Mandatsverhältnis und die strafrechtliche Verantwortung des Steuerberaters auswirken, hängt sicherlich im Detail von deren konkreter Ausgestaltung ab. Da (vermeintliche) Verfehlungen im Steuer(straf)recht in der jüngsten Vergangenheit häufig von einer eher emotionalen als sachlichen Berichterstattung und öffentlichen Diskussion getragen wurden und in Zusammenhang mit den Panama- oder Paradise-Papers der ungehemmte Ruf nach Steuergerechtigkeit und schonungsloser Strafverfolgung laut wird, bleibt zu hoffen, dass der Gesetzgeber mit Augenmaß tätig wird. Aber auch jetzt schon können Steuerberater in Steuerstraftaten oder Steuerordnungswidrigkeiten involviert sein. Die Rolle, die sie dabei einnehmen können, hängt vom Einzelfall ab. Sie können Täter, Mittäter oder als Anstifter beziehungsweise Gehilfe auch Teilnehmer an einer Steuerstraftat sein. Daneben oder auch gleichzeitig können Steuerberater Verteidiger oder Zeuge sein.

Der Steuerberater als Täter

Obwohl es zunächst merkwürdig anmutet, kann der Steuerberater aufgrund der weiten Formulierung des § 370 Abs. 1 Satz 1 Abgabenordnung (AO nicht nur in eigener Sache Täter einer Steuerhinterziehung sein.

Er kann als Mittäter in Betracht kommen. Mittäter (§ 25 Abs. 2 Strafgesetzbuch (StGB) ist nach der Rechtsprechung des BGH (vgl. Urteil vom 30.06.2005 – 5 StR 12/05) nicht nur, wer fremdes Tun fördert, sondern auch derjenige, der einen eigenen Tatbeitrag als Ergänzung in eine gemeinschaftliche Tat einfügt. Dabei sind unter objektiven beziehungsweise subjektiven Gesichtspunkten Kenntnis, Willen und ein eigenes Interesse am Taterfolg mögliche Abgrenzungskriterien (vgl. BFH, Urteil vom 19.12.2002 – IV R 37/01). Geht man davon aus, dass bereits das Honorarinteresse des Steuerberaters zur Bejahung eines mittäterschaftlichen Eigeninteresses führen kann (vgl. Finanzgericht München, Beschluss vom 28.09.2009 – 1 V 1824/09; BGH, Urteil vom 24.08.1983 – 3 StR 89/83), bliebe als wesentliches Entlastungskriterium nur noch die Unkenntnis des Steuerberaters. Vor dem Hintergrund, dass die Tat dem Angeklagten nicht nachgewiesen werden muss, weil nach § 261 Strafprozessordnung (StPO) das Gericht lediglich nach freier Überzeugung entscheidet, scheint ein bloßes Bestreiten mit Nichtwissen für eine fachlich vorgebildete Person und Berufsträger im Steuerstrafverfahren nur wenig erfolgversprechend.

Der Steuerberater als Teilnehmer

Der Steuerberater kann unter (steuer-)strafrechtlichen Gesichtspunkten sowohl als Anstifter (§ 26 StGB) als auch Gehilfe (§ 27 StGB) Teilnehmer an einer Steuerstraftat sein. Der Steuerberater als Anstifter hat in der Praxis wegen der Abgrenzung zur Mittäterschaft Bedeutung. Anstifter ist, wer bei einer anderen Person, die nicht bereits zur Tat entschlossen war, vorsätzlich einen Tatentschluss zu einer vorsätzlich zu begehenden Tat hervorruft und will, dass die Haupttat begangen wird (doppelter Vorsatz). Im Rahmen der Gestaltungsberatung, also für den Fall der Gestaltung potenziell schädlicher steuerlicher Gestaltungen, ist anhand dieser Kriterien zu prüfen, ob Mittäterschaft oder Anstiftung vorliegt. War der Täter bereits vor der Beratung zur Tat entschlossen, scheidet eine Anstiftung aus. Der Steuerberater kann auch als Gehilfe an der Tat des Steuerstraftäters teilnehmen. Als strafbare Hilfeleistung ist dabei grundsätzlich jede Handlung anzusehen, welche die Herbeiführung des Taterfolgs des Haupttäters objektiv fördert, ohne dass sie für den Erfolg selbst ursächlich sein muss (ständige Rechtsprechung; vgl. unter anderem BGH, Urteil vom 20.12.1955 – 5 StR 363/55). Ausreichend hierfür ist, dass die Hilfe an sich geeignet ist, die fremde Haupttat zu fördern oder zu erleichtern, und der Hilfeleistende das weiß. Der Gehilfe kann sich auch nicht dadurch retten, dass er ausdrücklich erklärt, er missbillige die Haupttat (vgl. BGH, Urteil vom 01.08.2000 – 5 StR 624/99). Im Hinblick auf eine eventuelle Strafbarkeit des Steuerberaters wegen Beihilfe bedeutet dies, dass er einen Taterfolg lediglich für möglich halten oder billigend in Kauf nehmen muss. Mangels vorsätzlicher Haupttat scheidet allerdings eine Beihilfe zur leichtfertigen Steuerverkürzung (§ 378 AO) aus und ist nicht strafbar. Gleichwohl besteht unter bestimmten Voraussetzungen ein haftungsrechtliches Schadenersatzrisiko, etwa für eine gegen den Mandanten festgesetzte Geldbuße.

Sicht der Literatur und Rechtsprechung

Im Hinblick auf die verfassungsrechtlich gewährleistete Berufsausübung ist bei der Frage der Strafbarkeit des Steuerberaters zu prüfen, ob er sogenannte neutrale/berufstypische Handlungen vorgenommen hat. In Abgrenzung zur strafbaren Beihilfe werden die Kriterien in Literatur und Rechtsprechung kontrovers diskutiert, wobei hier lediglich auf die Auffassung des BGH (vgl. BGH, Urteil vom 01.08.2000 – 5 StR 624/99; Urteil vom 22.01.2014 – 5 StR 468/12) eingegangen werden soll.

Die höchstrichterliche Rechtsprechung stellt vorwiegend auf die subjektive Seite ab, wonach sich der Gehilfe strafbar macht, der um die Haupttat sicher weiß, während der zweifelnde Gehilfe grundsätzlich straflos bleibt, es sei denn, er fördert einen erkennbar Tatgeneigten. Zudem sei der Gehilfe, der durch alltägliche Handlungen eine vorsätzliche rechtswidrige Haupttat fördere, von der Haupttat aber nicht sicher wisse, erst dann strafbar, wenn Umstände gegeben seien, die es sehr wahrscheinlich machen, dass es zu dieser Tat kommen wird. Für den Steuerberater führt das zu dem wenig schmeichelhaften Ergebnis, dass ihn im Ernstfall nur Nichtwissen vor dem strafrechtlichen Vorwurf einer Beihilfe schützt. Vor allem, wenn Gegenstand der Steuerberaterleistung eine Gestaltungsberatung war, der umfangreiche Sachverhaltsermittlungen vorangegangen sind, oder bei einfachen Sachverhalten dürfte in der Praxis das erforderliche Wissen häufig vermutet werden.

> Steuerberater können Täter, Mittäter oder als Anstifter beziehungsweise Gehilfe auch Teilnehmer einer Steuerstraftat sein.

Anlagen mit Sachverhaltserläuterungen

Insoweit gibt es auch eine Gratwanderung des Steuerberaters, die etwa bei der Erstellung von Steuererklärungen zu bewältigen ist. Da in Steuererklärungsformularen für Sachverhaltsangaben regelmäßig kein Raum ist und lediglich Zahlen in ein Formular eingetragen werden, wird nach außen nicht erkennbar, wie der Steuerberater den zugrundeliegenden Sachverhalt unter eine Rechtsnorm subsumiert hat. So könnte auch die Gefahr bestehen, dass durch Anwendung einer falschen Rechtsauffassung eine Steuerstraftat begangen wird. Zwar ist im Zweifel nicht jede von der Finanzverwaltung abweichende Rechtsauffassung, die ihren Niederschlag in einer Steuererklärung findet, strafrechtlich relevant. In der Praxis ist die Grenze jedoch wohl dann überschritten, wenn Angaben in einer Steuererklärung auf unvertretbaren Rechtsauffassungen beruhen. Aus Vorsichtsgründen scheint es deswegen inzwischen Praxis zu sein, bei Zweifeln entsprechende Anlagen zu Steuererklärungen mit Sachverhaltserläuterungen beizufügen.

