



Wer darf was sehen?

Die Regeln für Datenschutz, IT-Sicherheit und KI sind Grundlage vertrauensvoller Kooperation. Was das für Kanzleien bedeutet. → 10

Clever sanieren

Wie beim Kauf hoch verschuldeter Firmen Verlustvorträge erhalten bleiben. → 26

Niemals aufgeben

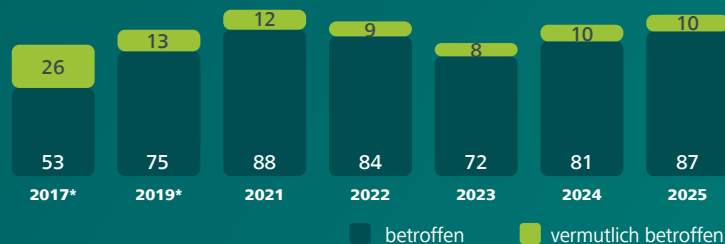
Wie eine Steuerberaterin die Hürden auf dem Weg zur eigenen Kanzlei überwand. → 36

Digitale Gefahr

Das Risiko von Cyberattacken in Deutschland steigt; der Wirtschaft entstehen Schäden in Milliardenhöhe durch Datendiebstahl, Spionage und Sabotage. Und die reale Bedrohung ist sogar größer als die gefühlte.

Es trifft nahezu jeden

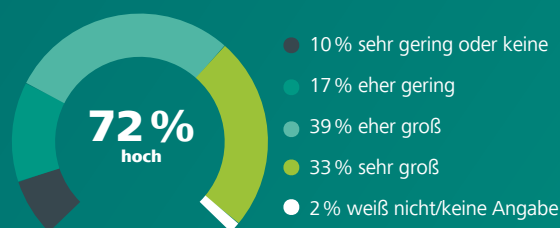
Anteil der tatsächlich oder mutmaßlich von Cyberangriffen betroffenen Unternehmen



Angaben in Prozent; * 2017/2019: letzte zwei Jahre; ab 2021: letzte zwölf Monate

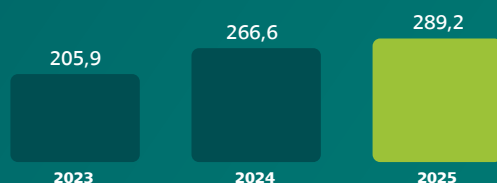
Großteil der Firmen beunruhigt

Wie Unternehmen die Bedrohungslage einstufen



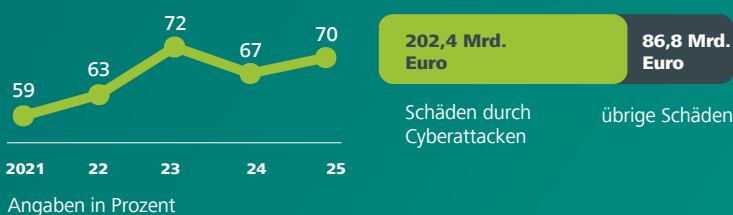
Der wirtschaftliche Schaden wächst ...

Schäden durch Diebstahl, Industriespionage und Sabotage (in Mrd. Euro)



... der Anteil am Gesamtschaden auch

Anteil der durch Cyberangriffe verursachten Schäden am Gesamtschaden



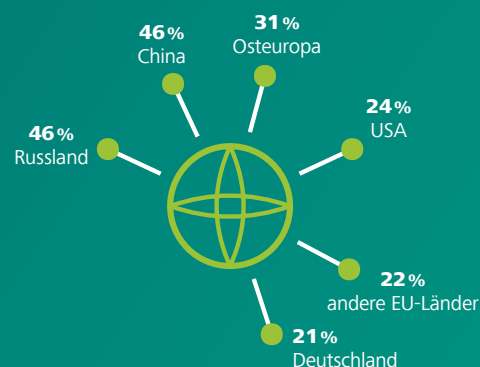
Sabotieren, stehlen, ausspähen

Cyberangriffe, von denen Unternehmen in den vergangenen zwölf Monaten betroffen waren (Mehrfachnennungen möglich)



Viele Attacken aus Russland und China

Regionen, denen Cyberangriffe auf deutsche Unternehmen zugeordnet werden konnten (Mehrfachnennungen möglich)



Schadsoftware und Bot-Attacken

Cyberangriffe, die bei Firmen in den vergangenen zwölf Monaten Schäden verursacht haben





Liebe Leserinnen und Leser,

45 Millionen Euro – so hoch war die Strafe, die ein Telekommunikationskonzern im vergangenen Jahr zahlen musste. Der Grund? Datenschutzverstöße. Auch wenn eine Strafe in dieser Höhe bislang die Ausnahme ist, macht der Fall deutlich, wie wichtig der verantwortungsvolle Umgang mit personenbezogenen Daten ist.

Datenschutz begegnet uns täglich. An Cookie-Banner haben wir uns längst gewöhnt, Onlinebestellungen gehören für viele zum Alltag. Wir geben Daten an, teilen sie mit Anbietern und vertrauen darauf, dass sie dort sicher sind.

Was im Alltag selbstverständlich erscheint, ist für Unternehmen und Kanzleien mit klaren rechtlichen Anforderungen verbunden. Verschiedene Gesetze und Regelungen geben dafür den Rahmen vor. In dieser Ausgabe zeigen wir, wie diese zusammenspielen, welche Anforderungen für Steuerberater sich daraus ergeben und wie Sie sich in Ihrer Kanzlei vor Datenschutzvorfällen schützen können.

**VIEL SPASS BEIM LESEN
WÜNSCHT IHNEN**

KATHRIN RITTER
Chefredakteurin DATEV magazin

FOLGEN SIE UNS



In dieser Ausgabe



Perspektiven

Warum digitale Identitäten zu einer Schlüsseltechnologie für den Berufsstand werden, erklärt DATEV-CEO Prof. Dr. Robert Mayr. → Seite 8

FOKUS

- 10 Datenschutz**
Was der neue EU-Rechtsrahmen für Steuerberater heißt.
- 17 Datensouveränität**
Wie DATEV die Integrität ihrer IT-Systeme sicherstellt.
- 18 Datenlecks**
Wie Sie Sicherheitslücken im Alltag finden und abstellen.
- 20 Datenattacke**
Die Systeme geschützt und trotzdem gehackt: ein Praxisbericht.
- 23 Datensicherheit**
Ist Ihre Kanzlei ausreichend auf Cyberangriffe vorbereitet?
- 24 Interview**
Prof. Dr. Tobias Keber über digitale Kompetenzen und menschliche Kontrolle.

PRAXIS

- 26 Firmensanierung**
Wie Verlustvorträge Unternehmen retten.
- 29 Influencer**
Worauf Steuerberater bei diesen Mandanten achten müssen.





FOTOS: DANIEL TKATSCHE, LEFDI BW, KANZLEI MUSCHKE; ILLUSTRATIONEN: ALEXANDER GLANDIEN, MINA KIM, JSTUDIOS/GETTY IMAGES

- 30 Minijobs**
Diese Fallstricke sollten Berater und Mandanten kennen.

DATEV

- 32 Cloudtransformation**
Wie läuft die Umstellung konkret ab? Ein Pilotanwender erzählt.
- 34 Vertreterrat**
Antworten auf die wichtigsten Fragen zur Cloudumstellung.
- 35 Kolumne**
Standards machen vieles einfacher, findet Dr. Markus Algner.
- 36 Eine von uns**
Beharrlich bis zur eigenen Kanzlei.

STANDARDS

- 02** Zahlen, bitte
- 03** Editorial
- 06** Register
- 38** Recht kurios, Impressum
- 39** Update

Mehr entdecken



Fachinformationen für Fachleute

Viele Leser schätzen die Fachbeiträge im DATEV magazin, in denen Steuer- und Rechtsexperten ein konkretes Problem aus ihrem Fachgebiet ausführlich erläutern. Mehr dazu finden Sie auf unserer Website.



→ go.datev.de/praxis

Experten in dieser Ausgabe:



Marius Siemen

Der Münchner Rechtsanwalt weiß, wie aus Verlusten der Vergangenheit die Basis für die Zukunft wird: → **Seite 26**



Dr. Susanne Grimm

Beim Influencer-Marketing müssen alle Beteiligten einiges beachten, erläutert die Rechtsanwältin: → **Seite 29**



Benjamin Onnis

Minijobs haben enge Grenzen. Wer die nicht kennt, bekommt Probleme, erläutert der Rechtsanwalt: → **Seite 30**



Volker Andres

Viele Mitglieder haben Fragen zur Cloud. Der stellvertretende Vorsitzende des Vertreterrats hat Antworten: → **Seite 34**



Register

WISSEN, WAS
WICHTIG WIRD

Fakten für Fachleute



Fachbuch zur betrieblichen Altersversorgung

Das Zweite Betriebsrentenstärkungsgesetz gibt der bAV neue Impulse. Das Buch führt praxisnah durch die Möglichkeiten und zeigt Fallstricke sowie Gestaltungsmöglichkeiten auf.

→ datev.de/shop/35899



EU-weite E-Rechnung kommt 2030

Die E-Rechnung wird in Europa zum Standard. Erfahren Sie, welche Regeln schon jetzt in den EU-Staaten gelten und wie der grenzüberschreitende Rechnungsaustausch gelingt.

→ go.datev.de/e-rechnung-in-europa



DATEV-Marktplatz Expo online 2026

Rund 60 DATEV-Marktplatz Partner stellen am 12. November ihre Lösungen im Zusammenspiel mit DATEV-Software vor. Jetzt kostenfrei anmelden:

→ go.datev.de/marktplatz-expo



WISSEN

Weiterbildung rund um den Jahreswechsel

Seminare und Fachliteratur von DATEV unterstützen Sie dabei, sich gut auf die anstehenden Neuregelungen zum Jahreswechsel vorzubereiten. Ob Personalwirtschaft oder Steuern – frischen Sie Ihr Wissen auf, und bauen Sie Ihre Kompetenz weiter aus. Einen Überblick über alle Angebote finden Sie unter → go.datev.de/jahreswechsel-weiterbildung

Digitale Entgeltunterlagen werden Pflicht

Führen Sie oder Ihre Mandanten Personalunterlagen noch in Papierform? Vom 1. Januar 2027 an müssen alle Arbeitgeber relevante Entgeltunterlagen elektronisch führen. Bis dahin mögliche Befreiungen von der Pflicht enden zum 31. Dezember 2026. Die Unterlagen müssen dem jeweiligen Beschäftigten eindeutig zugeordnet, vollständig und für eine Betriebsprüfung digital verfügbar sein. Mit DATEV Personal sind Arbeitgeber optimal vorbereitet. Alle relevanten Infos finden Sie kompakt zusammengefasst in einem Whitepaper, das Sie hier kostenlos herunterladen können:
→ go.datev.de/datev-personal



KOMPAKTWISSEN Grundsteuer

Das Buch gibt einen Überblick zur aktuellen Rechtslage unter Berücksichtigung der anhängigen und bereits entschiedenen Gerichtsverfahren. Außerdem erhalten Sie Informationen zu wesentlichen Entwicklungen in der Besteuerungs- und Beratungspraxis.

→ datev.de/shop/34151

SPEKTRUM MITTELSTAND

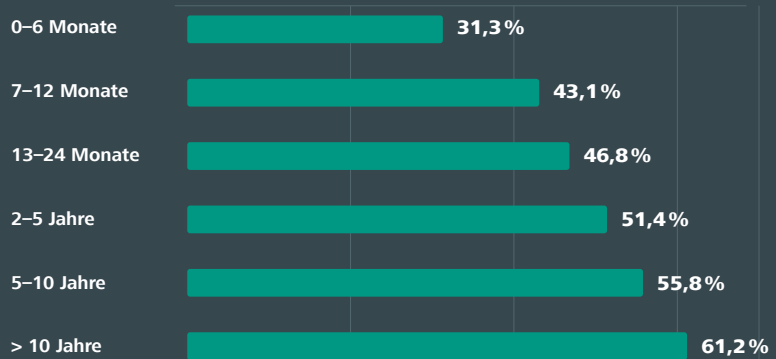
Entlastung mit Nebenwirkung

Die Inflationsausgleichsprämie (IAP) sollte Mitarbeiterinnen und Mitarbeiter angesichts der stark gestiegenen Energie- und Lebenshaltungskosten entlasten. Das aktuelle DATEV Spotlight 4/2026 „Zwischen Entlastung und Mitnahmeeffekten: eine Bilanz der Inflationsausgleichsprämie“ zeigt jedoch: Im Mittelstand wurde die Prämie nicht nur als sozialpolitisches Entlastungsinstrument genutzt. Häufigkeit und Höhe der Zahlungen folgten deutlich der Logik von Mitarbeiterbindung, Qualifikation und finanzieller Leistungsfähigkeit der Unternehmen.

So erhielten Beschäftigte mit höherem Einkommen, längerer Betriebszugehörigkeit und anspruchsvolleren Tätigkeiten häufigere und höhere Prämien als Beschäftigte mit niedrigem Einkommen oder einfachen Tätigkeiten. Jene Gruppen, die von Energiepreisschocks besonders stark betroffen sind, wurden damit nur begrenzt erreicht. Die Ergebnisse zeigen die Nützlichkeit und Bedeutung der DATEV Mittelstandsindex-Daten für die Beurteilung wirtschafts- und steuerpolitischer Maßnahmen. Unternehmen reagieren auf politische Anreize häufig anders als von der Politik erwartet.

Langjährige Mitarbeiter bekommen mehr

Anteil der IAP-Empfänger nach Dauer der Betriebszugehörigkeit



Quelle: DATEV Economics; dargestellt ist der Anteil an den Beschäftigten, die mindestens eine Inflationsausgleichsprämienzahlung erhalten haben

DATEV Economics⁷

→ go.datev.de/economics → go.datev.de/spotlights

© Copyright DATEV Mittelstandsindex/DATEV eG



Aktuelle Daten und Zahlen, auch nach IHK-Regionen im geschützten Mitgliederbereich, finden Sie unter: → mittelstandsindex.datev.de

„Vertrauen braucht eine Identität“

Digitale Identitäten sind weit mehr als nur der Personalausweis auf dem Smartphone. Sie können zu einer Schlüsseltechnologie für sichere, durchgängige Prozesse werden – gerade für unseren Berufsstand.



Können Sie sich noch erinnern, wie wir vor 25 Jahren gearbeitet haben? Ich war damals noch nicht lange Steuerberater. Papier, Stempel und Faxgerät gehörten zum Alltag. Auch Identität und Vertretungsberechtigung waren meist an Papier gebunden: Ausweis vorlegen, Vollmacht unterschreiben, Dokument kopieren, ablegen, prüfen.

Heute sind viele Prozesse digital. Eine entscheidende Frage ist erstaunlich oft analog geblieben: Woher weiß ein digitales System zuverlässig, wer da vor ihm sitzt und für wen diese Person handeln darf? Deshalb halte ich die Entwicklung rund um digitale Identitäten für strategisch so bedeutsam.

Nicht der Ausweis ist entscheidend

Mit der European Digital Identity Wallet, kurz EUDI-Wallet, entsteht eine europaweit nutzbare Infrastruktur für digitale Identitäten. Deutschland will Anfang 2027 mit einer ersten Ausbaustufe starten. Perspektivisch sollen sich damit neben der eigenen Identität auch Nachweise und berufliche Eigenschaften digital belegen lassen. Der eigentliche Fortschritt liegt für mich aber nicht darin, dass der Personalausweis aufs Smartphone wandert. Entscheidend ist, dass Vertrauen maschinenlesbar wird. Denn für unseren Berufsstand ist nicht nur wichtig, wer jemand ist. Mindestens genauso wichtig ist: In welcher Rolle handelt diese Person, und wen darf sie vertreten?