Steuerberater als Verteidiger oder Zeuge

Der steuerliche Berater darf auch als alleiniger Verteidiger seines Mandanten im Strafverfahren, das durch die Finanzbehörde selbstständig geführt wird, unter Beachtung der Voraussetzungen des § 392 AO tätig werden. Ob dies in Fällen, in denen er im Rahmen seiner bisherigen Tätigkeit bereits involviert war, sinnvoll ist, sollte einzelfallabhängig entschieden werden. Nur in den seltensten Fällen wird das tatsächlich zu bejahen sein. Während in der Literatur mögliche Kostenvorteile für den Mandanten aufgrund der Vorbefassung des Steuerberaters diskutiert werden, sollte nicht unbeachtet bleiben, dass der Steuerberater selbst in den Verdacht geraten kann, Tatbeteiligter zu sein. Die daraus entstehenden potenziellen Interessenkonflikte dürften regelmäßig eine Tätigkeit als Verteidiger ausschließen und auch mögliche Kostenvorteile relativieren. Neben der häufig fehlenden Erfahrung des Steuerberaters, die ein Tätigwerden als Verteidiger ausschließt, endet seine (Allein-)Verteidigungsbefugnis ohnehin, wenn sich ein Gericht mit der Strafsache befasst oder er als (Entlastungs-)Zeuge in Betracht kommt und dem Berater somit die Teilnahme an der Hauptverhandlung verwehrt ist.

Fazit

Abschließend ist darauf hinzuweisen, dass der Steuerberater aufgrund der Komplexität des Steuerrechts und der sich verstärkenden öffentlichen Ablehnung einzelner (teilweise legaler) Steuergestaltungen stets auch besondere Aufmerksamkeit auf das Steuerstrafrecht wie auch die haftungs- und berufsrechtliche Normen richten sollte. Eine Dokumentation des Mandantenauftrags, des zugrunde liegenden Sachverhalts sowie dessen rechtliche Beurteilung sollte nicht nur vor dem strafrechtlichen Hintergrund und möglicher Gesetzgebungsvorhaben selbstverständlich sein. Auch ein klares und entschiedenes Verhalten bei gefahrgeneigten Mandaten wird den Steuerberater nicht nur vor eigenen strafrechtlichen Konsequenzen schützen können. ●

THORSTEN STIELOW
Diplom-Finanzwirt, Steuerberater, CPA
ANJA REICHLING
Rechtsanwältin (Syndikusrechtsanwältin) sowie Fachanwältin für Steuerrecht
beide Wagemann + Partner PartG mbB, Steuerberater | Wirtschaftsprüfer, Berlin

Einheitlich geplant

Standardisierung von Kassendaten | Das Gesetz zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen sieht eine einheitliche digitale Schnittstelle vor, um eine reibungslose Datenübertragung für Prüfungszwecke zu gewährleisten. Kassenhersteller sollen diese im Zusammenhang zur technischen Sicherheitseinrichtung bis 2020 umgesetzt haben.

Autoren: Stephan Greulich und Tobias Teutemacher

Die Standardisierungsbestrebungen von Kassendaten sind im Rahmen der Digitalisierung von Geschäftsprozessen absolut zu begrüßen. Bislang jedoch liegt von gesetzgeberischer Seite kein passendes semantisches Datenmodell für die inhaltliche Ausgestaltung der einheitlichen Schnittstelle vor. Der Deutsche Fachverband für Kassen- und Abrechnungssystemtechnik e.V. (DFKA) hat sich bereits Anfang 2016 mit der Standardisierung von Kassenaufzeichnungen beschäftigt und dazu verschiedene Experten aus Wirtschaft und Verwaltung an einen Tisch gebracht. So sind Hard -und Softwarehersteller von Kassensystemen, IT-Dienstleister und Software-Anbieter von Buchführungsprogrammen, Vertreter des steuerberatenden und wirtschaftsprüfenden Berufsstands sowie Vertreter der Finanzverwaltung in der Arbeitsgruppe vertreten.

Die Arbeitsgruppe verfolgt insbesondere die folgenden Ziele, die mit der Standardisierung erreicht werden sollen:

- einheitliche Datenbereitstellung für die Finanzverwaltung (Außenprüfungen, Umsatzsteuer- und Kassennachschau)
- Ermöglichung der Auslagerung aller im jeweiligen System generierten Kassendaten in ein Archivsystem (Kasseneinzeldaten und Kassenabschlüsse)
- Ermöglichung einer möglichst automatisierten (Weiter-)Verarbeitung der strukturierten Kassendaten in der Finanzbuchführung sowie unterstützender Vollständigkeits- und Plausibilitätsbeurteilungen (betriebswirtschaftliche Analysen) durch den Kassenführenden

Angesichts der vom Gesetzgeber geforderten einheitlichen digitalen Schnittstelle sollen auch Unsicherheiten bezüglich der Datenaufbereitung und Archivierung abgebaut werden. Daher beab-

Fotos: roccomontoya/Getty Images

sichtigt die Arbeitsgruppe in der Zusammensetzung von Experten aus Wirtschaft und Verwaltung, mit der inhaltlichen Standardisierung von Kassendaten ein Erfolgsmodell für die weitere Ausgestaltung der gesetzlichen Anforderungen zum Schutz vor Manipulationen an digitalen Grundaufzeichnungen aufzuzeigen.

Struktur der Taxonomie der Kassendaten

Das Stammdatenmodul enthält Informationen zum Datensatz (zum Beispiel Erstellungsdatum, Berichtsnummer, Version der Taxonomie), Informationen zum Aufzeichnungsgerät und zur Berichtsperiode sowie Angaben zum Unternehmen. Eine Stammdatenhistorisierung ist nicht notwendig, da bei Erzeugung des Datensatzes sämtliche Stammdaten mit dem jeweiligen Bewegungssatz im Einzelaufzeichnungsmodul gespeichert werden.

In dem Kassenabschlussmodul sind die aggregierten Werte aller Einzelbewegungen getrennt nach Geschäftsvorfall und Zahlungsart dargestellt. Dabei werden ausschließlich Geschäftsvorfälle aggregiert, die für die umsatzsteuerliche und ertragsteuerliche Weiterverarbeitung Relevanz besitzen. Das Kassenabschlussmodul stellt somit die notwendige Basis für die gesetzlich geforderte Nachvollziehbarkeit und Nachprüfbarkeit der aggregierten Werte für die nachgelagerte und verdichtete buchhalterische Abbildung im Rechnungswesen dar. Anhand des Kassenabschlussmoduls ist die Einhaltung des Prüfungspfads von der verdichteten Einzelbuchung, wie beispielsweise der gesamten Bareinnahmen eines Tages, über das Kassenabschlussmodul bis zu den jeweiligen Einzelaufzeichnungen im Einzelaufzeichnungsmodul und zurück sichergestellt. Darüber hinaus bietet das Kassenabschlussmodul die Möglichkeit, den tatsächlich gezählten Bargeldbestand einer Kasse im Hinblick auf die Kassensturzfähigkeit rechnerisch abzubilden.

Das Einzelaufzeichnungsmodul ist das Kernelement der Kassentaxonomie, da hier sämtliche Details des aufzeichnungspflichtigen Geschäftsvorfalls hinterlegt werden. Anhand dieser Struktur werden die Anforderungen an die Einzelaufzeichnungspflicht (§ 146 Abs. 1 Satz 1 Abgabenordnung – AO) und die Angaben auf dem Beleg sichergestellt. Wie auch bereits heute in einigen Kassensystemen etabliert, werden die einzelnen Transaktionen entsprechenden Typen (sogenannte Bontypen) zugeordnet. Mithilfe dieser Kategorisierung lassen sich Transaktionen etwa zwischen Rechnungen, Lieferscheinen und reinen Bestellungen differenzieren. Aber auch Merkmale für eine transparente Darstellung der Storno- oder Trainingsbuchungen sowie der Zahlungswege sind in der Datensatzbeschreibung vorgesehen.

Die Kassentaxonomie sieht grundsätzlich einen sehr hohen Detailierungsgrad bei der Erfassung der Informationen am Kassensystem vor und ist darüber hinaus für weitere nicht strukturierte Sachverhalte noch individualisierbar. Das hat aber nicht zur Folge, dass sämtliche Kassensysteme auch diesen Detailierungsgrad unterstützen müssen. Am Markt werden eine Reihe von Kassensystemen angeboten, die nicht auf dieser feinen Granularität aufzeichnen und somit in Folge auch auf einer höher aggregierten Taxonomieposition die Werte abbilden können. Dies entspricht auch einer ordnungsmäßigen Kassenführung, sofern die progressive und retrograde Prüfbarkeit für sachverständige Dritte (Prüfer der Finanzverwaltung) gegeben ist. Sofern ein Kassensystem jedoch die entsprechenden Inhalte direkt aufzeichnet, sind diese steuerrelevanten Daten auch im Rahmen der Kassenführung archivierungspflichtig und für die steuerliche Außenprüfung bereitzustellen.

Wartung und Pflege des Standards

Taxonomien als semantische Datenmodelle zur Erfüllung von Aufzeichnungs-, Deklarations- und Offenlegungspflichten unterliegen einem stetigen Wandel. So sind regelmäßig gesetzliche Änderungen und sonstige marktübliche Gegebenheiten zu bewerten und in die Datensatzbeschreibung aufzunehmen. Für die Akzeptanz und für die Verbreitung eines Standards ist ein geregelter Prozess der Wartung und Pflege von sehr großer Bedeutung. Der DFKA als Herausgeber der Kassentaxonomie hat daher bereits vor Veröffentlichung der ersten Version die nachhaltige Entwicklung in einer entsprechenden Arbeitsgruppe unter dem Dach des Verbands sichergestellt. Durch öffentliche Reviews der jeweiligen Taxonomieversionen wird ein hohes Maß an Akzeptanz und Praktikabilität bei der Implementierung und Nutzung des Standards sichergestellt. ●

TOBIAS TEUTEMACHER
Steuerfahnder beim Finanzamt für Steuerstrafsachen und Steuerfahndung Münster (NRW)

STEPHAN GREULICH
DATEV eG, fachliche Basis Rechnungswesen

MEHR DAZU

Für weitere Informationen zur Kassentaxonomie sei auf die Internetseiten des DFKA unter www.dfka.net/taxonomie/ verwiesen.

Fachliteratur zum Thema:

Mandanten-Info-Broschüren

Ordnungsgemäße Rechnung, Art.-Nr. 36181

Kassen-Nachschau ab 2018, Art.-Nr. 32068

Fachbücher für Mandanten

Kassenführung - Bargeschäfte sicher dokumentieren, 2. Auflage, Art.-Nr. 35154

Lexikon der Kassenführung, Art.-Nr. 35155

Einheitlicher Datenschutz

DSGVO | Die neuen Gesetze treten Ende Mai in Kraft.

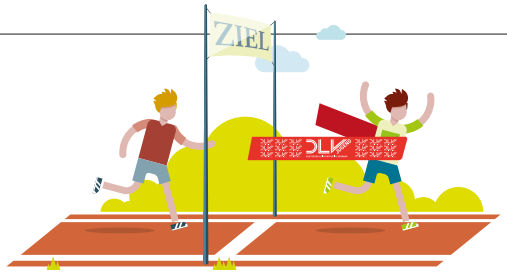
Am 25. Mai wird es ernst. Dann gilt die EU-Datenschutzgrundverordnung in allen Mitgliedsländern einheitlich. Bei Verstößen drohen hohe Bußgelder. Die EU-Kommission hat einen Leitfaden für Unternehmen bereitgestellt. Die deutschen Aufsichtsbehörden informieren über Kurzpapiere über Anforderungen. DATEV hat alle notwendigen Vorbereitungen für die Zusammenarbeit mit den Mitgliedern nach dem 25. Mai getroffen sowie unter www.datev.de/dsgvo viele Informationen für Steuerberater, Rechtsanwälte und Wirtschaftsprüfer bereitgestellt. Darüber hinaus aber darf die DATEV keine individuelle, rechtliche Beratung leisten. Grundsätzliche Fragen rund um den Kanzleibetrieb sind mit den berufsständischen Vertretern (Kammern und Verband) zu klären.

Neuer Geschäftsführer bei TeleTax und TeleLex

Führungswechsel | Stefan Meisel steht an der Spitze des Weiterbildungsanbieters.

Die spezialisierten Weiterbildungsanbieter TeleTax GmbH und TeleLex GmbH haben einen neuen Geschäftsführer. Zum Jahresbeginn hat Stefan Meisel die Position in beiden Unternehmensbeteiligungen der DATEV eG von Frank Meinhold übernommen, der nach 31 Jahren bei DATEV in den Ruhestand getreten ist. Meisel übt die Tätigkeiten neben seinen Aufgaben als Mitglied der Geschäftsleitung der DATEV eG aus, für deren Außendienst er verantwortlich zeichnet.

Die TeleTax GmbH ist ein Gemeinschaftsunternehmen der deutschen Steuerberaterverbände und der DATEV. Sie bietet Fortbildungsangebote zu steuerrechtlichen und betriebswirtschaftlichen Themen. Zielgruppe sind steuerlich Beratende sowie Mandanten. Stefan Meisel nimmt die Geschäftsführung von TeleTax gemeinsam mit Sabine Motte wahr. Die TeleLex GmbH ist auf Online-Fortbildung für Rechtsanwälte spezialisiert. Sie bündelt als Gemeinschaftsunternehmen des Verlags Dr. Otto Schmidt und der DATEV das Know-how beider Partner in der multimedialen Weiterbildung. Abgerundet wird das Angebot durch ausgewählte Fachtitel. Die Geschäftsführung von TeleLex besteht aus Stefan Meisel und Prof. Dr. Felix Hey.



Sport und Integration

Kooperation | Im Februar fand das erste Event in Zusammenarbeit mit dem Deutschen Leichtathletik-Verband statt.

Der Verein TABALiNGO Sport & Kultur intergrativ e.V. war zu Gast in der mit 4.000 Besuchern ausverkauften Halle in Dortmund. Rund 40 Kinder und Jugendliche mit körperlicher und geistiger Einschränkung maßen sich auf der offiziellen Wettkampffläche in Weitsprung, Hürdenlauf und Staffelauf. Bei der Siegerehrung überreichten der Präsident des DLV Jürgen Kessing und der Leiter der DATEV-Niederlassung Jürgen Offermann jedem Kind eine Teilnehmerurkunde. Anschließend wurde ein Gruppenfoto gemacht. Die nächste Veranstaltung findet am 21.–22. Juli im Max-Morlock-Stadion in Nürnberg statt. Schulen, Vereine und andere Einrichtungen, die mit Kindern und Jugendlichen mit körperlichen und geistigen Einschränkungen arbeiten sowie das Thema Inklusion leben, sind eingeladen, sich anzumelden.

IMPRESSUM

Herausgeber: DATEV eG | Paumgartnerstraße 6–14 | 90329 Nürnberg **Verantwortlich (Redaktion, Anzeigen):** Claus Fesel **Chefredakteur:** Markus Korherr, Tel.: +49 911 319-53157 | Fax: +49 911 147-01705 **Stellvertretender Chefredakteur:** Herbert Fritschka (M.A.) **Redaktion Rubrik Praxis:** Robert Brütting (RA), **CvD:** Kerstin Putschke (M.A.) | E-Mail: magazin@datev.de **Redaktionsbeirat:** Prof. Dr. Andrea Back (St. Gallen), Dr. Peter Leidel (Regen), Prof. Dr. Peter Lutz (München), Solange van Rens (Passau), Prof. Dr. Hanns R. Skopp (Straubing) **Realisation:** Christian Alt, Jan Bintakies, Georg Gorontzi, Monika Krüger, Jens Sommerfeld | TERRITORY CTR GmbH | Carl-Bertelsmann-Str. 33 | 33311 Gütersloh | www.territory.de **Fotos:** Getty Images, DATEV eG, Adobe Stock **Anzeigenleitung:** Herbert Fritschka, Tel.: +49 911 319-53145 | Fax: +49 911 14704208 | E-Mail: magazin.anzeigen@datev.de **Druck:** Mayr Miesbach GmbH | Am Windfeld 15 | 83714 Miesbach **ISSN:** 2197-2893 | Das DATEV magazin erscheint monatlich in einer Druckauflage von 51.000 Exemplaren. Namentlich gekennzeichnete Veröffentlichungen geben in erster Linie die Auffassung des Autors wieder.

Fotos: Scar1984/Getty Images

Nummer sicher

Notfallkonzept | Kaum eine Kanzlei kann heute auf ihre IT verzichten. Ein Notfallkonzept haben aber die wenigsten. Dabei ist es überlebenswichtig für die Kanzlei.

Autorin: Manuela Moretta

Fotos: alexfiodorov, CostinT, freestylephoto/Getty Images

Ein Bagger, der versehentlich die Stromversorgung einer ganzen Straße lahmlegt; ein Wasserrohrbruch in der Wohnung über der Kanzlei; eine Festplatte, die in Flammen aufgeht … – für eine Kanzlei gibt es viele Unwägbarkeiten, die ein normales Weiterarbeiten unmöglich machen. Dazu kommt die zunehmende Verbreitung von Schad-Software oder auch Datenverlust durch Nachlässigkeit oder falsche Bedienung. Gravierende IT-Sicherheitsprobleme oder Imageverlust können die Folge sein.

Entscheider gefragt

Beim IT-Notfallmanagement oder Notfallkonzept geht es keineswegs nur um rein technische Fragen, die ohne Vorüberlegung an einen Dritten ausgelagert werden können, zum Beispiel an einen Systempartner. Die Bewertung der wirtschaftlichen und rechtlichen Auswirkung ist vielmehr Aufgabe der Kanzleileitung. Zunächst geht es um organisatorische Lösungen, die den laufenden Betrieb in der Kanzlei gewährleisten sollen. Daraus ergeben sich die auszuwählenden technischen Lösungen, die eine unterstützende Funktion haben. Ein Außenstehender kann nur schwer bewerten, welche Daten und Prozesse für das Wiederanlaufen der Kanzlei nötig sind und deshalb hohe Priorität haben.
Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet umfangreiche Konzepte für ein IT-Notfallmanagement, gleichermaßen für multinationale Konzerne und für Kleinstunternehmen. Für eine kleine Kanzlei kann aber auch ein abgespeckter Notfallplan durchaus reichen – sofern er dafür sorgt, dass in einer Notfallsituation die Kanzleiprozesse nicht oder nur kurzfristig unterbrochen werden.