An diesem Punkt wird es spannend. Denn Steuerberaterinnen und Steuerberater handeln täglich im Auftrag anderer. Dabei müssen private und berufliche Identität sauber getrennt sein.

Heute verteilen sich Identität, Vollmacht und Berechtigung häufig noch auf unterschiedliche Systeme und Nachweise. Die geplante European Business Wallet könnte diese Lücke schließen. Sie soll Unternehmen und Organisationen ermöglichen, Identitäten, Rollen, Vertretungsrechte und Nachweise digital und vertrauenswürdig bereitzustellen. In diesem Zusammenspiel liegt für mich der eigentliche Paradigmenwechsel:



Prof. Dr. Robert Mayr ist CEO der DATEV eG sowie Steuerberater und Wirtschaftsprüfer.



Vernetzen Sie sich mit Prof. Dr. Robert Mayr auf LinkedIn.



Die EUDI-Wallet weist nach, wer ich bin. Die Business Wallet kann ergänzen, für wen und in welcher Rolle ich handle. Damit könnten Mandatsaufnahme, Vollmachten, Signaturen, Behördenkontakte oder die Prüfung von Geschäftspartnern künftig durchgängig digital und grenzüberschreitend funktionieren.

Das passt zu einer Überzeugung, die mich seit Langem begleitet: Digitalisierung entfaltet ihren Nutzen nicht durch digitale Inseln, sondern durch eine umfassende Vernetzung. Für DATEV eröffnet das konkrete Perspektiven, etwa beim digitalen Onboarding, bei der E-Rechnung oder beim Management von Rollen, Rechten und Vollmachten.

Gemeinsam mit Kammern und Partnern können wir dazu beitragen, berufliche Eigenschaften und Vertretungsberechtigungen sicher in Fachprozesse zu integrieren. Ich sehe darin die Chance, unseren Berufsstand zum Vorreiter für praxistaugliche digitale Identitäten zu machen.

Vertrauen bleibt die Währung

Natürlich müssen wir in diesem Zusammenhang über Sicherheit, Datenschutz, Haftung und Nutzerfreundlichkeit sprechen. Gerade weil digitale Identitäten zur kritischen Infrastruktur werden können, sind diese Fragen nicht verhandelbar.

Aber wir sollten nicht nur über die Risiken sprechen. Wir sollten diese Infrastruktur aktiv mitgestalten, statt darauf zu warten, dass andere die Standards für uns definieren. Denn wenn uns das gelingt, digitalisieren wir nicht einfach den Ausweis. Wir schaffen eine Infrastruktur, die unseren Berufsstand entlasten, Medienbrüche beseitigen und neue durchgängige Prozesse ermöglichen kann.

Aus Vertrauen wird dann digitale Infrastruktur, und aus Regulierung wird echter Fortschritt. ○

**Herzlich
Robert Mayr**

Nürnberg, im August 2026



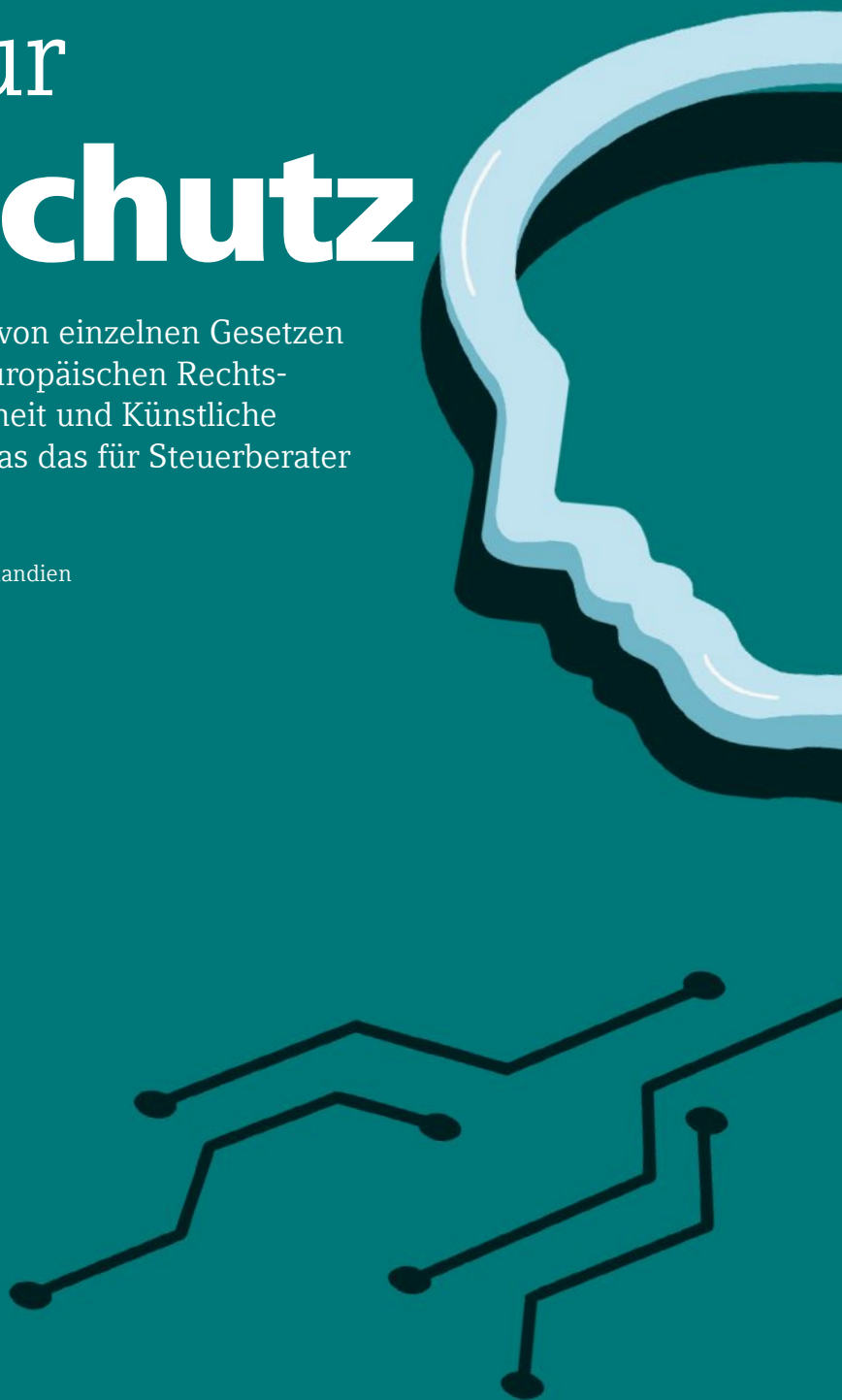
Mehr als nur Datenschutz

Die Digitalisierung wird nicht mehr von einzelnen Gesetzen geregelt. Die EU entwickelt einen europäischen Rechtsrahmen, der Datenschutz, IT-Sicherheit und Künstliche Intelligenz zusammen betrachtet. Was das für Steuerberater und Kanzleien bedeutet.

Text: Walter Deinzer **Illustrationen:** Alexander Glandien

Der erste Mandant hat seine Unterlagen bereits über die Web-Anwendung DATEV Unternehmen online hochgeladen. Im Büro nebenan werden Lohnabrechnungen erstellt, während eine Kollegin den Entwurf eines Schreibens mit Unterstützung von KI überarbeitet. Dokumente werden digital archiviert, Daten zwischen verschiedenen Anwendungen mit Mandanten zur Weiterverarbeitung ausgetauscht.

Für Steuerkanzleien ist das längst Alltag. Kaum jemand denkt bei diesen Arbeitsschritten an europäische Gesetzgebung. Tatsächlich gelten für viele dieser Prozesse heute aber unterschiedliche regulatorische Vorgaben. Die Datenschutz-Grundverordnung (DS-GVO) regelt den Umgang mit personenbezogenen Daten. Der AI Act formuliert Vorgaben für den Umgang mit Künstlicher Intelligenz. NIS2 stellt höhere Anforderungen an die Cybersicherheit. Mit dem Data Act sollen Daten besser nutzbar werden. Hinzu kommen weitere europäische Regelwerke wie DORA, der Cyber Resilience Act oder die Entgelttransparenzrichtlinie. »







”

Die Anzahl an regulatorischen Vorgaben wächst. Der Gesetzgeber ist gefordert, dadurch auch Rechtssicherheit zu schaffen.

“

RUDI KRAMER

Fachberater und stellvertretender Datenschutzbeauftragter der DATEV eG

Jedes dieser Gesetze verfolgt einen eigenen Zweck. Gemeinsam verändern sie jedoch die Rahmenbedingungen, unter denen Steuerkanzleien arbeiten.

Vor gut zehn Jahren, im April 2016, wurde die Datenschutz-Grundverordnung im Amtsblatt der Europäischen Union veröffentlicht. Zwei Jahre später wurde sie unmittelbar geltendes Recht in allen Mitgliedstaaten. Viele ihrer Grundgedanken waren bereits in der europäischen Datenschutzrichtlinie von 1995 angelegt und lassen sich auf Artikel 8 der Charta der Grundrechte der Europäischen Union zurückführen. Dennoch bedeutete die DS-GVO für Unternehmen und freie Berufe einen tiefgreifenden Wandel.

Zahlreiche Anforderungen mussten erstmals umgesetzt werden. Gleichzeitig entstanden neue Auslegungsfragen. Orientierung bei deren Klärung gaben Leitlinien des Europäischen Datenschutzausschusses, Entscheidungen der Datenschutzaufsichtsbehörden oder Urteile des Europäischen Gerichtshofs. Auch der nationale Gesetzgeber griff an einzelnen Stellen ein. Für Steuerberater sorgte § 11 Steuerberatungsgesetz für Klarheit bei der datenschutzrechtlichen Einordnung des Mandatsverhältnisses.

Die DS-GVO wird weiterentwickelt

Auch wenn die umfangreichen Dokumentationspflichten das sichtbarste Element der DS-GVO sind, reicht ihre grundlegende Intention jedoch

weit darüber hinaus. Datenschutz soll sicherstellen, dass Menschen in Bezug auf über sie gespeicherte Informationen rechtmäßig behandelt werden und Transparenz einfordern können. Betroffenenrechte wie Auskunft oder Berichtigung sind Ausdruck dieses Schutzgedankens. Gerade für Steuerkanzleien ist dieser Ansatz von besonderer Bedeutung. Das Vertrauensverhältnis zwischen Mandant und Berater setzt voraus, dass personenbezogene Informationen verantwortungsvoll verarbeitet werden.

Die DS-GVO steht also klar im Dienst der einzelnen Person. Und sie schafft Rechtssicherheit für Einheiten, die personenbezogene Daten verarbeiten wollen oder müssen. In der öffentlichen Diskussion wurde sie dennoch häufig auf ihren bürokratischen Aufwand reduziert. Zehn Jahre nach ihrem Inkrafttreten stellt sich daher die Frage, ob einzelne Regelungen noch zeitgemäß und praxistauglich sind – oder weiterentwickelt werden sollten. „Die Anzahl an regulatorischen Vorgaben wächst“, sagt Rudi Kramer, Fachberater

FOTO: HENDRIK SCHMAHL



KOMPAKT-WISSEN

Alles Wichtige für Ihre Praxis lesen Sie in *Datenschutzrecht für Berater* (StB, RA, WP)
→ datev.de/shop/35940



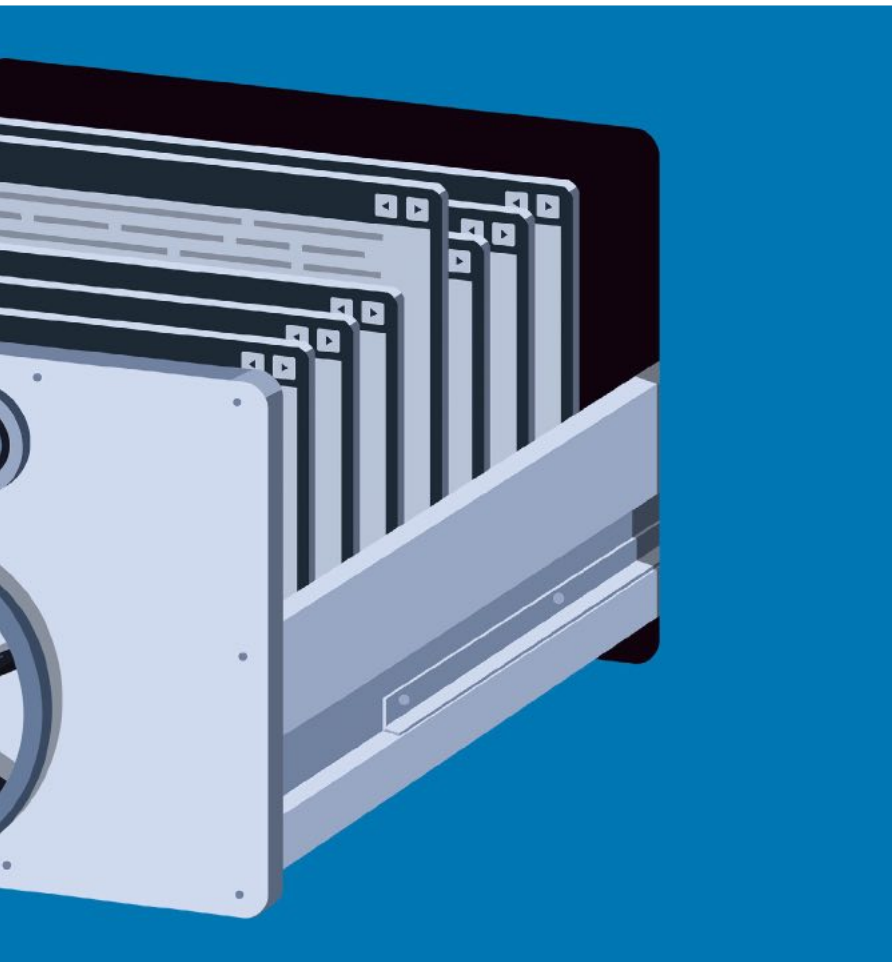
und stellvertretender Datenschutzbeauftragter der DATEV eG sowie Leiter des Arbeitskreises Datenschutz und Informationssicherheit bei der Arbeitsgemeinschaft für wirtschaftliche Verwaltung (AWV). „Der Gesetzgeber ist gefordert, dadurch auch Rechtssicherheit zu schaffen.“

Diese Diskussion hat die Europäische Kommission aufgegriffen. Der im November 2025 vorgestellten Digitale Omnibus soll bestehende digitale Regelwerke vereinfachen und besser aufeinander abstimmen. Besonders weitreichend sind dabei die vorgeschlagenen Änderungen an der Datenschutz-Grundverordnung.

Unter anderem soll die Verarbeitung personenbezogener Daten für die Entwicklung und den Betrieb von KI-Systemen unter bestimmten Voraussetzungen auf das sogenannte berechnete Interesse gestützt werden können. Außerdem schlägt die Kommission vor, die Verarbeitung sensibler Daten für die Entwicklung und den Betrieb von KI-Systemen ausdrücklich zuzulassen, sofern strenge technische und organisatori- »



Ordnung schaffen:
Die digitalen Regelwerke der EU sollen besser aufeinander abgestimmt werden.



Sicherheitsvorfall vs. Datenschutzvorfall

Nicht jeder Verstoß gegen IT-Sicherheitsregeln ist schon ein Datenschutzvorfall. Doch was ist zu tun, wenn es doch passiert?