Vorgehensweise

Oft lohnt es sich, hier einen Experten heranzuziehen, der über das branchenübliche, für die Kanzlei nötige Wissen verfügt, die erforderlichen Maßnahmen kennt und umsetzen kann, wie es zum Beispiel auch beim DATEV IT-Consulting gehandhabt wird.
Am Anfang sollte eine Betriebsunterbrechungsanalyse stehen (Business Impact Analysis). Damit ermittelt die Kanzlei, wie sich ein Schadensszenario generell auf die Geschäftsprozesse auswirkt. So lässt sich genauer feststellen, nach wie vielen Stunden oder Tagen der Geschäftsbetrieb bereits existenzbedrohend gefährdet ist.

1. Beginnen Sie mit dem Überlebensszenario

Wer für seine Kanzlei die Entwicklung eines IT-Notfallplans beschleunigen möchte, konzentriert sich am besten auf das Wesentliche, um möglichst schnell wieder ein akzeptables Funktionsniveau zu erreichen. Das ist das Überlebensszenario.
Die Kanzleileitung sollte grundsätzlich diese Fragen klären:

- Welche Katastrophenszenarien könnten existenzbedrohend für die Kanzlei sein und zum Konkurs der Kanzlei führen?
- Wie schnell (in Stunden, Tagen oder Wochen) muss die Kanzlei sich erholen, damit sie eine katastrophenbedingte Störung übersteht?
- Was sind die kritischen Ressourcen, von deren Verfügbarkeit die Existenz der Kanzlei abhängt?
- Welche Arten von Katastrophen und Unfällen könnten in den nächsten Jahren eintreten und möglicherweise einen Worst Case auslösen?

Wichtig ist, dass alle Mitarbeiter und Führungskräfte wissen, wo sie die benötigten Notfallinformationen finden und was zu tun ist.

2. Vorsorge

Bei der Notfallvorsorge wird geplant, wie mit den möglichen Schäden umzugehen ist. Um die kritischen Geschäftsprozesse zu schützen, können unterschiedliche technische oder organisatorische Verfahren angewendet werden, zum Beispiel Datensicherungen und Vertreterregelungen.
Prinzipiell wird sich in einer Kanzlei der Ausfall des Internets und eine nicht erreichbare Homepage nicht so dramatisch auswirken wie ein Ausfall des Servers mit

einhergehendem Datenverlust. Denn auch Kanzleien, die per Cloud Sourcing arbeiten, können den Internetausfall durch entsprechende Sicherungsmaßnahmen verkürzen.

Das Herzstück ist eine gute Datensicherung. Ihre Merkmale:

- Dass alle notwendigen Daten auch tatsächlich enthalten sind, muss regelmäßig durch Reviews überprüft werden. Daten einer neu eingesetzten Software oder andere, durch neue Prozesse eingeführte Speicherorte dürfen nicht vergessen werden.
- Die Datensicherung sollte außerhalb der Technikräume aufbewahrt werden, mindestens in einem anderen Brandabschnitt, besser außerhalb des Hauptgebäudes.
- Sie muss gegen unbefugten Zugriff gesichert sein. Wird sie außerhalb der eigenen Räume aufbewahrt, sollte sie verschlüsselt sein.
- Aktuelle Datensicherungen werden vom Netzwerk getrennt aufbewahrt. Eine Infektion des Netzwerks infiziert dann nicht automatisch auch die Datensicherung.
- Regelmäßige Rücksicherungstests stellen die Lesbarkeit sicher und üben die Vorgehensweise ein.

3. Den Notfall bewältigen

Auch bei gutem Schutz lassen sich nicht alle gefährlichen Situationen eliminieren. Ein Notfall kann immer eintreten. Dann geht es um die konkrete Bewältigung. Hilfreich in kritischen Situationen ist ein Notfallhandbuch, nach dem man Schritt für Schritt vorgehen kann. Es sollte digital und in gedruckter Form vorhanden sein, über eine strukturierte Dokumentation mit Notfallplänen und Checklisten verfügen, die man abarbeiten kann. Das entlastet vor allem in Stresssituationen und hilft, einen kühlen Kopf zu bewahren.

4. In Abständen überprüfen

Notfallpläne und Handbücher müssen regelmäßig kritisch darauf überprüft werden, ob sie praktikabel und aktuell sind. Besonders nach umfangreichen Änderungen in der Organisation oder der IT. Das gilt für Maßnahmen und Dokumente und auch für den Notfallprozess an sich.

In der Steuerberatungskanzlei kann das bedeuten, dass zum Beispiel bei der Datensicherung die Backups in regelmäßigen Abständen überprüft werden: ob sie funktioniert und wie lang die Wiederanlaufzeit ist, bis die Kanzlei wieder arbeiten kann. Wichtig ist hier die klare und eindeutige Kommunikation zwischen Kanzleiinhaber und Systempartner, um sicherzustellen, dass die Kanzlei ihre Fristen und Termine einhalten kann.

5. Testen, üben, verbessern

Die Vorsorgemaßnahmen, Strukturen und Pläne müssen regelmäßig getestet und geübt werden, damit sie im Ernstfall funktionieren. Alle Mitarbeiter sollen die Inhalte verstehen und im Notfall richtig anwenden können. Formulieren Sie also klar und einfach. Der aktuelle Kenntnisstand sollte aufrechterhalten werden – durch Schulungen sowie ständige Weiterentwicklung und Anpassung der Konzepte, Dokumente und des Vorgehens.

Klein anfangen

Die angemessene Vorbereitung auf Notsituationen ist zwingend erforderlich und gesetzlich vorgeschrieben. Für eine Umsetzung fehlen aber vielerorts praktikable Rezepte. Dabei kann schon ein einfacher Notfallplan auf Basis weniger Notfallszenarien rasch vorzeigbare Ergebnisse liefern – und er lässt sich sukzessive zu einem umfassenden Konzept erweitern.

DATEV ProCheck unterstützt bei der Dokumentation und dem Nachweis regelmäßiger Tests und Übungen. ●

MANUELA MORETTA
DATEV eG, IT und Organisation

PHASEN DES NOTFALLMANAGEMENTS

- Initiierung durch den Kanzleiinhaber
- Konzeption der Notfallstrategie und Vorsorgemaßnahmen durch Risikoanalysen und Ermittlung kritischer Kanzleiprozesse sowie Ressourcen
- Realisierung des Konzepts auf Basis von Prioritätenlisten und Verantwortlichkeiten
- Bewältigung von Notfällen anhand Verhaltensregeln, Plänen und definierten Zuständigkeiten
- Tests und Übungen, um mögliche Probleme und Lücken zu erkennen und zu optimieren
- Aufrechterhaltung und kontinuierliche Verbesserung der Konzepte und Maßnahmen

Den Einstieg finden

Digitalisierung | Die Kanzlei Hegele & Partner hatte exakt null Mandanten, die DATEV Unternehmen online einsetzen. Durch eine sehr geschickt geplante Mandantenveranstaltung hat sich das geändert.

Interview: Klaus Meier

DATEV magazin: Sie haben letztes Jahr eine ganz spezielle Veranstaltung für Ihre Mandanten angeboten. Erzählen Sie doch mal.
ROLAND HEGELE: Mein Vater Alfred Hegele hat unsere Kanzlei vor 50 Jahren gegründet und ist nebenbei bemerkt noch heute für unsere Mandanten aktiv. Anlässlich unseres 50-jährigen Kanzleijubiläums haben wir uns gefragt, welchen Nutzen unsere Mandanten von unserem Jubiläum haben und was in Erinnerung bleiben soll. Zu diesem Zeitpunkt war zufällig unsere DATEV-Kundenberaterin Marie Julie Hübner zum Jahresgespräch bei uns im Haus.

MARIE JULIE HÜBNER: Anlässlich des Jubiläums hatte ich die Idee, eine Mandantenveranstaltung anzubieten. Die Kanzleien hatten und haben mit den Verschärfungen der GoBD zu kämpfen, insbesondere im Zusammenhang mit der Datenarchivierung und der Kassenthematik. Deshalb dachte ich, es wäre sowohl für die Kanzlei als auch für die Mandanten ein echter Mehrwert, einen geeigneten externen Referenten über die GoBD referieren zu lassen. Damit die Mandanten aber nicht mit den zum Teil schon bedrückenden Anforderungen alleine gelassen werden, sollte anschließend ein DATEV-Kollege die GoBD-konformen Lösungen der DATEV vorstellen, die die Kanzlei anbieten kann.

Die GoBD gelten seit Anfang 2015. Ist das mittlerweile nicht ein alter Hut und jedes Unternehmen hat die neuen Regeln im Griff?
ROLAND HEGELE: Die Mandanten beschäftigen sich durchaus mit den GoBD, sind aber oft unsicher, ob sie die Anforderungen der GoBD richtig beachten und erfüllen. Das Thema Archivierung beschäftigt viele. Ebenso viele schreiben auch ihre Rechnungen noch immer mithilfe von Excel oder Word. Mit Unternehmen online können hier viele Probleme gelöst werden. Deshalb wollten wir unsere Mandanten über die Digitalisierung von Unternehmensprozessen informieren und aufklären.

Wie war die Resonanz?
ROLAND HEGELE: Wir haben auch vorher schon Mandantenveranstaltungen und Vorträge zu anderen Themen angeboten. Dass wir mit dem Thema Digitalisierung über 300 Teilnehmer gewinnen und begeistern konnten, das war für uns allerdings schon überraschend und sehr erfreulich.

Haben Sie Ihre Mandanten von der Notwendigkeit zur Digitalisierung und von den DATEV-Lösungen überzeugt?
ROLAND HEGELE: Das ist uns in der Tat gelungen. Die Mandanten waren sich einig, dass der Weg in die digitale Zukunft notwendig ist und dass sie diesen Weg mit Unternehmen online gehen werden. Dass wir die Mandanten überzeugt haben, sehen wir auch an den Zahlen: Statt der fünf neuen Unternehmen online-Mandate, mit denen wir kalkuliert hatten, haben wir über 30 generiert – und die Nachfrage reißt nicht ab.

Da haben Sie wohl vieles richtig gemacht. Woran lag es, dass der Zuspruch so groß war?
ROLAND HEGELE: Vielleicht lag es am Gesamtkonzept. Wir haben Themenskripte entwickelt und sie zusammen mit dem Einladungsschreiben verschickt. Wir haben entsprechend der Themen ganz gezielt eingeladen und auch mehrere Termine zur Auswahl angeboten. Kurz vor der Veranstaltung haben wir nochmal an den Termin erinnert. Und wir haben sehr großen Wert auf die Rückmeldungen gelegt, egal ob Zu- oder Absage. Auf diese Weise kamen wir mit den Mandanten ins Gespräch.

Wie lief die Digitalisierung vor dieser Mandantenveranstaltung in Ihrer Kanzlei?
ROLAND HEGELE: Wie wahrscheinlich in vielen anderen Kanzleien: Man nimmt die Digitalisierung wahr, setzt sich aber nicht ernsthaft damit auseinander. Das Tagesgeschäft dominiert den Kanzleialltag. Es bleibt wenig Zeit für die Entwicklung von Strategien, mit denen man den Herausforderungen der Digitalisierung begegnen kann.

Wie viele Mandate für Unternehmen online hatten Sie zuvor?
ROLAND HEGELE: Kein einziges. Die Kanzlei hatten wir zwar schon umgestellt, damit wir uns keine Blöße geben, wenn Mandanten nach Unternehmen online fragen. Von uns aus hatten wir das den Mandanten aber nicht angeboten. Diese Veranstaltung war tatsächlich der erste Versuch, die Mandanten direkt anzusprechen.

Wie sehen Ihre Mitarbeiter in der Kanzlei die Digitalisierung?
ROLAND HEGELE: Unsere Mitarbeiter haben damit überhaupt kein Problem. Im Gegenteil. Sie sind sehr froh und sehr dankbar, dass wir uns mit diesen Zukunftsthemen beschäftigen und

dass sie nicht abgehängt werden. Es ist zwar für alle anstrengend, und ich erwarte auch sehr viel, aber ich beobachte auch: Kanzleien, die gar nichts tun, verlieren ihre Mitarbeiter, weil die das Gefühl haben, sie verlieren den Anschluss.

Kommen wir nochmal zurück zur Veranstaltung. Zuerst Angst vor den GoBD schüren, danach die DATEV-Programme als Rettung in der Not anbieten. Das klingt ein wenig berechnend. War das die Absicht und ging die Rechnung auf?
ROLAND HEGELE: Unsere Absicht war nicht, den Mandanten Angst zu machen, sondern ihnen die Notwendigkeit, aber vor allem die Vorteile der digitalen Prozesse möglichst transparent zu machen. Um dieses Ziel zu erreichen, brauchten wir natürlich die volle Aufmerksamkeit der Mandanten. Und die hatten wir, dank unseres Konzepts. Die neue digitale Betriebsprüfung hat die Mandanten sehr interessiert.

MARIE JULIE HÜBNER: Mit Guido Preuss vom Institut für Unternehmensführung (IFU) hatten wir auch einen Topreferenten. Und glauben Sie mir: Während seines Vortrags ist es im Saal immer ruhiger geworden. Im Anschluss hat mein Kollege Georg Schoty dann die DATEV-Lösungen zur GoBD aufgezeigt, sodass die Stimmung sichtlich wieder besser wurde.

Was sagen Sie persönlich: Hat sich Ihr Einsatz gelohnt?
ROLAND HEGELE: Auf jeden Fall. Wir hatten ausschließlich positive Rückmeldungen. Unsere Mandanten fühlen sich jetzt, glaube ich, noch wohler bei uns, weil wir uns um die Digitalisierung kümmern und sie bei den GoBD unterstützen. Meine Mandanten kennen sich, reden miteinander und fragen sich gegenseitig, wie weit sie sind. Sie unterhalten sich auch mit Unternehmern, die nicht unsere Mandanten sind. Und die sprechen dann wieder ihre jeweiligen Steuerberater auf das Thema an.

MARIE JULIE HÜBNER: Sogar sehr, sehr große Steuerberatungskanzleien haben nach unseren Skripten gefragt. Darauf sind wir schon ein bisschen stolz.

Was empfehlen Sie Berufskollegen, die den Einstieg in die Digitalisierung nicht finden?
ROLAND HEGELE: Nutzen Sie die Informationsmöglichkeiten, die DATEV anbietet. Das Angebot ist wirklich vielseitig, egal ob Sie Einsteiger, Steckenbleiber oder Digitalisierungsprofi sind. Besuchen Sie zum Beispiel die Regional-Info-Tage oder die Sprechtage der DATEV. Das lohnt sich immer, auch weil man sich dort mit den Berufskollegen austauschen kann. Sprechen Sie auch mit Ihrem DATEV-Kundenberater. Die Beratung ist Gold wert. Unsere DATEV-Kundenberaterin Marie Julie Hübner zum Beispiel hatte die Idee mit den Mandantenveranstaltungen, aus der letztlich eine große Sache geworden ist. Andere Kanzleien können diese Idee jederzeit kopieren. DATEV hat die Skripte und stellt sie auch zur Verfügung.

MARIE JULIE HÜBNER: Meine Kollegin Svetlana Becker hat mittlerweile ein eigenes Skript entwickelt. Wir bieten übrigens auch an, dass jemand von DATEV den GoBD-Vortrag hält.

ROLAND HEGELE: Ganz wichtig ist, dass die Kanzlei dranbleibt. Die Kanzlei muss in Kontakt mit den Mandanten bleiben, sie sinnbildlich an die Hand nehmen und auf dem Weg in die Digitalisierung begleiten. Ansonsten besteht die Gefahr, dass der Mandant aufgibt und wieder in alte Gewohnheiten zurückkehrt. ●

KLAUS MEIER
Redaktion DATEV magazin

DIE GESPRÄCHSTEILNEHMER

MARIE JULIE HÜBNER,
DATEV eG, Kundenberaterin Regionalvertrieb

ROLAND HEGELE,
Kanzleimanager Hegele & Partner Steuerberatungsgesellschaft mbB, Zusmarshausen

MEHR DAZU

Bei Fragen zur Veranstaltung und zu den Skripten helfen: mariejulie.huebner@datev.de oder svetlana.becker@datev.de

Referenten und Themen der Mandantenveranstaltungen:

Guido Preuß vom Institut für Unternehmensführung (IFU) in Bonn zum Thema Die neuen Arbeitsweisen der Finanzverwaltung – Risikomanagement, Kassen, GoBD, Digitale Betriebsprüfung

Georg Schoty von DATEV zum Thema Umsetzung der GoBD-Anforderungen mit Hilfe der DATEV-Programme

Roland Schätzle von DATEV zum Thema DATEV-Online-Lösungen in der Personalwirtschaft

Svetlana Becker von DATEV zum Thema DATEV Unternehmen online

Managementseminar

Lernen mit Blick aufs Meer

DATEV-Sommerakademie 2018 | Beschäftigen Sie sich fünf Tage intensiv mit den Zukunftsthemen Ihrer Kanzlei – abseits des beruflichen Alltags, mit speziell auf Kanzleiinhaber zugeschnittenen Seminarinhalten und Zeit für den Erfahrungsaustausch mit Berufskollegen.