1 Jedes Ereignis, das die Vertraulichkeit, Integrität oder Verfügbarkeit von Daten oder IT-Systemen angreift, gilt als Sicherheitsvorfall. Eine Datenschutzverletzung liegt vor, wenn personenbezogene Daten unrechtmäßig verändert werden, verloren gehen oder unbefugt eingesehen werden können.

2 Tritt ein Datenschutzverstoß ein, muss der datenschutzrechtlich Verantwortliche prüfen, welche Daten betroffen sind und welche Folgen für die betroffenen Personen entstehen können. Jeder Datenschutzvorfall muss dokumentiert werden, ebenso die Bewertung und die ergriffenen Maßnahmen.

3 Besteht ein Risiko für die Rechte und Freiheiten der betroffenen Personen, muss der Verantwortliche den Vorfall binnen 72 Stunden der Aufsichtsbehörde melden. Bei einem hohen Risiko müssen auch die betroffenen Personen informiert werden, um sich vor möglichen Folgen wie Betrugsversuchen oder Identitätsdiebstahl schützen zu können. Auftragsverarbeiter müssen den Auftraggeber informieren, damit dieser seinen Pflichten nachkommen kann.

4 Neben den datenschutzrechtlichen Vorgaben können je nach Branche und Art des Vorfalls weitere Meldepflichten bestehen, etwa für Finanzdienstleister oder aufgrund der NIS2-Richtlinie. Wer den Vorfall verursacht hat, ist aus rechtlicher Sicht zunächst unerheblich. Verantwortlich im datenschutzrechtlichen Sinn ist stets die Stelle, die über die Datenverarbeitung entscheidet.

sche Schutzmaßnahmen eingehalten werden. So soll der Rechtsrahmen innovationsfreundlicher werden, ohne das Datenschutzniveau grundsätzlich infrage zu stellen.

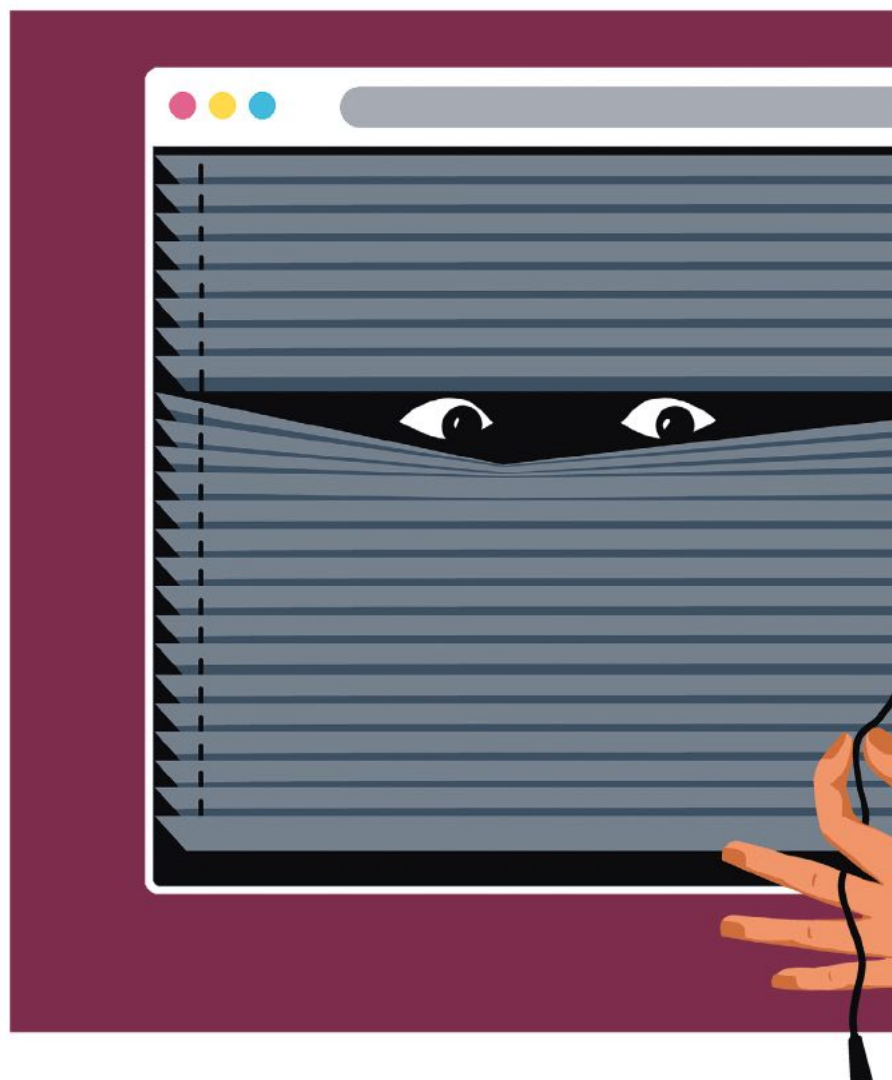
Der Digitale Omnibus greift darüber hinaus zahlreiche Erfahrungen aus zehn Jahren DS-GVO-Praxis auf. Vorgesehen sind unter anderem stärker risikobasierte Meldepflichten bei Datenschutzverletzungen sowie Maßnahmen gegen missbräuchliche oder exzessive Auskunftsanfragen. Auch Rechtsprechung des Europäischen Gerichtshofs soll unmittelbar im Gesetz nachvollzogen werden, um mehr Rechtssicherheit bei der Anwendung der DS-GVO zu schaffen.

Ergebnisse nicht vor Mitte 2027

Der Ansatz kommt grundsätzlich positiv an. Er greift praktische Anwendungsprobleme auf; datenbasierte Innovationen könnten durch die vorgeschlagenen Änderungen erleichtert werden. Gleichzeitig bleiben wesentliche Fragen offen. Dazu zählen unter anderem, wie sich die neuen Regelungen technologieoffen gestalten lassen, wie mit anonymisierten und pseudonymisierten Daten umzugehen ist oder wie digitale Produkte weiterentwickelt sowie das Zusammenspiel zwischen Verantwortlichen und Auftragsverarbeitern entlang der gesamten Datenverarbeitungskette ausgestaltet werden können.

Noch handelt es sich um einen Vorschlag der Europäischen Kommission. Der Rat der Europäischen Union und das Europäische Parlament werden ihre Positionen dazu entwickeln und dann im Trilog über einen Kompromiss verhandeln. Dementsprechend ist nicht vor Mitte 2027 mit einem Abschluss des Gesetzgebungsverfahrens zu rechnen. „Die Digital-Omnibus-Initiative soll die DS-GVO vereinfachen“, sagt Dr. Johannes Niklas Holtz vom DATEV EU Office. „Ob daraus eine spürbare Entlastung für Unternehmen entsteht, wird das weitere Gesetzgebungsverfahren zeigen.“

Während die DS-GVO angepasst wird, um den damit verbundenen Aufwand zu senken, sind die Anforderungen für die digitale Wirtschaft im europäischen Rechtsraum insgesamt in den vergangenen Jahren deutlich gestiegen und tun dies weiter. Die Network and Information Security Directive 2 – bekannt als NIS2 – verstärkt die Anforderungen an Cybersicherheit. Sie steht in einer Reihe europäischer Maßnahmen zur Stärkung der Cyber- und Informationssicherheit. Bereits 2016 trat die erste NIS-Richtlinie in Kraft. Sie verpflichtete Betreiber Kritischer Infrastrukturen und bestimmter digitaler Dienste zu Mindest-

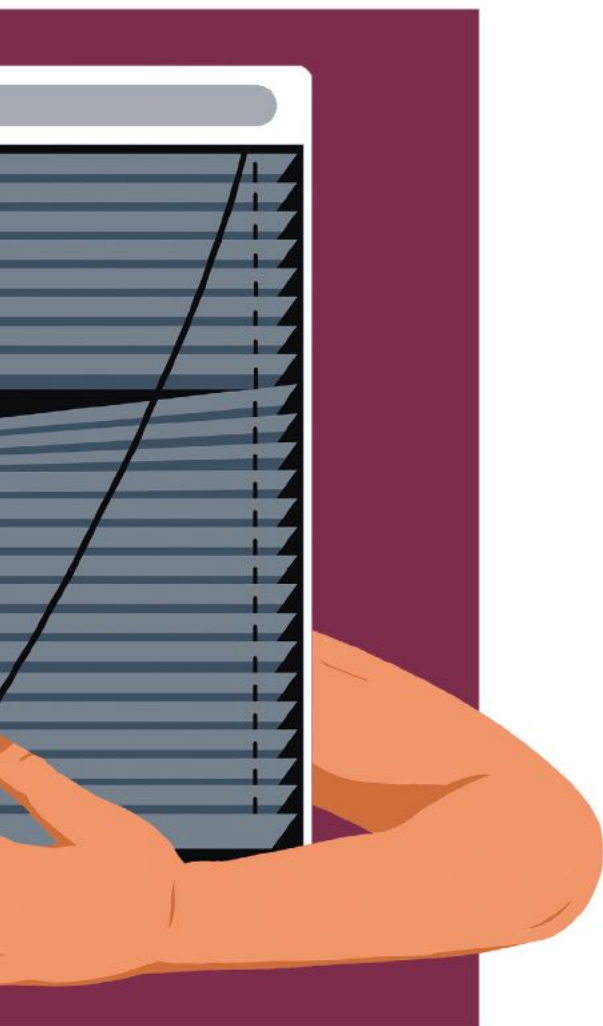


”

Ob aus der Vereinfachung eine Entlastung für Unternehmen entsteht, wird das Gesetzgebungsverfahren zeigen.

“

DR. JOHANNES NIKLAS HOLTZ
DATEV EU Office



maßnahmen der Informationssicherheit und zur Meldung erheblicher Sicherheitsvorfälle. Mit der fortschreitenden Digitalisierung und einer wachsenden Bedrohungslage durch Cyberangriffe stieß dieser Rechtsrahmen jedoch zunehmend an seine Grenzen. Die EU verabschiedete deshalb Ende 2022 die umfassende Weiterentwicklung NIS2.

Diese Richtlinie verfolgt das Ziel, ein europaweit einheitlich hohes Cybersicherheitsniveau zu schaffen. Entsprechend wurden die Anforderungen an Governance, Risikomanagement, Lieferketten-sicherheit, Krisenmanagement und die Meldepflichten verschärft. Gefordert wird nicht nur die Einführung von Schutzmaßnahmen, sondern auch deren nachvollziehbare Steuerung, Kontrolle und Dokumentation. Durch die starke Einbindung der Unternehmensleitung wird Cybersicher- »

Rechte und Pflichten

Die Datenschutz-Grundverordnung (DS-GVO) räumt allen Menschen weitreichende Rechte ein zu erfahren, was mit ihren persönlichen Daten passiert. Alle Institutionen, die Daten speichern und verarbeiten, haben entsprechende Pflichten. Ein Überblick.

Text: Rudi Kramer

Auskunftsrecht Jede natürliche Person hat das Recht, unter anderem zu erfahren, ob und welche personenbezogenen Daten über sie verarbeitet werden. Auskunftspflichtig ist der datenschutzrechtlich Verantwortliche, also die Stelle, die über den Zweck und die Art und Weise der Datenverarbeitung entscheidet.

Anspruch auf Inhalte Dies umfasst nicht nur die Frage, ob personenbezogene Daten verarbeitet werden, sondern auch, welche und zu welchem Zweck sie genutzt werden. Auch wenn bisher keine personenbezogenen Daten vorhanden sind, muss die Anfrage beantwortet werden. Dann wird eine sogenannte Negativauskunft erteilt, und die Daten aus der Anfrage werden beauskunftet.

Klare Fristen Die Auskunft muss unverzüglich, spätestens aber innerhalb eines Monats erteilt werden. Ist die Bearbeitung komplex oder liegen sehr viele Anfragen vor, kann die Frist um bis zu zwei weitere Monate verlängert werden. Die betroffene Person muss darüber mit einer Begründung innerhalb der ersten Monatsfrist informiert werden.

Dokumentenherausgabe Anspruch auf vollständige Dokumente oder Akten haben

Antragsteller nur, wenn diese erforderlich sind, damit die personenbezogenen Daten verständlich eingeordnet werden können. Das hat der Europäische Gerichtshof entschieden (EuGH, 4. Mai 2023, C-487/21). Gleichzeitig dürfen durch die Herausgabe keine Rechte Dritter verletzt werden. Dazu gehören insbesondere Geschäftsgeheimnisse, geistiges Eigentum oder urheberrechtlich geschützte Inhalte.

Begründung Aus welchem Grund eine Person Auskunft verlangt, spielt grundsätzlich keine Rolle. Allerdings kann sich ein Unternehmen in Ausnahmefällen darauf berufen, dass ein Auskunftersuchen rechtsmissbräuchlich gestellt wurde, etwa wenn es nachvollziehbar darlegen kann, dass die Auskunft ausschließlich zur Vorbereitung eines Schadenersatzanspruchs verlangt wird (Amtsgericht Arnsberg, 1. Juli 2026, Az. 42 C 434/23).

Zuständigkeit Geht eine Anfrage nicht beim Verantwortlichen, sondern bei einem Auftragsverarbeiter ein, muss dieser die Anfrage an den datenschutzrechtlich Verantwortlichen weiterleiten, sofern dieser aus der Anfrage erkennbar ist. Er muss schließlich die Auskunft erteilen.



”
KRITIS-Vorgaben betrachten vor allem einzelne kritische Dienstleistungen und Anlagen, NIS2 die Organisation als Ganzes.
“

CLAUDIA TOPINKA

Expertin Informationssicherheit bei DATEV

heit zudem ausdrücklich zur Führungsaufgabe. „KRITIS-Vorgaben betrachten vor allem einzelne kritische Dienstleistungen und Anlagen, NIS2 die Organisation als Ganzes“, sagt Claudia Topinka, Expertin für Informationssicherheit bei DATEV.

Ihre Wirkung entfaltet NIS2 jedoch nicht nur bei den unmittelbar betroffenen Einrichtungen, sondern auch entlang digitaler Wertschöpfungs- und Dienstleistungsketten. Hintergrund ist der deutlich stärkere Fokus auf Abhängigkeiten von externen Dienstleistern und Geschäftspartnern. Betroffene Unternehmen müssen daher bewerten, welche Risiken von diesen ausgehen und entsprechende Sicherheitsanforderungen vertraglich und organisatorisch absichern. Dadurch können auch Unternehmen und Kanzleien, die selbst nicht unter NIS2 fallen, vermehrt mit Sicherheitsfragebögen, Auditanfragen oder Nachweisforderungen ihrer Mandanten und Kunden konfrontiert werden.

Mit NIS2 ist die Entwicklung allerdings nicht abgeschlossen. Die Richtlinie steht exemplarisch für eine europäische Regulierung, die Fragen der Digitalisierung, Informationssicherheit und Resilienz zunehmend in den Fokus rückt. Gleichzeitig sehen sich Unternehmen einer wachsenden Zahl weiterer regulatorischer Anforderungen gegenüber. Die Herausforderung besteht daher nicht nur in der Umsetzung der Regelwerke, sondern auch darin, den Überblick über ein zunehmend komplexes regulatorisches Umfeld zu behalten.

Für Kanzleien bedeutet das einen Perspektivwechsel. Datenschutz bleibt ein zentrales Element,



Walter Deinzer

ist seit 2022 Datenschutzbeauftragter der DATEV eG und beschäftigt sich mit der Umsetzung von Datenschutz und regulatorischen Anforderungen in der Praxis, insbesondere an der Schnittstelle von Recht und Technologie.

wird aber Teil eines größeren Ganzen. Informationssicherheit, Datennutzung, digitale Resilienz und verantwortungsvoller Technologieeinsatz lassen sich immer weniger getrennt betrachten.