Die eigene Kanzlei erfolgreich in die Zukunft zu führen, ist eine anspruchsvolle Aufgabe und auch eher ein Marathon als ein Sprint. Umso wichtiger ist es, dabei strukturiert vorzugehen. DATEV bietet die Expertise für eine erfolgreiche Umsetzung: Die DATEV-Sommerakademie 2018 in Rostock-Warnemünde.

Inhalte der DATEV-Sommerakademie

Beschäftigen Sie sich fünf Tage intensiv mit den wichtigsten Handlungsfeldern der Kanzlei. Abseits des beruflichen Alltags können Sie sich voll und ganz der Entwicklung Ihrer Kanzlei widmen und die wesentlichen Anforderungen und Antriebsmotoren für deren Zukunfts- und Wettbewerbsfähigkeit erarbeiten. Daneben erlernen Sie auch Methoden, wie Sie sich Auszeiten einräumen und in angespannten Situationen den Überblick behalten – alles an einem attraktiven Tagungsziel, im Austausch mit Berufsträgern und Referenten.

Mit neu konzipierten Inhalten und Referenten auch ein interessantes Angebot für Teilnehmer aus vergangenen Akademien.

Das Programm im Überblick

- Tag 1: Vom Leitbild zur Strategie
  Leitplanken der Strategieentwicklung kennenlernen und umsetzen
- Tag 2: Effizienz und Sicherheit durch digitale Prozesse steigern
  Mehrwerte für Kanzlei und Mandanten schaffen
- Tag 3: Erfolgreiches Kanzleimarketing
  Kanzleistärken nutzen, um Mandanten zu begeistern und als Multiplikatoren zu gewinnen
- Tag 4: Mitarbeiter fördern und führen
  Führungsinstrumente und -methoden für eine erfolgreiche Personalentwicklung umsetzen
- Tag 5: Herausforderungen aktiv meistern
  Rückschläge und Umbrüche mit geeigneten Methoden bewältigen

Termin und Ort

23. bis 27. Juli 2018,
Hotel Neptun in Rostock-Warnemünde

MEHR DAZU

Buchungsmöglichkeiten und weitere Informationen:

DATEV-Sommerakademie 2018, Art.-Nr. 70120

Alle Themen der DATEV-Sommerakademie sind Bestandteil der Management-Weiterbildung und auch einzeln und in beliebiger Reihenfolge buchbar – an mehreren Terminen und verschiedenen Orten deutschlandweit.

Management-Weiterbildung, **www.datev.de/management-seminare**

Neue Aktion

DATEV-Verlagsmedien kennenlernen

Fachliteratur | Mit rund 360 Titeln bietet der DATEV-Shop eine umfassende und unverzichtbare Praxisbibliothek für Steuerberater, Rechtsanwälte und Wirtschaftsprüfer – und übrigens auch deren Kanzleimitarbeiter.

Testen Sie uns – vollkommen gratis und unverbindlich. Bis 31. Mai 2018 können Sie folgende Titel der DATEV-Fachliteratur kostenlos im DATEV-Shop bestellen und sich selbst überzeugen:

Kompaktwissen Lohn und Personal:

- Beschäftigung von Praktikanten,
  E-Book: Art.-Nr. 19690
- Arbeitsrecht und Sozialversicherungsrecht in der Insolvenz,
  E-Book: Art.-Nr. 19561

Kompaktwissen Baugewerbe

- Zuschlagssätze und Verrechnungslohn im Bau, 2. Auflage,
  E-Book: Art.-Nr. 19868

Kompaktwissen Berater

- Häusliches Arbeitszimmer,
  E-Book: Art.-Nr. 19689

Kompaktwissen GmbH-Berater

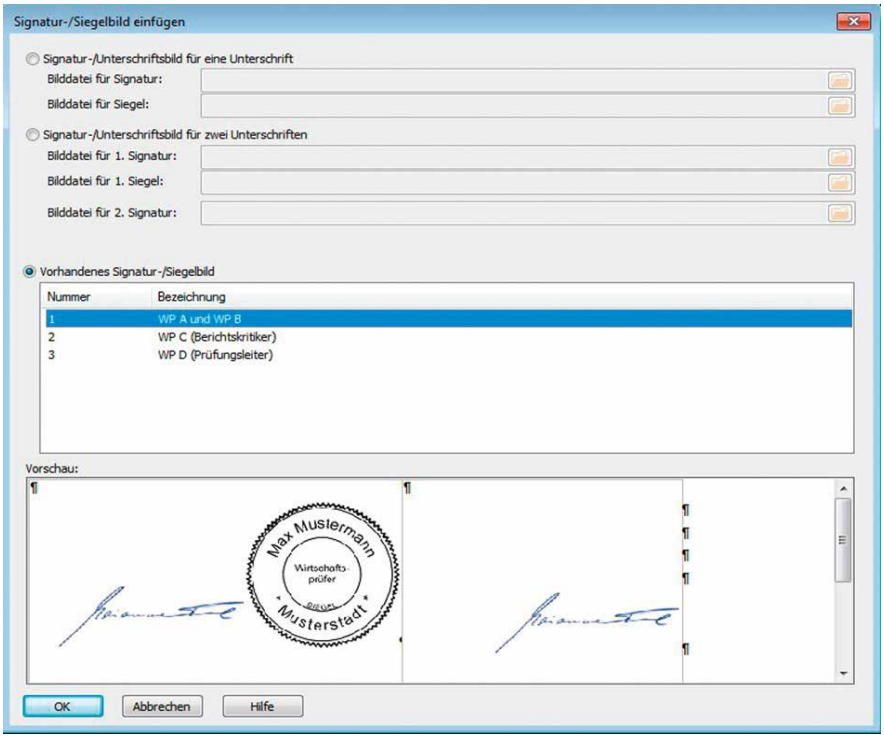
- Verlustverrechnung bei der GmbH, 3. Auflage,
  E-Book: Art.-Nr. 19871

Abschlussprüfung

Prüfungsberichte digital unterschreiben

Digitale Signatur | Die Digitalisierung verändert vor allem Routinetätigkeiten. Stellen Sie sich dieser Herausforderung und nutzen Sie die Chance, gedruckte Prüfungsberichte komplett oder teilweise durch elektronisch qualifiziert signierte PDF-Prüfungsberichte zu ersetzen.

Die Voraussetzungen dafür wurden bereits geschaffen. Die eIDAS-Verordnung und die Änderung der Berufssatzung für Wirtschaftsprüfer/Vereidigte Buchprüfer machen es möglich, und die DATEV-Programme zur Abschlussprüfung unterstützen Sie bei der Umsetzung.



Voraussetzungen schaffen

Damit Sie Ihre Prüfungsberichte in elektronischer Form abgeben können, benötigen Sie:

1. Eine Signaturkarte für qualifizierte Signaturen und ein kompatibles Kartenlesegerät
2. Eine Signatur-Software für qualifizierte Signaturen: Die prozessintegrierte Signatur-Software Sign Live! CC des Anbieters intarsys mit DATEV-Schnittstelle unterstützt Sie komfortabel im gewohnten DATEV-Programmumfeld. Weitere Informationen dazu finden Sie auf dem DATEV-Marktplatz
3. Ihre Unterschrift und Ihr Berufssiegel in elektronischer Form

Digitale Signatur einfügen

Haben Sie die Voraussetzungen erfüllt, steht der qualifizierten Signatur nichts mehr im Weg. Fügen Sie im ersten Schritt Ihre Signatur und Ihr Berufssiegel über Einfügen | Signatur/Siegelbild in Ihren Prüfungsbericht ein. Über das neue Fenster Signatur-/Siegelbild einfügen wird eine Einfach- oder auch Zweifachsignatur unterstützt.

Bei Bedarf können Sie nach dem Einfügen die Signaturzeile nach Ihren Wünschen gestalten, um sie anschließend als Signaturzeile zu speichern und auch in anderen Berichten zu verwenden.

PDF erstellen und qualifiziert signieren

Nach Bearbeitung Ihres Dokuments wählen Sie Datei | Ausgeben | PDF mit qualifizierter Signatur, um eine PDF-Datei mit qualifizierter Signatur und Siegel zu erstellen. Für die Revisionssicherheit muss ein Schreibschutz gesetzt und der Dokumentstatus auf fertiggestellt geändert werden. So wird sichergestellt, dass nur fertiggestellte und nicht veränderbare Berichte ausgegeben werden.