Diese Entwicklung spiegelt sich unmittelbar im Kanzleialltag wider. Der Einsatz Künstlicher Intelligenz wirft neue datenschutzrechtliche Fragen auf. Immer raffiniertere Cyberangriffe machen Informationssicherheit zur organisatorischen Aufgabe. Neue regulatorische Anforderungen müssen in bestehende Prozesse integriert werden. Datenschutz wird damit zunehmend zum verbindenden Element zwischen Recht, Organisation und Technologie.

Die Anforderungen an Kanzleien verändern sich nicht durch ein einzelnes Gesetz. Sie verändern sich, weil Europa den digitalen Rechtsrahmen weiterentwickelt. Wer diese Entwicklung versteht, kann regulatorische Anforderungen besser einordnen und die Digitalisierung seiner Kanzlei sicher und verantwortungsvoll gestalten. ○

Nachweisbar sicher

Wer sensible Steuer-, Finanz- und Personendaten verarbeitet, trägt besondere Verantwortung. DS-GVO, NIS2, DORA und Cyber Resilience Act erweitern die Anforderungen an Datenschutz, Informationssicherheit und Resilienz.

Text: Sabine Wächter

DATEV als Auftragsverarbeiter ist in der Pflicht, personenbezogene und geschäftskritische Informationen zu schützen. Datenschutz, Informationssicherheit und Compliance müssen so organisiert sein, dass sie dauerhaft wirksam bleiben und sich gegenüber Kunden, Partnern und Aufsichtsbehörden transparent nachweisen lassen. Grundlage dafür ist ein integriertes Datenschutz- und Informationssicherheitsmanagementsystem, das Prozesse, Verantwortlichkeiten, Risikomanagement und Kontrollen verbindet. Ergänzt wird es durch Schulungs- und Awareness-Maßnahmen, die den sicheren Umgang mit Informationen unterstützen.

DATEV verfolgt eine langfristige Zertifizierungsstrategie und lässt Compliance-, Datenschutz- und Informationssicherheitsprozesse regelmäßig durch unabhängige Auditoren und Zertifizierungsstellen überprüfen. Zertifizierungen nach ISO 27001, ISO 27017 und ISO 27701 bestätigen, dass DATEV Datenschutz- und Informationssicherheitsanforderungen systematisch in ihren Prozessen verankert hat. Insbesondere durch die Erweiterung um die Zertifizierung nach

ISO 27017 belegt DATEV zusätzlich die sichere Nutzung und Bereitstellung von Cloudservices und stellt ergänzend für ausgewählte Dienstleistungen ISAE-3402-Testate bereit. Während Zertifizierungen Aufbau und Wirksamkeit von Managementsystemen bestätigen, beweisen die Prüfberichte, dass definierte Kontrollen und Prozesse über einen längeren Zeitraum funktioniert haben. Sie gewinnen zunehmend an Bedeutung.

Die Zertifizierungen, Prüfberichte und Testate dienen als nachvollziehbare Belege für Datenschutz, Informationssicherheit und Compliance. Sie helfen auch Mitgliedern und Kunden dabei, ihre eigenen gesetzlichen und regulatorischen Anforderungen zu erfüllen. Denn diese müssen die Sicherheits- und Datenschutzmaßnahmen von DATEV als ihren Auftragsverarbeiter und der von DATEV eingesetzten Subdienstleister regelmäßig nachvollziehen und dokumentieren.



Weitere Infos und Zertifikate der DATEV eG
→ go.datev.de/zertifizierungen



Sabine Wächter

ist Abteilungsleiterin Datenschutz und Zertifizierung der DATEV eG. Für die studierte Softwareentwicklerin sind Datenschutz und Informationssicherheit die Grundlage für das Vertrauen, das die Genossenschaft bei den Kunden genießt.

Server oder Cloud? Kanzlei-IT zukunftsicher aufstellen

Eigene Server sind ressourcenintensiv und werden angesichts steigender Anforderungen zunehmend zur Belastung. Die Auslagerung von IT-Tätigkeiten bietet Kanzleien eine Alternative.

IT-Infrastruktur Für viele Kanzleien stellt sich die Frage, ob sich die Anschaffung eines eigenen lokalen Servers noch lohnt. Die Anforderungen steigen, Fachkräftemangel, höhere Sicherheitsstandards sowie Betrieb und Wartung einer eigenen IT-Infrastruktur binden Ressourcen. Zugleich haben der Boom Künstlicher Intelligenz (KI) sowie die hohe Nachfrage nach Hardware Preise und Lieferzeiten für Server erhöht.

Cloudsourcing schafft Freiräume Mit DATEVasp, SmartIT und PARTNERasp stehen Alternativen bereit. Kanzleien profitieren dabei von einer professionell betriebenen Infrastruktur, ohne selbst Serverhardware beschaffen und warten zu müssen. Planbare monatliche Kosten ersetzen hohe Einmalinvestitionen.

Zukunftsfähig Cloudsourcing erleichtert auch den Übergang von einer

serverzentrierten zu einer arbeitsplatzzentrierten IT. Damit werden die Voraussetzungen für Clouddienste, automatisierte Prozesse und den sicheren Einsatz von KI-gestützten Lösungen geschaffen. Denn die Sicherheit muss in der zukünftigen cloudbasierten Arbeitswelt stets dem Anwender folgen – unabhängig davon, von wo aus er auf Daten und Anwendungen zugreift.



Mehr zu den Cloud-Sourcing-Lösungen:
→ go.datev.de/it-outsourcing

6

kritische Risiken für den Datenschutz

Digitalisierung bringt ein hohes Maß an Verantwortung mit sich. Wie sich Schwachstellen im Kanzleialltag schnell erkennen und gezielt abstellen lassen.

Text: Marco Krapp

Steuerberatungskanzleien verwalten täglich besonders schützenswerte Daten: Finanzinformationen, Lohn- und Gehaltsdaten, persönliche Angaben und vertrauliche Unterlagen. Gleichzeitig wird der Arbeitsalltag immer digitaler – und damit wachsen die Sicherheitsrisiken. Die Gefahr entsteht dabei nicht nur durch Angriffe von außen. Oft sind es alltägliche Situationen, die den Datenschutz gefährden: ein ungeschütztes Endgerät, zu weit gefasste Zugriffsrechte, unbedachter Umgang mit Künstlicher Intelligenz oder eine Nachricht, die versehentlich an den falschen Empfänger geht. Auch analoge Unterlagen können zum Problem werden. Datenschutz ist deshalb keine reine IT-Aufgabe. Entscheidend sind Technik, klare Regeln und ein wachsamer Umgang mit sensiblen Informationen. Die größten Datenschutzfallen zeigen, wo sich genaues Hinsehen lohnt – und welche Risiken sich mit wenig Aufwand vermeiden lassen.



1

UNGESCHÜTZTE ENDGERÄTE

Notebook, Smartphone oder Tablet sind zentrale Arbeitsmittel. Werden Betriebssysteme nicht aktualisiert oder Schutzmechanismen unzureichend gepflegt, entstehen vermeidbare Sicherheitslücken. Gerade Ransomware nutzt häufig bereits bekannte Schwachstellen aus. Ein konsequentes Patch-Management und aktuelle Sicherheitslösungen gehören zu den wirksamsten Schutzmaßnahmen.

2

KI OHNE SPIELREGELN

Beim Einsatz generativer KI wird es kritisch, wenn personenbezogene oder mandatsbezogene Informationen in externe Anwendungen eingegeben werden. Schnell drohen dann Verstöße gegen das Datenschutzrecht und die berufsrechtliche Verschwiegenheitspflicht. Bevor Künstliche Intelligenz produktiv eingesetzt wird, sollte deshalb verbindlich festgelegt werden, welche Anwendungen zulässig sind und welche Daten damit verarbeitet werden dürfen.

3

ZU WEIT REICHENDE ZUGRIFFSRECHTE



Nicht jeder Mitarbeiter benötigt Zugriff auf alle Mandatsdaten. Fehlen Rollen- und Berechtigungskonzepte, steigt das Risiko unbeabsichtigter Einsichtnahmen ebenso wie das Missbrauchspotenzial. Zugriffsrechte sollten deshalb konsequent nach dem Need-to-know-Prinzip vergeben und regelmäßig überprüft werden.

4

FEHLENDES SICHERHEITSBEWUSSTSEIN

Technische Maßnahmen entfalten ihre Wirkung nur, wenn sie im Alltag konsequent angewendet werden. Neue Betrugsmaschinen, Social Engineering oder geänderte Arbeitsabläufe erfordern deshalb eine regelmäßige Sensibilisierung. Datenschutz ist eine Kompetenz, die kontinuierlich gepflegt und geschult werden muss.



Digitale Sicherheit: Datenschutz entfaltet seine Wirkung nur, wenn er konsequent gelebt wird – eine Kompetenz, die regelmäßig geschult werden muss.

5

E-MAIL ALS EINFALLSTOR

Noch immer beginnen viele Datenschutzvorfälle mit einer E-Mail. Falsche Adressierungen, unverschlüsselte Anhänge oder professionell gestaltete Phishing-Mails führen schnell dazu, dass vertrauliche Informationen in falsche Hände geraten. Sichere Kommunikationswege und etablierte Prüfprozesse reduzieren dieses Risiko erheblich.



6

ANALOGUE UNTERLAGEN AUS DEM BLICK VERLIEREN

Die Digitalisierung hat die Papierakte noch nicht vollständig ersetzt. Vergessene Ausdrucke am Drucker, offen herumliegende Akten oder in Besprechungsräumen verbliebene Notizen laden zu unbefugten Einblicken ein. Datenschutz endet deshalb nicht am Bildschirm. Auch für analoge Unterlagen braucht es klare Regeln zur Aufbewahrung, Nutzung und Vernichtung.





Die übersehene Tür

Die Kanzlei von Daniel Strathaus hatte Server geschützt, Mitarbeitende sensibilisiert und technische Vorkehrungen getroffen. Trotzdem gelang Angreifern der Zugriff. Nicht über das Netzwerk, sondern über die Website. Der Vorfall zeigt, warum auch ausgelagerte Systeme zur eigenen Sicherheitsarchitektur gehören.

Text: Dietmar Zeilinger **Fotos:** Severin Wohlleben

Die erste Nachricht wirkte wie eine plumpe Fälschung. Der Absender war ungewöhnlich geschrieben, der Text knapp, ein Link führte auf eine dubiose Adresse. Daniel Strathaus, Steuerberater und Partner in einer mittelständischen Kanzlei mit drei Berufsträgern und zwölf Mitarbeitern, reagierte, wie er selbst es seinem Team regelmäßig empfiehlt: Nicht klicken, die E-Mail löschen und auch den Papierkorb leeren. Kurz darauf meldete sich jedoch der Hosting-Anbieter. Er hatte die Kanzlei-website gesperrt, weil darüber offenbar schädliche E-Mails versendet worden waren. Damit änderte sich die Lage. Die verdächtige Nachricht war nicht von außen an die Kanzlei geschickt worden. Sie stand mit der eigenen Website in Verbindung. „Ich hatte im Vorfeld keine großen Sicherheitsbedenken bei meiner Homepage“, sagt Strathaus. Die Server in der Kanzlei waren abgesichert, die Mitarbeiter geschult, Firewall und Virenschutz regelmäßig geprüft. Die Website dagegen lief bei einem externen Dienstleister. Sie war beauftragt, gestaltet und veröffentlicht worden und damit nicht mehr im eigenen Fokus.

Der Vorfall spielte sich innerhalb weniger Tage ab. Der Hosting-Anbieter blockierte den Zugriff, die Webagentur informierte ihren Programmierer, Passwörter wurden geändert und Updates eingespielt. Nachdem alle Beteiligten grünes Licht gegeben hatten, schaltete Daniel Strathaus die Seite wieder frei. Ob und an wen zuvor Nachrichten verschickt worden waren, ließ sich jedoch nicht zuverlässig feststellen. DATEV-Consultant Peter Menneke riet deshalb dazu, den Vorgang nicht zu unterschätzen. Die Kanzlei informierte das Landeskriminalamt, prüfte eine Meldung an die Datenschutzaufsicht und setzte ihre Cyberversicherung in Kenntnis. Ein meldepflichtiger Schaden wurde nicht festgestellt. Auf dem Webserver lagen keine personenbezogenen Informationen, und mandantenbezogene Daten werden dort ohnehin nicht verarbeitet.

Das Sicherheitsupdate lag schon bereit

„Das Unbekannte trägt das Risiko in sich“, sagt DATEV-Experte Menneke. Solange unklar bleibt, wie viele Nachrichten versendet wurden und ob Empfänger auf den Link geklickt haben, muss eine Kanzlei den Vorfall nachvollziehbar bewerten und dokumentieren. Entscheidend sei, belegen zu können, welche Maßnahmen ergriffen, welche Stellen informiert und welche Entscheidungen getroffen wurden. Für Strathaus lag die wichtigste Erkenntnis außerhalb der eigenen Räume. „Die

”
Die Website ist eine digitale Tür, durch die jemand eintreten kann, den ich nicht haben will.
“

PETER MENNEKE
DATEV-Consultant

Homepage liegt außer Haus, da verliert man den Blick dafür“, sagt er. Wer eine Website extern betreiben lässt, gibt die technische Arbeit ab, nicht aber die Verantwortung. Im Nachgang zeigte sich, dass für das eingesetzte System bereits ein Sicherheitsupdate bereitstand. Es war offenbar nicht rechtzeitig installiert worden. Zugleich waren die Zuständigkeiten zwischen Kanzlei, Agentur und Programmierer nicht so eindeutig geregelt, wie es nötig gewesen wäre.

Strathaus zieht daraus eine Konsequenz. Die Kanzlei prüft ihre Verträge mit externen IT-Dienstleistern und legt genauer fest, wer Updates einspielt, Sicherheitslücken überwacht und Vorfälle meldet. „Zunächst hatte ich den Eindruck, dass alles geregelt ist. Später stellte sich jedoch heraus, dass noch nachzubessern ist.“

Gerade weil Kanzleieinhaber die technische Qualität einer Dienstleistung kaum selbst beurteilen können, müssen Pflichten konkret beschrieben sein. Ein allgemeiner Hinweis auf Datenschutz oder sichere Verarbeitung reicht nicht. Menneke sieht darin ein verbreitetes Problem: Viele Kanzleien konzentrierten sich auf Server, E-Mail-Systeme und Zugänge zum Rechenzentrum. Die Website werde dagegen als digitale Visitenkarte betrachtet, nicht als Teil der IT-Sicherheit. Dabei kann eine manipulierte Seite Besucher gefährden, Schadsoftware ausliefern, Kontaktformulare missbrauchen oder Inhalte veröffentlichen, die den Ruf der Kanzlei beschädigen. „Die Webseite ist eine digitale Tür“, sagt Menneke. „Wohin sie auch immer führt, ist eine andere Geschichte. Aber es ist meine digitale Tür, durch die jemand eintreten kann, den ich nicht haben will.“

Diese Türen gibt es nicht nur auf der Website. Auch Drucker, Frankiermaschinen, Multifunktionsgeräte oder Router kommunizieren mit externen Diensten. Sie beziehen Updates, melden >>



DIE KANZLEI

Seit über 70 Jahren ist Kaebisch & Partner in Warburg verwurzelt. Mit Daniel Strathaus, seit 2023 Partner der Kanzlei, steht die nächste Generation für den Anspruch, Bewährtes weiterzuentwickeln. Der Diplom-Finanzwirt und Steuerberater verbindet Tradition mit digitalen Prozessen und neuen Perspektiven.

62

Prozent der Internetnutzer in Deutschland wurden in den vergangenen zwölf Monaten Opfer von Cyberkriminalität.

70

Prozent sehen in Cyberattacken ein hohes generelles Risiko – aber nur 37 Prozent für sich selbst.

Quelle: Bitkom 2025



”
*Ich hatte im
 Vorfeld keine
 großen Sicher-
 heitsbedenken
 bei meiner
 Homepage.*
 “

DANIEL STRATHAUS
 Steuerberater und Partner
 Kaebisch & Partner in Warburg



IT-Sicherheit im Arbeitsalltag:

Daniel Strathaus
 bespricht mögliche
 Gefahren stets,
 wenn neue Geräte
 oder Dienste ein-
 gerichtet werden.

Tonerstände oder erlauben Fernwartung. Was den Büroalltag erleichtert, schafft zusätzliche Verbindungen nach außen. Die Frage lautet deshalb nicht nur, ob ein System geschützt ist, sondern auch, welche Geräte und Dienste mit dem Kanzleinetz verbunden sind und wer sie betreut.

Innehalten und nach dem Warum fragen

Allein die Technik im Blick zu haben, genügt dennoch nicht. Strathaus bespricht verdächtige E-Mails regelmäßig im Team und zeigt konkrete Beispiele. Links werden grundsätzlich nicht geöffnet, sofern ihr Anlass nicht eindeutig nachvollziehbar ist. USB-Sticks kommen nicht direkt an die Kanzleirechner, sondern werden auf einem separaten Gerät geprüft.

Menneke hält diese Aufmerksamkeit für unverzichtbar: „Der Faktor Mensch ist das größte Einfallstor und die beste Sicherheitsmaßnahme.“ Phishing-Mails seien heute sprachlich sauberer, stärker personalisiert und oft auf typische Stresssituationen zugeschnitten. Wer unter Zeitdruck handelt, übersieht leichter einen falschen Absender oder eine ungewöhnliche Aufforderung. Sein Rat lautet: immer innehalten und nach dem

Warum fragen. Warum soll ich diesen Link öffnen? Warum soll ich mich ausgerechnet jetzt anmelden? Und warum fordert mich diese Person zu einer im Grunde genommen ungewöhnlichen Handlung auf?

Eine einmalige Schulung allein reiche nicht zur dauerhaften Sensibilisierung. Das Thema müsse im Arbeitsalltag präsent bleiben, in Teambesprechungen, bei auffälligen Nachrichten und immer dann, wenn neue Geräte, Dienste oder Zugänge eingerichtet werden.

Der Vorfall blieb für die Kanzlei ohne Abfluss von Mandantendaten und ohne Konsequenzen. Sie hatte auch nichts falsch gemacht und sich bestmöglich gewappnet. Dennoch zeigt die Episode eine weit verbreitete Lücke: Die Website wurde außerhalb der Kanzlei betrieben und angegriffen. Doch auch dort muss sie Teil der Sicherheitsarchitektur der Kanzlei sein.

Seitdem betrachtet die Kanzlei die Website nicht mehr als einen erledigten Auftrag. Sie prüft nun Verträge, Zuständigkeiten und technische Pflichten genauer. Der Angriff hat vor allem sichtbar gemacht, was zuvor kaum beachtet wurde: Auch die digitale Tür außerhalb des eigenen Hauses muss kontrolliert werden. ○

Ist Ihre Kanzlei ausreichend auf einen digitalen Angriff vorbereitet?

Cybersicherheit ist kein IT-Projekt, sondern eine Führungsaufgabe. Technik schützt Systeme. Klare Zuständigkeiten, geübte Abläufe und eine offene Kommunikation schützen die Kanzlei. Nutzen Sie die folgende Checkliste, um Ihre Kanzlei auf mögliche Krisensituationen vorzubereiten und bestehende Prozesse kritisch zu überprüfen.

Text: Marc Fuchs, Judith Birkmann, Lutz Voswinkel

VORBEREITUNG

Wer trägt Verantwortung?

- ☐ Ist eindeutig geregelt, wer im Ernstfall die Koordination übernimmt?
- ☐ Sind Zuständigkeiten zwischen Kanzlei, IT-Dienstleister, Hosting-Anbieter und Agentur klar definiert?
- ☐ Sind Notfallkontakte jederzeit verfügbar?
- ☐ Wissen alle Mitarbeiter, an wen sie sich bei einem Verdacht wenden?

Wie gut ist Ihre digitale Infrastruktur geschützt?

- ☐ Werden Betriebssysteme, Anwendungen und das Content-Management-System regelmäßig aktualisiert?
- ☐ Sind Administratorzugänge durch starke Passwörter und Mehrfaktor-Authentifizierung geschützt?
- ☐ Werden nicht mehr benötigte Benutzerkonten und Zugänge konsequent entfernt?
- ☐ Gibt es regelmäßige Backups, und wurde deren Wiederherstellung bereits getestet?

Wissen Sie, wo Ihre Schwachstellen liegen?

- ☐ Ist bekannt, welche personenbezogenen Daten verarbeitet werden?
- ☐ Werden ungewöhnliche Zugriffe oder fehlgeschlagene Anmeldungen ausgewertet?
- ☐ Werden Website und IT-Systeme auf Sicherheitslücken überprüft?

- ☐ Sind externe Dienstleister und Schnittstellen dokumentiert?

IM ERNSTFALL

Je schneller die Ursache eingegrenzt wird, desto gezielter können die nächsten Schritte erfolgen.

- ☐ Ruhe bewahren und den Vorfall einordnen.
- ☐ Klären Sie zunächst, womit Sie es zu tun haben:
 - Cyberangriff oder Ransomware
 - Datenschutzvorfall
 - technischer Ausfall

Schaden begrenzen

- ☐ Betroffene Systeme sofort vom Netzwerk trennen.
- ☐ Den Vorfall intern melden und Verantwortliche informieren.
- ☐ Mitarbeitenden klare Anweisungen geben, etwa keine weiteren Anmeldungen oder Änderungen an den Systemen vorzunehmen.
- ☐ Erste Maßnahmen und Zeitpunkte dokumentieren.

Spezialisten einbinden

- ☐ IT-Dienstleister oder Administrator informieren.
- ☐ Datenschutzbeauftragte oder Datenschutzbeauftragten einbeziehen.
- ☐ Cyberversicherung kontaktieren.
- ☐ Falls nötig: Polizei oder Landeskriminalamt einschalten. Nicht jeder Vorfall lässt sich allein lösen.

Entscheidend ist, frühzeitig die passende Expertise einzubinden.

Kommunikation steuern

- ☐ Wer muss informiert werden? Mitarbeitende, Mandanten, Geschäftspartner, Datenschutzaufsichtsbehörde, betroffene Personen?
- ☐ Gibt es Mandate oder Fristen, die besonders kritisch sind?
- ☐ Ist festgelegt, wer die externe Kommunikation übernimmt?

Aus dem Vorfall lernen

- ☐ Wodurch konnte der Vorfall entstehen?
- ☐ Welche Abläufe haben funktioniert, welche nicht?
- ☐ Müssen Verantwortlichkeiten angepasst werden?
- ☐ Welche technischen oder organisatorischen Maßnahmen verhindern einen ähnlichen Vorfall künftig?

FRAGEN, DIE SICH JEDE KANZLEI STELLEN SOLLTE

- ☐ Können wir einen Cybervorfall tatsächlich innerhalb weniger Minuten erkennen?
- ☐ Weiß jeder Mitarbeiter wirklich, was in den ersten 30 Minuten konkret zu tun ist?
- ☐ Könnten wir nach einem Ausfall kurzfristig weiterarbeiten, und wären die wichtigsten Anwendungen, Daten und Zugänge dafür verfügbar?

„Datenschutz ist als Freiheitsrecht festgeschrieben“

Künstliche Intelligenz soll unterstützen, nicht entscheiden. Was zählt, sind menschliche Kontrolle und digitale Kompetenz. Der Landesbeauftragte für Datenschutz und Informationsfreiheit Baden-Württemberg spricht Klartext für die Kanzlei im Wandel.

Interview: Benedikt Leder, Birgit Schnee

Steuerberater arbeiten seit jeher mit sensiblen Informationen ihrer Mandanten. Was früher in verschlossenen Aktenschränken lag, fließt heute durch Cloudsysteme, KI-Anwendungen und digitale Plattformen. Die Technik verändert sich rasant, das Prinzip dahinter nicht: Vertrauen bleibt die wichtigste Währung des Berufsstands. Doch wie entsteht Vertrauen in einer Zeit, in der Daten zum Rohstoff und Algorithmen zum Arbeitswerkzeug werden? Ein Gespräch mit Professor Tobias Keber, Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg und Vorsitzender der Datenschutzkonferenz 2026.

DATEV magazin: Stellen wir uns vor, Sie betreten heute Morgen eine durchschnittliche Steuerberatungskanzlei. Woran würden Sie innerhalb weniger Minuten erkennen, ob Datenschutz dort tatsächlich gelebt und nicht nur dokumentiert wird?

Prof. Dr. Tobias Keber: Wahrscheinlich würden mir zunächst die Dinge ins Auge fallen, die auch für jeden anderen sichtbar sind: Liegen Akten oder Unterlagen so in den Büros herum, dass ich und damit auch jeder andere Kenntnis von Daten nehmen könnte? Stehen die Monitore am Empfang in einem Winkel, in dem ich direkt mitlesen kann, wer vor mir da war oder wer nach mir noch kommt? Es sind solche Kleinigkeiten, die einem als Erstes auffallen würden. Ich bin mir aber ziemlich sicher, dass die meisten Kanzleien großen Wert auf Datenschutz legen. Viele würden an dieser Stelle vermutlich auch den Begriff „Diskretion“ verwenden.

Wenn Sie anschließend mit der Kanzlei-leitung sprechen: Welche Frage würden Sie zuerst stellen? Und welche Antwort würde Ihnen zeigen, dass Datenschutz strategisch verstanden wird?

Man könnte zum Beispiel fragen, wann die letzte Schulung zu datenschutzrechtlichen Fragen war und wie die Mitarbeiterinnen und Mitarbeiter diese bewertet haben. Dann würde mich aber auch brennend interessieren, wie wir als Datenschutzaufsicht behilflich sein können, die Datenschutzfragen in der täglichen Arbeit zu klären: Sollten wir zu einem Thema eine Handreichung veröffentlichen, Schulungen anbieten?

Digitalisierung verändert Arbeitsweisen, Kommunikationswege und Geschäftsmodelle. Verändert sie damit auch das Vertrauensverhältnis zwischen Steuerberater und Mandant oder verändern sich lediglich die Werkzeuge?

Das Denken muss sich verändern, meine ich. Es wird nicht funktionieren, einmal etwas zu digitalisieren und dann zu glauben, dass alles gut ist. Digitalisierung ist ein permanenter Prozess, der von allen Beteiligten Digitalkompetenz erfordert. Auch ist es nötig, großen Wert auf IT-Sicherheit zu legen und kontinuierlich die Systeme zu pflegen, damit sie sicher bleiben. Mit dem Einsatz von KI-Systemen steigt der Bedarf an Digitalkompetenz und Sicherheit noch einmal zusätzlich.

Wenn Sie einer Steuerberatungskanzlei nur drei Grundsätze für einen verantwor-



Eine Frage der Verantwortung:

Prof. Dr. Tobias Keber hält menschliche Kontrolle, Datenschutz sowie Vertraulichkeit, Kompetenz und Sensibilisierung beim Einsatz von KI für unerlässlich.

4

Rechtsakte prägen den digitalen Ordnungsrahmen: Datenschutz-Grundverordnung, NIS2 und Data Act.



”
**Mitarbeiter sollten
im sicheren und
verantwortungsvollen
Umgang mit KI regelmäßig
geschult werden.**
“

PROF. DR. TOBIAS KEBER

Landesbeauftragter für Datenschutz und
Informationsfreiheit Baden-Württemberg

laufend überprüft werden. Regulierung muss kohärent, verständlich und praxistauglich sein. Wenn aber nicht mit anderen Digitalrechtsakten harmonisierte neue gesetzliche Regelungen geschaffen werden, führt das zwangsläufig zu Rechtsunsicherheiten bei Unternehmen. Die europäischen Datenschützer geben nicht zuletzt deswegen Hilfestellungen durch Interplay Guidelines. Wir raten verantwortlichen Stellen auch: Nutzt die Beratungsangebote der Aufsichtsbehörden, geht mit ihnen ins Gespräch. Denn klar ist: Auch wenn Datenschutz wie zuletzt schlechterdings als bürokratischer Aufwand heruntergeredet wird – der Grundrechtsschutz wird immer wichtiger. Datenschutz ist in der Europäischen Charta der Menschenrechte prominent als Freiheitsrecht festgeschrieben. Wer menschenzentriert Fortschritt und sich im Rahmen unserer europäischen Werteordnung bewegen will, muss Grundrechte achten. Als Datenschützer haben wir auch Vorschläge gemacht, wie man die DS-GVO wirksam anpassen kann, sodass sie einfacher und effizienter anwendbar ist.

Wenn Sie auf die kommenden fünf Jahre blicken: Welche Entwicklung wird Steuerberatungskanzleien stärker verändern als alle anderen? Künstliche Intelligenz, Cyberkriminalität oder Regulierung?

Wir müssen davon ausgehen, dass der Einsatz Künstlicher Intelligenz alltäglicher wird. Gerade deswegen sollten sich alle Verantwortlichen intensiv mit Digitalisierung befassen und darauf achten, einen guten Grundrechtsausgleich hinzubekommen. Der Schutz von sensiblen Daten bleibt auch in Zukunft wichtig. ○

tungsvollen Einsatz von KI mitgeben dürfen: Welche wären das?

Erstens: menschliche Kontrolle im Kernbereich. KI sollte unterstützen und nicht die Entscheidung ersetzen. Zweitens: Datenschutz und Vertraulichkeit. Der KI-Einsatz muss die rechtlichen Anforderungen einhalten. Drittens: Kompetenz und Sensibilisierung. Mitarbeiter sollten im sicheren und verantwortungsvollen Umgang mit KI regelmäßig geschult werden; dabei sollten rechtliche, technische und gesellschaftliche Fragen in Zusammenhang mit KI thematisiert werden.

Kanzleien bewegen sich heute in einem dichten Geflecht europäischer Regelwerke – von der DS-GVO über den AI Act hin zu NIS2 und dem Data Act. Entsteht daraus ein schlüssiger Ordnungsrahmen, oder wächst die Gefahr, dass Unternehmen den Überblick verlieren?

Wir haben zahlreiche neue datenrechtliche Anforderungen, die bereits gelten oder in die Geltung kommen werden. Das Zusammenspiel der DS-GVO mit den anderen Digitalrechtsakten muss daher



Prof. Dr. Tobias Keber

ist Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg und zudem Vorsitzender der Datenschutzkonferenz 2026.



Firmen retten mit **Steuern**

Bei der Sanierung eines Unternehmens können steuerliche Verlustvorträge für den Erfolg entscheidend sein. Ein neues Schreiben des Bundesfinanzministeriums zeigt, wann sie bei einem Eigentümerwechsel erhalten bleiben – und worauf Berater besonders achten sollten.