Abschließend müssen Sie nur noch die PIN Ihrer qualifizierten Signaturkarte zur Authentifizierung eingeben. Damit ist der Signaturvorgang abgeschlossen, und ein revisionssicheres PDF/A-Dokument wird automatisch an einem von Ihnen ausgewählten Speicherort abgelegt. Der fertige PDF-Prüfungsbericht macht den gedruckten, handsignierten und gesiegelten Prüfungsbericht unnötig. Dieser Prozess ist laut der Berufssatzung der Steuerberater natürlich auch für Erstellungsberichte zulässig.

MEHR DAZU

Weitere Informationen einschließlich einem Servicevideo zur digitalen Signatur finden Sie in der Info-Datenbank (Dok.-Nr. 1001335).

Kontakt: Fragen zum Programm Abschlussprüfung beantwortet der Programmservice Abschlussprüfung
Telefon: +49 911 319-37891
E-Mail: abschlusspruefung@service.datev.de

Fragen zum Programm Bilanzbericht beantwortet der Programmservice Bilanzbericht
Telefon: +49 911 319-34735
E-Mail: bilanzbericht@service.datev.de

DATEV Abschluss- und Datenprüfung

Effizienter IT-Einsatz

Praxiswerkstatt | Sehen Sie anhand eines Musterfalls, wie Sie mit DATEV-Software bei der Abschlussprüfung effizient auch bei großen Datenmengen arbeiten.

Der Musterfall handelt von der Musterglas GmbH, deren Vertrieb ausschließlich über einen Onlineshop stattfindet. Viele Transaktionen im Shop sind automatisiert. Der Fall stellt somit eine typische Herausforderung dar: Wie prüfe ich mit dieser Fülle an EDV-Daten möglichst wirtschaftlich? Nur ein effizienter IT-Einsatz, etwa mittels Massendatenanalyse, macht die Prüfung aufgrund der Fülle der EDV-Daten wirtschaftlich. Durch Übungen, die Sie selbstständig am Schulungs-PC durchführen, lernen und erarbeiten Sie die Methoden, um den Software-Einsatz zu optimieren.
Im Programm Abschlussprüfung comfort erfassen Sie die Prüfungsergebnisse, die Sie unter anderem mithilfe des Programms Datenprüfung erzielt haben.
Hinweis: Aufgrund der technischen Gegebenheiten sind die Teilnehmerplätze auf zehn begrenzt.

Termine

17.04. – 18.04.2018	Berlin
24.04. – 25.04.2018	Dortmund
16.07. – 17.07.2018	Stuttgart
25.07. – 26.07.2018	München
17.09. – 18.09.2018	Frankfurt
09.10. – 10.10.2018	Köln

MEHR DAZU

Weitere Informationen auf **www.datev.de/praxiswerkstatt-ap**

Im DATEV-Shop: Art.-Nr. 73925

Ansprechpartnerin: Kerstin Ringel

E-Mail: apveranstaltungen@service.datev.de

Fotos: vladwel, erhui1979/Getty Images

DATEV Unternehmen online

Auswertungen modernisiert

Personalwirtschaft | Das in DATEV Unternehmen online sowie in der compact-Variante enthaltene Programm Auswertungen online Personalwirtschaft zeigt sich seit Jahresbeginn moderner und intuitiver.

Für alle Anwender von DATEV Unternehmen online sowie der compact-Variante bietet die überarbeitete Anwendung eine einfachere Möglichkeit, die Lohnauswertungen an Mandanten zu verteilen. Abgesehen davon, dass die Auswertungen zentral an einer Stelle verfügbar sind, wartet das Programm mit weiteren neuen Features auf:

- E-Mail-Versand war gestern; heute: ein intuitiv bedienbarer und sicherer Weg, um Lohnauswertungen bereitzustellen
- verbesserte Suche und Filter, über die Sie gezielt Lohnauswertungen finden
- einfacher Einstieg in die digitale Zusammenarbeit mit DATEV Unternehmen online
- für internationale Kanzleien/Mandanten geeignet durch eine englischsprachige Programmoberfläche

MEHR ZUM THEMA

Wie Sie mit den Auswertungen der Lohnbuchführung in DATEV Unternehmen online arbeiten, erfahren Sie in der Info-Datenbank: Unternehmen online: mit Auswertungen der Lohnbuchführung arbeiten (Dok.-Nr. 1071569)

Windows

Abkündigung von Betriebssystemen

Supportende | Microsoft beendet den Support für die Betriebssysteme Windows 7 und Windows Server 2008 R2 ab 13. Januar 2020. Sicherheitslücken, die danach erkannt werden, schließt Microsoft nicht mehr. Daher wird auch DATEV ab Januar 2020 diese Betriebssysteme nicht mehr unterstützen.

Januar 2020
Parallel zur Auslieferung der DATEV-Programme 14.1 werden Windows 7 und Windows Server 2008 R2 abgekündigt. Die DATEV-Programme 14.1 werden nicht mehr auf Verträglichkeit unter diesen Betriebssystemen getestet. Mit Lieferung der DATEV-Programme 12.0 im Sommer 2018 werden betroffene Rechner gelb gekennzeichnet, damit Sie frühzeitig die Umstellung auf ein aktuelles Betriebssystem planen können.
Sommer 2018
Parallel zur Auslieferung der DATEV-Programme 12.0 (voraussichtlich August) endet der DATEV-Support für Windows 8.1, Windows Server 2012 (ohne R2) und Windows Server 2008 (ohne R2).
Die Installation wird angehalten und kann nicht fortgesetzt werden. Online-Programme, die DATEV derzeit entwickelt, werden schon heute nicht mehr auf Windows Server 2008 getestet. Wechseln Sie auf das aktuelle Server-Betriebssystem Windows Server 2016 oder auf das Arbeitsplatz-Betriebssystem Windows 10.

MEHR DAZU

www.datev.de/betriebssystem-abkuendigung

Der Tulpencrash

Fotos: nicoolay, Katsumi Murouchi, mashuk/Getty Images

Börsencrash | Die erste Spekulationsblase der Welt entstand nicht durch Wetten auf Kursschwankungen oder Immobilienwerte. Im Februar 1637 steuerte die niederländische „Tulpenmanie“ auf ihren Höhepunkt zu. Seit vier Jahren schossen die Preise für die unscheinbaren Knollen in fantastische Höhen. Doch der Traum vom schnellen und leichten Gewinn zerplatzte und die Finanzwelt erlebte ihren ersten Börsencrash.

Autoren: Lukas Wollscheid, Tobias Birken

Langsam brach der Verkäufer in Angstschweiß aus. Drei Mal hatte er bereits seine Tulpenzwiebeln im abendlichen Schankkollegium (so wurde die Auktionsversammlung genannt) zum Verkauf angeboten. Den ursprünglichen Preis von 1.250 Gulden pro Pfund hatte er bereits auf 1.000 Gulden gesenkt – im Vergleich zu den vorangegangenen Tagen ein Schnäppchen. Aber auch für dieses Angebot fand sich unter den anwesenden Auktionsteilnehmern kein Interessent. Die meisten von ihnen hatten in den letzten Tagen vergleichbare Summen bezahlt, in der Absicht, durch die zu erwartende Wertsteigerung ihre Tulpenzwiebeln mit deutlichem Gewinn weiterverkaufen zu können. Und heute: immer noch kein Gebot. Ein Ruck ging durch die Versammlung und plötzlich wurde es laut. Die immer wilder gestikulierenden Männer kannten alle nur noch ein Ziel: verkaufen!

So ähnlich muss man sich den Dienstagabend des 3. Februar 1637 vorstellen, als in einem Haarlemer Gasthof zum ersten Mal eine Zwiebelauktion platzte. Innerhalb der nächsten zwei bis drei Monate verloren die meisten Tulpenzwiebeln bis zu 95 Prozent ihres Wertes. Mehrere Millionen Gulden an Kapital wurden so vernichtet. Tausende von Kleinanlegern und Spekulanten, von zeitgenössischen Kritikern abschätzig als „Floras Narrenkappen“ (nach einer angeblich im antiken Rom zur Göttin der Blumen erhobenen Kurtisane) bezeichnet, standen vor dem finanziellen Ruin.

Wirtschaftlich und kulturell befanden sich die Niederlande im ersten Drittel des 17. Jahrhunderts im sogenannten Goldenen Zeitalter. Die Kaufleute suchten nach Investitionsmöglichkeiten für den erwirtschafteten Gewinn. Tulpen, seit den 1560er Jahren in den Niederlanden bekannt, waren noch keine Massenware, und für seltene Sorten wurden hohe Preise gezahlt. Der wirtschaftliche Boom führte dazu, dass bald auch Geringverdiener kleine Vermögen sparen oder investieren konnten. Gleichzeitig machten die steigenden Preise die Tulpenzwiebel als vermeintlich selbstwachsende Investition für Anleger und Spekulanten attraktiv. Im Jahr 1633 trat erstmals der Fall ein, dass Tulpenzwiebeln als geldwertes Zahlungsmittel im Immobilienverkauf eingesetzt wurden. Mittlerweile wirkte sich der Preisanstieg nicht mehr nur auf die seltenen Exemplare aus. Sogar die einfachen Zwiebeln wurden ab 1634 immer teurer, die Tulpe wurde durch Neuzüchtungen zur Massenware.