Text: Robert Brütting



Eine Unternehmenssanierung kann an einer steuerlichen Frage hängen: Was passiert mit Verlustvorträgen, wenn ein neuer Investor einsteigt? Wenn sie verloren gehen, so kann das die Sanierung erheblich verteuern und eine Beteiligung unattraktiv machen. Für Unternehmen, Investoren und ihre Berater ist deshalb entscheidend zu wissen, wann die steuerlichen Verluste trotz eines Gesellschafterswechsels erhalten bleiben. Ein Schreiben des Bundesfinanzministeriums sorgt hier jetzt für mehr Klarheit.

Mit Schreiben vom 29. April 2026 hat das Bundesfinanzministerium (BMF) die Voraussetzungen der Sanierungsklausel im Körperschaftsteuergesetz (§ 8c Abs. 1a KStG) ausführlich erläutert. Auf 21 Seiten konkretisiert die Finanzverwaltung, wann Verlustvorträge trotz eines schädlichen Beteiligungserwerbs erhalten bleiben können. „Für Unternehmen in der Krise, Investoren und steuerliche Berater kann die Verwaltungsanweisung zu mehr Planungssicherheit führen“, sagt Rechtsanwalt Marius Siemen aus München.

Die Ausgangslage: Gehen innerhalb von fünf Jahren unmittelbar oder mittelbar mehr als 50 Prozent der Anteile einer Körperschaft auf einen Erwerber oder ihm nahestehende Personen über, dann gehen bis dahin nicht genutzte Verlustvorträge grundsätzlich vollständig unter. „Die Regelung soll den Handel mit sogenannten Mantelgesellschaften verhindern, also den Erwerb von Gesellschaften allein wegen ihrer steuerlichen Verluste“, erklärt Siemen, der auch Partner der Siemen Conrady GmbH ist. Zugleich soll eine Sanierung möglich bleiben, ohne dass die steuerlichen Verluste verloren gehen – schließlich will auch der Gesetzgeber wirtschaftlich sinnvolle Umstrukturierungen ermöglichen, um Arbeitsplätze zu sichern. Genau hier setzt die Sanierungsklausel des Körperschaftsteuergesetzes an.

Eine begünstigte Sanierung liegt nach der gesetzlichen Definition dann vor, wenn Maßnahmen darauf gerichtet sind, eine drohende oder bereits eingetretene Zahlungsunfähigkeit beziehungsweise Überschuldung zu verhindern oder zu beseitigen und zugleich die wesentlichen Betriebsstrukturen zu erhalten. Die Gesellschaft muss also sanierungsbedürftig und sanierungsfähig sein; auch die Maßnahmen, insbesondere der Beteiligungserwerb, müssen für die Sanierung geeignet sein.

Es muss ferner mindestens eine von drei Voraussetzungen erfüllt sein. Erstens: Es gibt eine Betriebsvereinbarung mit Regelungen zur Be-

”
In Sanierungsfällen ist die Zusammenarbeit aller beteiligten Berater unerlässlich.
“

schäftigung. Zweitens: Die maßgeblichen Lohnsummen erreichen innerhalb von fünf Jahren mindestens 400 Prozent der Ausgangslohnsumme. Oder drittens: Es wird durch Einlagen wesentliches Betriebsvermögen zugeführt. Für die Praxis sind Verlustvorträge bei einer Sanierung wirtschaftlich wichtig. „Der Untergang vorhandener Verlustvorträge schreckt Investoren häufig ab und erschwert langfristig sinnvolle Umstrukturierungen erheblich“, so Rechtsanwalt Siemen. Das BMF-Schreiben konkretisiert zentrale Begriffe sowie die erforderlichen Nachweise.

Beurteilung der Sanierungsbedürftigkeit

„In Sanierungsfällen ist die Zusammenarbeit aller beteiligten Berater – Insolvenzrechtler, Wirtschaftsprüfer, Steuerberater – unerlässlich“, weiß Siemen. „Dies zeigt sich auch bei der Konkretisierung der Nachweispflichten für das Vorliegen der Voraussetzungen der Sanierungsklausel.“

Für die Beurteilung der Sanierungsbedürftigkeit verweist das BMF-Schreiben auf die insolvenzrechtlichen Grundsätze der Insolvenzordnung (§§ 17 bis 19 InsO). Es beschreibt zudem, wie die Voraussetzungen belegt werden können. Genannt werden insbesondere Sanierungs- (§§ 217 ff. InsO) und Restrukturierungspläne (§§ 5 ff. Unternehmensstabilisierungs- und -restrukturierungsgesetz (StaRUG)) sowie Sanierungsgutachten, etwa vom Institut der Wirtschaftsprüfer in Deutschland.

Wichtig ist die Auslegung bei mehrstufigen Beteiligungen. Der Gesetzestext spricht nur vom „Beteiligungserwerb“ und regelt nicht ausdrücklich, wie Beteiligungsketten zu behandeln sind. Das Finanzministerium stellt nun klar: Ein unmittelbarer schädlicher Erwerb an der Konzernspitze kann zugleich mittelbare schädliche Erwerbe auf nachgelagerten Ebenen auslösen. Für jede betroffene Gesellschaft mit eigenen Verlustvorträgen ist deshalb gesondert zu prüfen, ob die Sanierungsklausel greift. Das kann in der Praxis einen entscheidenden Unterschied machen: Erfüllt die Gesellschaft auf der Erwerbsebene die Voraus- >>



Marius Siemen

ist Rechtsanwalt und Partner der Siemen Conrady GmbH in München. Er berät Unternehmen, Start-ups, Family Offices und institutionelle Investoren zu allen Bereichen des Steuerrechts, insbesondere bei Transaktionen, Restrukturierungen und im internationalen Steuerrecht.



Vernetzen
Sie sich mit
Marius Siemen
auf LinkedIn:



KOMPAKT-WISSEN

Das Buch *Kauf einer überschuldeten GmbH* ist ein Praxisleitfaden für Steuerberater
→ datev.de/shop/35637



Fünf Fakten zu Verlustvorträgen

Wann Verlustvorträge untergehen, welche Ausnahmen greifen und was bei Körperschaft- und Gewerbesteuer gilt: die wichtigsten Antworten, die bei Gesellschaftserwechseln entscheidend sein können.

Ab welchem Beteiligungsumfang ist der Verlustvortrag gefährdet?

Sobald innerhalb von fünf Jahren mehr als 50 Prozent der Anteile oder Stimmrechte an einen Erwerber oder eine Erwerbergruppe mit gleichgerichteten Interessen übertragen werden, verfallen sämtliche Verlustvorträge vollständig.

Betrifft der Untergang der Verlustvorträge nur die Körperschaftsteuer oder auch die Gewerbesteuer?

Der Untergang wirkt sowohl bei der Körperschaftsteuer als auch bei der Gewerbesteuer: § 10a Satz 10 GewStG verweist ausdrücklich auf § 8c KStG, sodass auch gewerbesteuerliche Verlustvorträge einer GmbH bei einem schädlichen Beteiligungserwerb untergehen können.

Kann ein bereits festgestellter Verlustvortrag noch genutzt werden, wenn der Gesellschafterwechsel im laufenden Jahr erfolgt?

Laut Rechtsprechung kann der bis zum schädlichen Beteiligungserwerb erzielte Gewinn noch mit bestehenden Verlust-

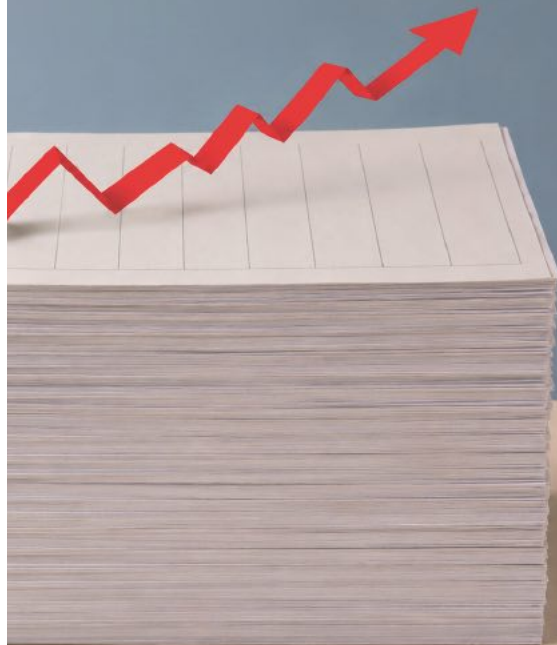
vorträgen verrechnet werden; das Abzugsverbot greift erst für die verbleibenden Verluste nach dieser Verrechnung (BFH, Urteil vom 30.11.2011 – I R 14/11).

Gibt es Möglichkeiten, den Verlustvortrag trotz Anteilsübertragung zu sichern?

Die Stille-Reserven-Klausel erlaubt die Berücksichtigung von Verlusten in Höhe vorhandener inländisch steuerpflichtiger stiller Reserven. Die Klausel schützt konzerninterne Übertragungen. Zusätzlich kann ein fortführungsgebundener Verlustvortrag nach § 8d KStG beantragt werden, wenn derselbe Geschäftsbetrieb fortgeführt wird.

Gilt § 8c KStG auch für Personengesellschaften?

§ 8c KStG regelt den Verlustabzug bei Körperschaften. Personengesellschaften sind nicht erfasst. Hier greifen andere Regeln, insbesondere § 10a GewStG sowie Vorschriften zu Verlusten des Kommanditisten. § 8c KStG wirkt nur, soweit eine Körperschaft als Mitunternehmerin beteiligt ist und die Verluste auf ihrer Ebene zu negativen Einkünften führen.



setzungen, folgt daraus nicht automatisch, dass auch eine Tochter- oder Enkelgesellschaft mit eigenen Verlustvorträgen begünstigt ist. Umgekehrt kann die Sanierungsklausel bei einer Tochterfirma greifen, obwohl sie beim unmittelbaren Erwerb nicht erfüllt ist.

Diese Trennung der Prüfebene ergibt sich nicht unmittelbar aus dem Gesetz, sondern aus der Konkretisierung des BMF. Auch bei den Nachweisen verlangt die Verwaltung eine Prüfung auf Ebene der jeweiligen Gesellschaft: Die nachgeordnete Gesellschaft muss selbst belegen, dass auch der sie betreffende mittelbare Erwerb der



Erfolgreiche Sanierung:

Wann bleiben steuerliche Verluste trotz eines Gesellschafterwechsels erhalten?

Sanierung dient. Ein konzernweiter Sanierungsplan kann dafür ausreichen, wenn daraus hervorgeht, dass die Gesellschaft tatsächlich Teil des Sanierungskonzepts ist. Ein pauschaler Verweis auf die Sanierung der Konzernmutter genügt nicht.

Für Steuerberater ergibt sich daraus ein Prüfungsauftrag: Bei einem Beteiligungserwerb im Zuge einer Sanierung sind die Voraussetzungen nicht nur auf Ebene des unmittelbaren Erwerbs zu betrachten. Entscheidend ist, ob die Voraussetzungen und Nachweise für jede betroffene Ebene vorliegen. Das BMF-Schreiben liefert dafür einen Orientierungsrahmen. ○



Steuerfall

Influencer:

Ab wann wird die Tätigkeit gewerblich?

Influencer für ihre Beiträge eine Gegenleistung erhalten, sei es in Form von Geld oder Sachleistungen, greift die Pflicht zur Kennzeichnung.

Geschäftsmäßig betriebene Social-Media-Auftritte unterliegen zudem der Impressumspflicht. „In der Praxis werden diese Anforderungen jedoch häufig unterschätzt“, sagt Grimm, die auch Fachanwältin für gewerblichen Rechtsschutz ist.

Nutzungsrechte oft nicht geklärt

Konfliktpotenzial birgt auch die Nutzung von Inhalten. Bilder, Videos oder Musik werden in Kampagnen integriert, ohne dass die erforderlichen Nutzungsrechte geklärt sind. Eine zentrale Rolle spielt zudem die Vertragsgestaltung. Influencer-Verträge sind oftmals lückenhaft und lassen wichtige Fragen offen: Welche Leistungen werden geschuldet? Wie werden Gegenleistungen bewertet? Welche Nutzungsrechte werden eingeräumt? „Unklare Regelungen können im Nachgang zu erheblichen steuerlichen Konsequenzen führen – etwa, wenn Finanzbehörden von sogenannten tauschähnlichen Umsätzen ausgehen“, sagt Grimm. Für Unternehmen stellen Kooperationen zwar grundsätzlich Betriebsausgaben dar, doch Sachzuwendungen wie Produkte oder Reisen unterliegen besonderen Regelungen.

Auch Influencer selbst haben steuerliche Pflichten. Zu den Einnahmen zählen nicht nur Honorare, sondern auch erhaltene Produkte, die mit ihrem Marktwert zu versteuern sind. Viele unterschätzen zudem, ab wann ihre Tätigkeit als gewerblich gilt. „Fehlerhafte Angaben oder eine unvollständige Buchführung werden häufig erst im Rahmen späterer Prüfungen sichtbar“, weiß Grimm.

Influencer-Marketing bietet Unternehmen enormes Potenzial – vorausgesetzt, die rechtlichen und steuerlichen Rahmenbedingungen werden frühzeitig berücksichtigt. „Wer Kooperationen strukturiert plant, vertraglich sauber regelt und interdisziplinär begleitet, kann Risiken deutlich reduzieren und gleichzeitig die Chancen optimal nutzen“, sagt Rechtsexperin Grimm. ○

Influencer-Marketing sicher gestalten

Warum neue Formen der Kommunikation auch neue steuerliche Fragen aufwerfen.

Text: Robert Brütting

Influencer-Marketing ist längst ein fester Bestandteil moderner Kommunikation. Für Steuerberater ist das Thema deshalb jetzt relevant: Unternehmen setzen auf Kooperationen mit Social-Media-Persönlichkeiten, um Zielgruppen authentisch anzusprechen und Reichweite zu generieren. Doch mit den Möglichkeiten wächst auch die Komplexität – insbesondere in rechtlicher und steuerlicher Hinsicht. Was wie eine rein kreative Zusammenarbeit erscheint – und ja auch erscheinen soll – ist faktisch ein sehr sensibles Geflecht aus Marketing, Recht und Steuern.

Risiken können bereits in der Planungsphase entstehen. Kampagnennamen, Hashtags oder Profilbezeichnungen bergen das Potenzial, Markenrechte Dritter zu verletzen. „Unternehmen sehen sich in solchen Fällen schnell mit Abmahnungen oder Schadenersatzforderungen konfrontiert“, sagt Rechtsanwältin Dr. Susanne Grimm von RÖDL in Stuttgart. Auch die Transparenz ist ein kritischer Punkt: Werbung muss klar erkennbar sein. Sobald



Dr. Susanne Grimm

ist Rechtsanwältin und Fachanwältin für gewerblichen Rechtsschutz. Sie leitet die nationale und internationale Praxisgruppe IP & Media bei RÖDL. Ihr Schwerpunkt: Recht und KI.



Vernetzen Sie sich mit Dr. Susanne Grimm auf LinkedIn



Mehr dazu im Fachbeitrag von Dr. Susanne Grimm → go.datev.de/influencer-steuern

Minijobs korrekt abrechnen

Mehrere Arbeitgeber, ein Beschäftigter oder Familienangehörige als Minijobber: Wo die gesetzlichen Grenzen liegen und welche Risiken Unternehmen und ihre steuerlichen Berater kennen sollten.