Ab Herbst 1635 begannen die Niederländer, mit den noch im Boden befindlichen Zwiebeln zu spekulieren. Die zuvor real gehandelten Tulpenzwiebeln wurden so durch Options- und Schuldscheine ersetzt. Die Gewinnerwartungen führten zur Entstehung eines Terminmarktes, was Kleinanleger wiederum zu kreditfinanzierten Ankäufen verführte. Die neue Praxis, die Zwiebeln statt nach Zahl nach Gewicht zu bewerten, steigerte deren Wert zusätzlich. Von nun an schossen die Preise in die Höhe, was sich zur Jahreswende 1636/37 durch den exorbitanten Zustrom neuer Kleinanleger noch einmal potenzierte. Zu diesem Zeitpunkt gingen in den Niederlanden mindestens 5.000 Züchter und Floristen dem Tulpenhandel nach – bei insgesamt rund zwei Millionen Einwohnern. Ein einziges Exemplar der Sorte „Viceroy“ kostete zu diesem Zeitpunkt 2.500 Gulden – der Gegenwert von: zwei Wagenladungen Roggen, vier Mastochsen, vier Mastschweinen, zwölf Schafen, vier Fässern Bier, zwei Fässern Wein, 1.000 Pfund Käse, einem Bett, einem Silberbecher und einem Anzug, wie ein damaliger Autor auflistete. Zum Vergleich: In den 1630er Jahren betrug der Jahreslohn eines Amsterdamer Tuchmachers 250 Gulden, der eines mittleren Kaufmanns 1.500 Gulden. Noch am 5. Februar 1637 wurde beim Verkauf einer Zwiebelsammlung ein Gesamterlös von 90.000 Gulden erzielt – dem ungefähren Wert von acht großen Kaufmannshäusern in Amsterdam.

Diese Summe markierte zugleich das Ende der Manie. Bereits zwei Tage zuvor war es zu den ersten Zusammenbrüchen gekommen. Im Nachhinein betrachtet existierten dafür zwei wesentliche Gründe: Erstens fehlte es durch den vermehrten Handel einfacher Knollen ab Februar 1637 an Vorräten, und die Neuzüchtungen deckten den Bedarf nicht. Gleichzeitig blieb neues Kapital aus, da sich Neueinsteiger die einfachen Zwiebeln nicht mehr leisten konnten. Zweitens verkauften zu diesem Zeitpunkt einige Großhändler ihre Bestände und entzogen so dem Markt Kapital. Der Mangel an neuer Ware und Geld nahm dem gesamten Handel die Substanz. Da es, im Gegensatz zu den qualitativ hochwertigen, für gewöhnliche Tulpen keine Käufer mehr gab, beschleunigte sich der Preisverfall. Diejenigen, die auf Kredit investiert hatten, zogen verzweifelt ihr Geld aus dem Markt. Es kam zu panikartigen Verkäufen, die potenzielle Käuferzahl sank, die Preise erreichten einen Tiefpunkt.

Der Zusammenbruch des Tulpenhandels 1637 weist das Schema eines klassischen Börsencrashs auf. Da die Tulpenzwiebeln allerdings nicht an der Börse, sondern nur am Rande des niederländischen Wirtschaftssystems gehandelt wurden, blieben die Auswirkungen auf die direkt Involvierten beschränkt. Gerichtlich verordnete Annullierungen vieler Verträge und die Liquidierung des Großteils der Schulden durch die Vereinbarung einer Ablösesumme bewirkten, dass bereits 1639 die meisten Streitfälle beigelegt worden waren. Zurück blieb schon bei den Zeitgenossen das Gefühl für einen gewissen Epochencharakter der Ereignisse. Bis heute gilt die Tulpenmanie als die erste in einer Reihe von Spekulationsblasen ●

LUKAS WOLLSCHEID, TOBIAS BIRKEN
Neumann & Kamp, Historische Projekte

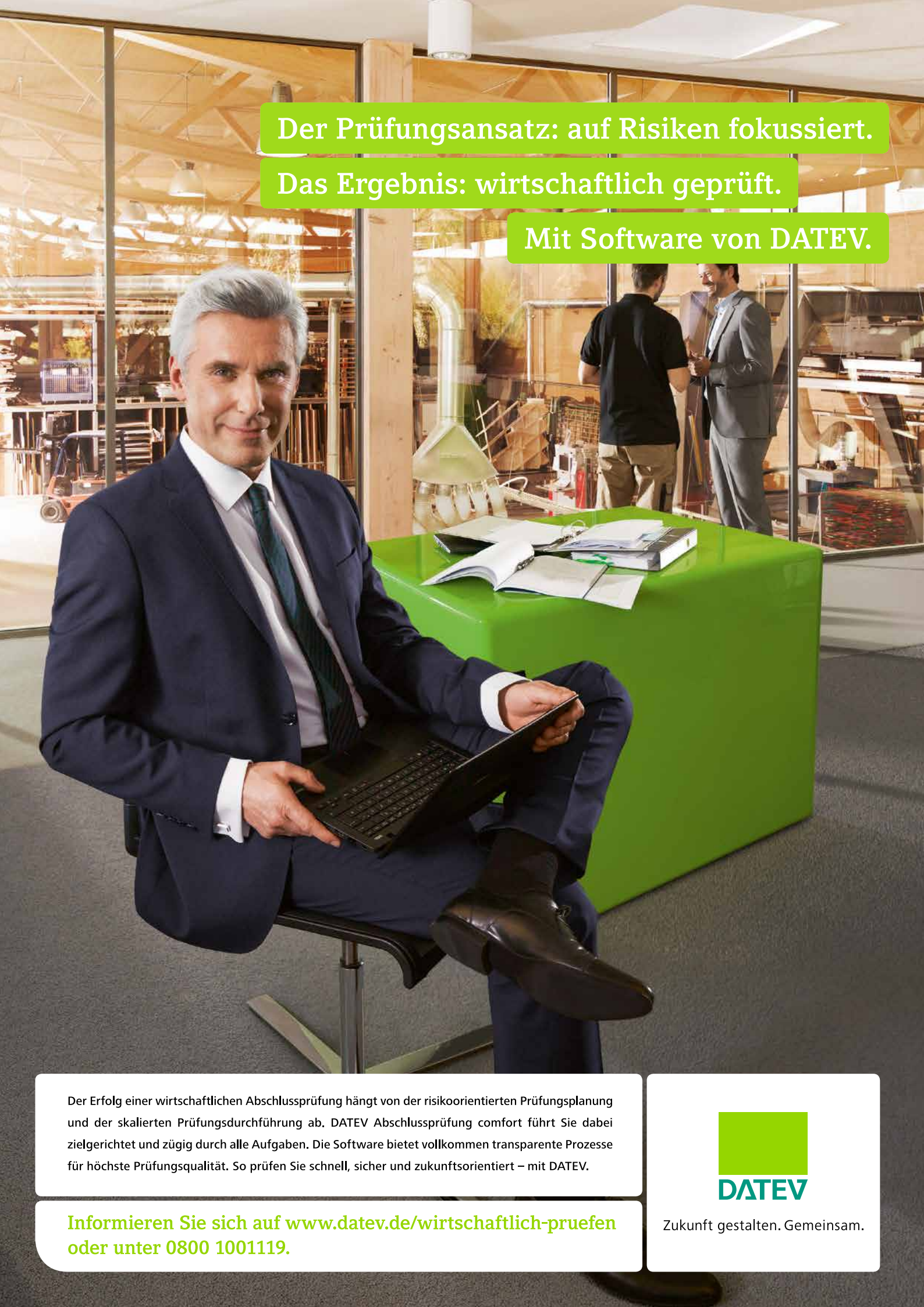
MEHR DAZU

Dash, Mike: Tulpenwahn. Die verrückteste Spekulation der Weltgeschichte, München 1999.

Graeber, David: Schulden. Die ersten 5000 Jahre, München 2014.

Piper, Nikolaus: Geschichte der Wirtschaft, Weinheim, Basel 2002.

Plumpe, Werner: Wirtschaftskrisen. Geschichte und Gegenwart, München 2013.



Der Erfolg einer wirtschaftlichen Abschlussprüfung hängt von der risikoorientierten Prüfungsplanung und der skalierten Prüfungsdurchführung ab. DATEV Abschlussprüfung comfort führt Sie dabei zielgerichtet und zügig durch alle Aufgaben. Die Software bietet vollkommen transparente Prozesse für höchste Prüfungsqualität. So prüfen Sie schnell, sicher und zukunftsorientiert – mit DATEV.

Informieren Sie sich auf www.datev.de/wirtschaftlich-pruefen oder unter 0800 1001119.

DATEV

Zukunft gestalten. Gemeinsam.