Text: Robert Brütting

Nur 603 Euro im Monat – mehr darf ein Minijobber derzeit grundsätzlich nicht verdienen. Doch was passiert, wenn mehrere Arbeitgeber beteiligt sind oder die Arbeitsleistung scheinbar auf mehrere Personen verteilt wird? Ein aktuelles Verfahren aus Regensburg zeigt, wie weit die Folgen reichen können, wenn die gesetzliche Grenze nicht tatsächlich, sondern nur auf dem Papier eingehalten wird. Ein prominenter Gastronom wurde wegen einer vermeintlich cleveren Gestaltung von Minijobs zu einer Freiheitsstrafe auf Bewährung verurteilt. Noch ist die Entscheidung nicht rechtskräftig, doch die Signalwirkung wird bereits jetzt deutlich.

Für Steuerberater ist die entscheidende Frage: Wer arbeitet tatsächlich, für wen und in welchem Umfang? Genau hier können vermeintlich saubere Beschäftigungsmodelle problematisch werden. Wer Mandanten bei der Lohnabrechnung begleitet, kann solche Konstellationen früh erkennen und auf die Risiken hinweisen.

Im Kern geht es um eine Praxis, die in bestimmten Branchen seit Jahren kursiert: das sogenannte Splitting von Minijobs. Die Staatsanwaltschaft formulierte die rechtliche Einordnung

im Verfahren unmissverständlich: „Es gibt kein Firmen-Splitting und kein Personen-Splitting.“ Gemeint ist damit, dass die gesetzliche Entgeltgrenze für Minijobs strikt personenbezogen gilt – unabhängig davon, wie viele Arbeitgeber beteiligt sind oder wie die vertragliche Konstruktion im Einzelfall ausgestaltet wird.

Das Prinzip des Minijobs ist einfach: Bis zu einer bestimmten monatlichen Verdienstgrenze – aktuell 603 Euro, künftig weiter ansteigend – bleibt die Beschäftigung für Arbeitnehmer weitgehend sozialabgabenfrei, während Arbeitgeber pauschale Abgaben entrichten. „Gerade für Branchen mit schwankendem Personalbedarf ist dieses Modell attraktiv“, sagt Rechtsanwalt Benjamin Onnis von



Flexibel mit Minijobs: Gerade für Branchen mit schwankendem Personalbedarf ist dieses Modell attraktiv, etwa für die Gastronomie.





Benjamin Onnis

ist Rechtsanwalt und Fachanwalt für Arbeitsrecht sowie Partner bei FPS Rechtsanwalts-gesellschaft mbH & Co. KG in Berlin. Dort berät er Unternehmen zu arbeitsrechtlichen Fragen.



Vernetzen Sie sich mit Benjamin Onnis auf LinkedIn.



Lena Grebe

ist Rechtsanwältin bei FPS in Berlin und berät Unternehmen im Arbeitsrecht. Zu ihren Schwerpunkten zählen unter anderem Anstellungs- und Aufhebungsverträge sowie Kündigungsverfahren.

der Kanzlei FPS in Berlin. „Doch die Versuchung, die Grenze faktisch zu vervielfachen, ist groß – und hier beginnt das rechtliche Risiko.“

Im zugrundeliegenden Fall sollen Beschäftigte parallel bei mehreren Unternehmen desselben Inhabers angemeldet worden sein. Ziel war es, die Verdienstgrenze pro Beschäftigungsverhältnis auszunutzen. In anderen Konstellationen wurde die Arbeitsleistung faktisch von einer Person erbracht, während mehrere Familienangehörige als Minijobber geführt und bezahlt wurden.

Rechtlich halten solche Konstruktionen einer Prüfung jedoch nicht stand. Nach den sozialversicherungsrechtlichen Vorgaben werden mehrere Beschäftigungen zusammengerechnet. Maßgeb-

lich ist zudem stets die tatsächliche Arbeitsleistung, nicht die vertragliche Gestaltung.

Erhebliche Konsequenzen

„Werden Tätigkeiten nur scheinbar auf mehrere Personen verteilt, spricht vieles für eine unzulässige Gestaltung oder sogar Schwarzarbeit“, sagt Onnis, der auch Fachanwalt für Arbeitsrecht ist. Die Konsequenzen sind erheblich. Neben strafrechtlichen Vorwürfen, insbesondere wegen Vorenthaltens und Veruntreuens von Arbeitsentgelt, drohen Nachzahlungen von Sozialversicherungsbeiträgen und Steuern. Hinzu kommen Säumniszuschläge und Zinsen. Dies kann – wie im aktuellen Fall – sogar existenzgefährdend sein.

Die Finanzkontrolle Schwarzarbeit des Zolls intensiviert schon seit Jahren ihre Prüfungen, vor allem in personalintensiven Branchen wie Gastronomie, Baugewerbe oder Transport. Minijobs stehen dabei regelmäßig im Fokus, weil sie einerseits weit verbreitet sind und andererseits Gestaltungsspielräume eröffnen, die missbraucht werden können. „Auffällig ist, dass viele Arbeitgeber die Risiken unterschätzen oder von falschen Annahmen ausgehen“, weiß Rechtsanwältin Lena Grebe, die ebenfalls bei FPS in Berlin tätig ist. „So hält sich hartnäckig der Glaube, mehrere Arbeitgeber könnten unabhängig voneinander einen Minijob gewähren oder Ehepartner könnten die Verdienstgrenze untereinander aufteilen.“ Beides ist unzutreffend. Entscheidend ist allein die Person des Beschäftigten und die Summe aller Einkünfte aus geringfügiger Beschäftigung.

Wer Minijobber beschäftigt, sollte die bestehenden Strukturen regelmäßig überprüfen. Dazu gehört insbesondere, sich über weitere Beschäftigungsverhältnisse der Mitarbeiter zu informieren und entsprechende Erklärungen einzuholen. Ebenso wichtig ist eine saubere Dokumentation der Arbeitszeiten und Tätigkeiten. „Auffällige Konstellationen – etwa bei Familienangehörigen – sollten besonders sorgfältig geprüft werden“, rät Grebe. Nicht zuletzt spielt die interne Organisation eine zentrale Rolle. Lohnbuchhaltung, Personalabteilung und Geschäftsleitung müssen eng zusammenarbeiten.

Bei Minijobs entscheidet nicht allein der Vertrag, sondern die tatsächliche Beschäftigung. Für Arbeitgeber gilt mehr denn je: Rechtssicherheit geht vor kurzfristiger Entlastung. „Denn was heute als kreative Lösung erscheint, kann morgen vor Gericht enden“, sagt Rechtsanwalt Onnis. ○



Lesen sie mehr im Fachbeitrag der Experten von FPS. → go.datev.de/minijobs-abrechnen

Gut vorbereitet auf die nächste Etappe

Der Weg in die Cloud beginnt nicht erst am Umstellungstag. Entscheidend ist eine frühe Vorbereitung. Warum dieser Weg gut vorbereitet sein muss und nur gemeinsam erfolgreich bewältigt werden kann, zeigt das Beispiel des Pilotanwenders Eugen Nazarenus.

Text: Carsten Fleckenstein

Zweimal Zeit aufwenden wollte Steuerberater Eugen Nazarenus nicht. Vor gut drei Jahren gründete er seine eigene Kanzlei in Frankfurt am Main. Als er erfuhr, dass die bewährte Software DATEV Eigenorganisation durch ein in der Cloud laufendes Kanzleimanagement ersetzt wird, traf er eine pragmatische Entscheidung und meldete sich als Pilotanwender. „Ich möchte nicht in drei Jahren noch mal Zeit in die Kanzleiorganisation investieren“, sagt Nazarenus. Er wolle „lieber von Anfang an mit der neuesten Software die Kanzleiorganisation optimieren“.

Er erinnert sich noch gut an frühere Softwareumstellungen, die er damals als Assistent erlebt hat. Diese Umstellungsarbeiten seien stets mit viel Zeit- und Ressourcenaufwand verbunden gewesen, und die Ausfallzeiten hätte man effektiver nutzen können. Aufgrund dieser Erfahrung war es für die Nazarenus Steuerberatung sehr wichtig, für die eigene Kanzlei möglichst früh eine Lösung einzuführen, die die Bearbeitung der Managementaufgaben unterstützt und Prozesse effizient gestaltet.

Dass der Umstieg auf die Cloud-Lösung Kanzleimanagement mehr als nur ein Softwarewechsel war, merkte Nazarenus, als er das Umstellungs-

cockpit öffnete. „Man hat die Vorbereitung komplett unterschätzt“, sagt er. Aus einer erwarteten Softwareumstellung wurde eine Reihe grundlegender Entscheidungen, die neben dem laufenden Kanzleialltag getroffen werden mussten.

Die Umstellung hieß für Nazarenus vor allem: Dokumente lesen, Entscheidungen treffen, Zusammenhänge verstehen. Nicht jeder Zusammenhang war auf Anhieb sichtbar. Dazu kamen Fragen zu Lizenzen, Berechtigungen und Freischaltungen. Die Einführung war kein Selbstläufer, sondern erforderte Zeit, Analyse und eine klare Vorstellung von der eigenen Kanzlei- und Mandantenarbeit.

Umstellungscockpit gibt Orientierung

Doch er hielt durch. Das Umstellungscockpit gab ihm Orientierung. „Zu jedem Schritt wird erklärt, was du zu tun hast“, sagt Nazarenus. Es sei ein „richtig guter roter Faden“ erkennbar, und es sei logisch aufgebaut. Entscheidend sei, „sich früh genug damit auseinanderzusetzen“. Am ersten Arbeitstag danach begann für Nazarenus die Praxisphase: „Wo sind meine Aufträge, was suche ich jetzt, wie fange ich an?“ Im Alltag spürt er die Veränderung vor allem beim Erstellen von Rechnungen sowie bei der Übersicht »

**Eugen Nazarenus**

führt seit 2023 seine eigene Kanzlei. Zuvor war er für mehrere Großkanzleien tätig. Er hat Betriebswirtschaft mit den Schwerpunkten Steuerlehre, Steuerrecht, Rechnungslegung und Wirtschaftsprüfung studiert.



Vernetzen Sie sich mit Eugen Nazarenus auf LinkedIn:

**DIE KANZLEI**

Die Nazarenus Steuerberatung steht für persönliche Beratung und kurze Wege. Neben Steuerberatung, Buchhaltung und Jahresabschluss unterstützt die Kanzlei bei betriebswirtschaftlichen Fragen und Unternehmensführung. Digitale Prozesse sorgen für effiziente Abläufe und schnelle Erreichbarkeit.

„*Das, was neu kommt, ist unvermeidbar – und das muss nicht schlechter sein.*“

EUGEN NAZARENUS

Inhaber der Nazarenus Steuerberatung

über Aufträge und Zeiten. „Du arbeitest jetzt auftragsbezogen.“ Leistungen ließen sich leichter zuordnen, Zeitaufwände schneller kontrollieren. Kanzleimanagement sei für ihn „viel, viel intuitiver und wirtschaftlicher geworden“. Insgesamt sei die Arbeit übersichtlicher.

Nazarenus sammelte diese Erfahrungen als freiwilliger Pilotanwender in einer frühen Phase von DATEV Kanzleimanagement. Für die regulären Umstellungen ist der Ablauf klar strukturiert: Die relevanten Informationen und Aufgaben sind im DATEV Umstellungscockpit gebündelt. Es zeigt, welche Schritte anstehen, und begleitet die Kanzlei durch Vorbereitung und Umstellung. In der Regel erfahren Kanzleien rund sechs Monate im Voraus von ihrem persönlichen Umstellungszeitraum. Diese Zeiträume berücksichtigen unter anderem die individuelle Nutzung, weitere Produktumstellungen sowie technische und organisatorische Voraussetzungen.

Bereit für die nächsten Schritte

Trotz der anfänglichen Schwierigkeiten überwiegt für den Frankfurter Steuerberater nach der ersten Umstellung jedoch das Positive. Jetzt wisse er, „wie das funktioniert“ und sei bereit für die nächsten Schritte. Bei weiteren Programmumstellungen habe er eine Chance, von Anfang an ein stabiles Fundament für die Kanzleiverwaltung aufzubauen.

Bedenken hatte Nazarenus vor der ersten Pilotierung keine. „Das, was neu kommt, ist unvermeidbar, und das muss nicht schlechter sein“, sagt er.

Was für Nazarenus aus eigener Initiative begann, wird für die kommenden Umstellungen zum Prinzip: rechtzeitig vorbereiten, den individuellen Umstellungszeitraum nutzen und Schritt für Schritt in der neuen Lösung ankommen. ○

Mehr als nur Technik

Die Umstellung der DATEV-Anwendungen auf Cloud-Lösungen wirft bei vielen Mitgliedern Fragen auf. Warum ist das nötig? Wieso dieses Timing? Ginge es nicht auch anders? Volker Andres, stellvertretender Vorsitzender des DATEV-Vertreterrats, klärt auf.



Volker Andres

ist Diplom-Betriebswirt (FH), Steuerberater und Gründer der Kanzlei Adjunktis in Mayen bei Koblenz. Seit vielen Jahren engagiert er sich im Vertreterrat bei DATEV, dessen stellvertretender Vorsitzender er ist.

Mehr als ein Softwarewechsel

„Die Cloud ist kein Produkt, das man einfach installiert – der Weg in die Cloud ist weit mehr als eine technische Umstellung. Mit der Cloud verändern sich Prozesse, Arbeitsweisen und die Zusammenarbeit mit den Mandanten. DATEV und Mitglieder müssen diesen Weg gemeinsam gestalten. DATEV entwickelt die technischen Lösungen, die Mitglieder bringen Praxiserfahrungen ein.“

Aufwand, der sich lohnt

„Die Erwartung ist oft: Man bekommt das Umstellungscockpit und kann den Umstieg damit ganz leicht machen. Das ist zu kurz gedacht. Wir haben Dinge, die historisch gewachsen sind. Vieles aus der On-Premises-Welt funktioniert in der neuen Welt nicht mehr. Jede Kanzlei sollte früh prüfen: Wo fehlen Standards, wo entstehen Medienbrüche? Bis zum Umstellungszeitraum sollte die Vorbereitung abgeschlossen sein.“

Gesteuerte Umstellung

„DATEV kann nicht warten und dann alle Kanzleien per Knopfdruck umstellen. Wenn alle bis zum Schluss warten würden, wäre kein geordneter Umstieg mehr möglich. Im Sinne der Planungssicherheit finde ich den schrittweisen Umstieg richtig.“

Mut zur Veränderung

„Veränderung ist immer auch mit Angst verbunden. Deshalb müssen die Mitglieder wissen: Sie gehen diesen Weg nicht allein, sondern gemeinsam als Genossenschaft. Pilotierungen helfen, die Lösungen für alle besser zu machen. Der Vertreterrat versteht sich dabei als Bindeglied zwischen DATEV und den Mitgliedern. Wir bringen die Perspektive der Mitglieder ein und begleiten die Veränderung aus der Praxis heraus. Wir reichen die Hand – gehen müssen die Kanzleien selbst.“

Gute Strukturen schaffen Freiraum

Warum klar definierte Prozesse keine Einschränkung sind und weshalb sie Raum für Beratung, Zusammenarbeit und Zukunftsgestaltung eröffnen.

Kürzlich war ich im Urlaub mit einem Mietwagen unterwegs. Obwohl ich dieses Automodell nie zuvor gefahren hatte und ich mich in einem anderen Land befand, dauerte es nur wenige Augenblicke, bis ich unterwegs war. Blinker, Bremse, Lenkrad und viele technische Standards funktionierten nach der vertrauten Logik. Ich musste nicht jedes Detail neu lernen. So konnte ich mich auf das konzentrieren, worauf es ankam: die Strecke, die Umgebung und das Ziel.

An diese Erfahrung musste ich denken, als in einem Gespräch über Standardisierung diskutiert wurde. Viele verbinden damit zunächst starre Vorgaben. In der Praxis sorgen Standards jedoch oft dafür, dass wir uns auf die eigentlich wesentlichen Aufgaben konzentrieren können.

Auch in Kanzleien entwickeln sich über die Jahre individuelle Arbeitsweisen. Zugleich lässt sich beobachten, dass jede Sonderlösung Abstimmungen und Rückfragen erzeugt. Sobald Brüche in Abläufen entstehen, kostet das Zeit.

Die Anforderungen an den Berufsstand verändern sich. Neue gesetzliche und bürokratische Vorgaben, E-Rechnung, Fachkräftemangel und die zuneh-

mende Nutzung Künstlicher Intelligenz erhöhen die Dynamik. Zugleich erwarten Mandanten schnelle Antworten und eine vorausschauende Beratung. Daher wird es immer wichtiger, dass Mitarbeiter ohne Umwege auf Daten zugreifen können und Abläufe klar geregelt sind.

Orientierung geben

Standardisierung bedeutet, wiederkehrende Aufgaben nachvollziehbar und verlässlich zu organisieren. Wo Prozesse einer gemeinsamen Logik folgen, entsteht Orientierung. Wissen lässt sich leichter weitergeben, neue Kolleginnen und Kollegen finden schneller ihren Platz im Team. Auch die Möglichkeiten der Cloud und der Einsatz von KI entfalten ihren Nutzen nicht allein durch Technologie. Entscheidend ist, dass Daten verlässlich vorliegen und Prozesse sauber aufeinander abgestimmt sind. Cloudlösungen und KI entfalten ihre Wirkung dort, wo die organisatorischen Grundlagen stimmen.

Am Ende geht es um die Freiräume, die dadurch entstehen. Wer weniger Zeit für die Informationssuche oder Abstimmungen benötigt, hat mehr Raum für Mandantengespräche und die Weiterentwicklung der eigenen Kanzlei.

Freiheit entsteht dort, wo das Wesentliche reibungslos funktioniert. Und genau deshalb schaffen klare Strukturen vor allem eines: Freiraum. ○

**Herzlich
Ihr Markus Aligner**
Chief Markets Officer (CMO)



Dr. Markus Aligner

ist Chief Markets
Officer bei DATEV.



Vernetzen Sie sich mit
Dr. Markus Aligner auf
LinkedIn.



**„Sobald Brüche in
Abläufen entstehen,
kostet das Zeit.“**



DIE KANZLEI

Die Kanzlei Muschke in Arendsee (Sachsen-Anhalt) verbindet regionale Nähe mit konsequenter Digitalisierung. Das siebenköpfige Team berät vor allem Handwerksbetriebe, Heilberufe und Freiberufler mit Blick auf die Zukunft: die Vorbereitung und Begleitung von Entscheidungen.



Wendekind mit Wunschkanzlei

Selbstreflexion und Beharrlichkeit brachten Anne-Kathrin Muschke auf einen neuen Weg. Heute führt sie eine Kanzlei, in der Beratung mit Weitblick wichtiger ist als der Blick zurück.

Text: Shania Vivienne Schmidt

Ein leises Schlüsselklicken, dann schwingt die Tür auf. Anne-Kathrin Muschke hält kurz inne. Jetzt also wirklich. Als sie im Januar 2022 über die Schwelle ihrer eigenen Kanzlei im beschaulichen Norden Sachsen-Anhalts tritt, kann sie es kaum glauben. Bis hierhin war es ein langer Weg. Doch dabei verlor sie nie das Ziel aus den Augen. Bereits als 16-Jährige im Osten Deutschlands, mitten in der Wendezeit, war ihr klar: Sie wollte Steuerberaterin werden.

Dass zwischen diesem Ziel und der eigenen Kanzlei zahlreiche Steine liegen würden, ahnte sie noch nicht. Der Zugang zum Studium gelang zunächst nur über einen Nachrückplatz. Die Steuer-

„*Es geht nicht nur um die Steuer an sich, sondern auch um das Steuern des Unternehmens.*“

beraterprüfung bestand sie erst im dritten Anlauf. Doch Aufgaben kam für Anne-Kathrin Muschke nie infrage. „Das bin ich nicht. Wenn es noch eine Chance gibt, nutze ich sie“, sagt sie.

Der Startschuss für die eigene Kanzlei fiel nicht durch die bestandene Prüfung oder den ersten Mandanten, sondern durch eine ehrliche Frage an sich selbst. Zehn Jahre brachte sich Anne-Kathrin Muschke als Teilhaberin in einer mittelständischen Steuerberatungskanzlei ein. Sie trieb Digitalisierungsthemen voran und beschäftigte sich damit, wie Steuerberatung Unternehmen besser im Hier und Jetzt unterstützen kann, statt lediglich Vergangenes zu dokumentieren.

Berufliche Zukunft in der Heimat

Mit der Zeit kollidierten ihre Vorstellungen und die der Kanzlei zunehmend. „2019 habe ich mich gefragt: Wo stehst du, wer bist du, und was willst du eigentlich?“, erinnert sich die Steuerberaterin. Ihre Antwort war: Sie wollte ihren eigenen Weg gehen. Rechtliche und organisatorische Hürden machten den Abschied von ihrem Geschäftspartner zu einem langwierigen Prozess. Noch zweieinhalb Jahre sollte es dauern, bis aus ihrem Wunsch nach Veränderung Realität wurde.

Trotz des Neuanfangs sollte sich dann aber doch nicht alles ändern. Eines stand fest: der Standort. Die eigene Kanzlei sollte dort entstehen, wo sie sich zu Hause fühlt. Obwohl sie während ihrer Zeit in der Wirtschaftsprüfung bundesweit unterwegs war, zog es sie nie dauerhaft weg aus Sachsen-Anhalt. „Heimat ist, wirklich angekommen zu sein, sich wohlfühlen“, sagt Anne-Kathrin Muschke. Dort habe sie ihr Netzwerk und Menschen, auf die sie sich verlassen könne. Dass sie ihre Zukunft dort sieht, zeigt auch ihr jüngstes Projekt. Ende Mai dieses Jahres bezog die Kanzlei einen Neubau in Arendsee, in dem nun die zuvor auf zwei Standorte verteilten Mitarbeiter tätig sind.

Dass die eher ländlich geprägte Region ein Widerspruch zu ihrer gelebt modernen Steuer-

beratung sein könnte, kam ihr nie in den Sinn: „Wenn ich für etwas stehe, dann brenne ich dafür, und dann kann ich auch wirklich gut überzeugen.“ Zweifel daran hatte sie nie. Vielmehr sieht sie gerade in der Region Vorteile. Die Wege sind kurz, Beziehungen bestehen oft über Jahre hinweg. „Hier kennt jeder jeden.“ Das erleichtere die Zusammenarbeit mit Mandanten, aber auch die Suche nach Mitarbeiterinnen und Mitarbeitern sowie nach Partnern.

Für Anne-Kathrin Muschke lebt ihre tägliche Arbeit nicht vom Blick zurück. „Ich sehe mich als Bindeglied zwischen Vergangenheit, Gegenwart und Zukunft“, erklärt sie. Ihre Auswertungen sollen nicht nur dokumentieren, was war, sondern auch den Mandanten helfen, Entscheidungen zu treffen – vor allem für das, was kommt.

Grammatikfehler als Leitsatz

Dieser Gedanke steckt auch im Leitsatz ihrer Kanzlei: „Wir helfen Ihnen Steuern.“ Grammatisch sei das eigentlich falsch, weiß die Inhaberin. Inhaltlich treffe es dagegen genau den Punkt. „Es geht nicht nur um die Steuer an sich, sondern auch um das Steuern des Unternehmens.“ Deshalb wird sie häufig frühzeitig einbezogen, etwa bei Unternehmensverkäufen, Nachfolgen oder privaten Umbrüchen.

Diese Entscheidungen begleitet Anne-Kathrin Muschke allerdings nicht allein: Ihr siebenköpfiges Team hält ihr dabei den Rücken frei. Was ihr in der Zusammenarbeit besonders wichtig ist, fasst eine neue Mitarbeiterin nach wenigen Wochen zusammen: „Jeder ist mal der Lehrende, mal der Lernende.“ Hinzu kommen Zusammenhalt und Loyalität. Dass das keine leeren Worte sind, zeigt ein Blick ins Team: Mit zwei Kollegen arbeitet sie bereits seit mehr als 30 Jahren zusammen.

Wer Anne-Kathrin Muschke nach Perspektiven fragt, bekommt keine Vision von weiterem Wachstum oder zusätzlichen Standorten. Ihre Antwort fällt schlicht aus. In der Zukunft soll ihre Kanzlei nämlich „genau so sein, wie sie heute ist“. Nicht größer, nicht lauter, nicht grundlegend anders.

Die Tür zu ihrer eigenen Kanzlei aufzuschließen, gehört für Anne-Kathrin Muschke inzwischen zum gelebten Alltag. Bereut hat sie den Schritt in die Selbstständigkeit nie. Zu sehr erfüllt sie bis heute das, was sie schon als 16-Jährige an dem Berufsbild faszinierte: mit Menschen zu arbeiten, dabei Orientierung zu geben und gemeinsam nach vorn zu schauen. Oder, wie sie selbst ausdrückt: „Es ist für mich einfach ein schönes Gefühl, den Menschen die Zahlen zu erklären.“ ○



Anne-Kathrin Muschke

ist Steuerberaterin und führt seit 2022 ihre eigene Kanzlei. Sie verbindet moderne Steuerberatung mit persönlicher Nähe und dem Blick in die Zukunft.



Vernetzen Sie sich mit Anne-Kathrin Muschke auf LinkedIn:



ROYALE STEUERZAHLUNG

Die Krone in der Anlage K

In Großbritannien trägt nun auch die Steuertransparenz Hermelin. König Charles III. hat offenlegen lassen, was die Krone seit seiner Thronbesteigung an Steuern gezahlt hat: mehr als 30 Millionen Pfund. Nicht die Überweisung ist neu, wohl aber ihre Veröffentlichung. Bei gewöhnlichen Steuerpflichtigen heißt so etwas Verwaltung; bei einem Monarchen wird daraus ein Ereignis mit Goldrand. Der Witz liegt im Kleingedruckten: Die Krone ist zu Einkommensteuer, Kapitalgewinnsteuer und Erbschaftsteuer rechtlich nicht verpflichtet, weil die einschlägigen Gesetze für sie nicht gelten. Gezahlt wird dennoch – freiwillig, auf Grundlage einer Verständigung mit dem Finanz-

ministerium. Der Fiskus triumphiert also nicht, sondern erhält eine höflich gerahmte Einverständniserklärung.

Die Einkünfte stammen unter anderem aus privaten Anlagen, den Anwesen Balmoral und Sandringham sowie dem Herzogtum Lancaster, einem historischen Portfolio aus Land, Immobilien und Investments. Zugleich soll der sanierte Buckingham Palace weiterhin vor allem Arbeitsplatz, Bühne und Besucherziel bleiben. Ein königliches Home Office, dem das Home abhandengekommen ist. Die königliche Kasse öffnet sich einen Spalt, lässt den Samtvorhang aber hängen. Eine Steuererklärung mit Krone ist eben zuerst Krone und dann Erklärung.



IMPRESSUM

Herausgeber

DATEV eG,
Paumgartnerstraße 6–14,
90429 Nürnberg

Verantwortlich:

Simone Wastl

Chefredakteurin:

Kathrin Ritter,
Tel.: +49 911 319-53162

E-Mail: magazin@datev.de

Stellv. Chefredakteur:

Sebastian Pech

Redaktion

Judith Birkmann, Robert Brütting (RA), Walter Deinzer, Constanze Elter, Carsten Fleckenstein, Marc Fuchs, Sabrina Huf, Rudi Kramer, Marco Krapp, Benedikt Leder, Shania Vivienne Schmidt, Astrid Schmitt, Birgit Schnee, Lutz Voswinkel, Sabine Wächter, Dietmar Zeilinger

Verlag

Vogel Corporate Solutions GmbH,
Axel-Springer-Straße 65,
10969 Berlin

Verlagsleitung: Ulf Reimer

Art Direction:

Thomas Schrimpf

CvD: Dominik Arndt (fr)

Bildredaktion: Anna Bianchi

Infografik: Julia Zimmermann

Herstellung: Silvio Schneider

Geschäftsführung:

Frank Parlow, Lutz Thalmann, Dennis Hirthammer, Matthias Bauer

E-Mail: ulf.reimer@vogel.de

Druck

DATEV Digital & Print Solution Center,
Sigmundstraße 172,
90431 Nürnberg

Das DATEV magazin erscheint monatlich in einer Druckauflage von 43.500 Exemplaren. Namentlich gekennzeichnete Veröffentlichungen geben in erster Linie die Auffassung des Autors wieder. Alle Beiträge sind urheberrechtlich geschützt. Alle Rechte sind vorbehalten.

Update

WAS SIE NICHT
VERPASSEN SOLLTEN



Individueller Newsletter für Wissen und Weiterbildung

Mit dem DATEV Wissens-Scout erhalten Sie regelmäßig passgenaue Empfehlungen zu Themen, die für gerade Ihre Kanzlei relevant sind – seien es Seminare, Lernvideos, Fachliteratur oder Recherchemedien. Den individuell für Sie zusammengestellten Newsletter erhalten sie immer aktuell und direkt per E-Mail.

→ go.datev.de/wissens-scout

Termine und Tagungen

27. und 28. Oktober

DATEV Sneak-Preview

In kurzen virtuellen Sessions erfahren Sie von DATEV-Produktverantwortlichen und -Experten aus dem Außendienst, was aktuell in der Produktentwicklung passiert und welche Konzepte und Lösungen umgesetzt werden. Die genaue Agenda wird kurz vor der Veranstaltung bekanntgegeben.

→ datev.de/shop/78269

12. November

DATEV-Marktplatz Expo

Bei der virtuellen Veranstaltung können Sie das Ökosystem im Detail erleben und sich über zahlreiche DATEV-Marktplatz Partner informieren. Diese stellen ihre Lösungen anhand von Livedemos in Sessions vor und zeigen dabei auch das Zusammenspiel mit DATEV-Software. Die Teilnahme ist kostenfrei.

→ go.datev.de/marktplatz-expo

2. Dezember

Digitale Datenanalysen

Steuerberater und Wirtschaftsprüfer lernen in dieser DATEV Info online die Grundlagen der Datenanalyse kennen. Außerdem geht es um die Einsatzfelder von DATEV Datenprüfung, zu denen die Analyse von Vorsystemen ebenso zählt wie die Anomalieerkennung und der Jahresabschluss.

→ datev.de/shop/77667

Die nächste Ausgabe erscheint am 30. Oktober 2026

Verpassen Sie nie mehr eine Ausgabe, und abonnieren Sie das DATEV magazin sowie den DATEV magazin Newsletter unter go.datev.de/magazin oder über den QR-Code.





Was wäre, wenn KI Sie im Kanzleialltag gezielt unterstützt?

Der DATEV Copilot bündelt relevante KI-Funktionen und steht Ihnen in MyDATEV als **zentraler KI-Assistent** zur Verfügung. Er unterstützt Sie in Ihren täglichen Kanzleiprozessen – **etwa bei der Texterstellung, der Analyse von Dokumenten oder bei Recherchen** – und hilft, Informationen schneller zu erfassen und gezielt weiterzuverwenden.

Die fachliche Bewertung und Entscheidung bleiben dabei jederzeit bei Ihnen. Der DATEV Copilot wird schrittweise in die DATEV-Cloud-Lösungen eingebettet und dort eingesetzt, wo KI sinnvoll entlastet.

Die Verarbeitung erfolgt **sicher und datenschutzkonform** innerhalb der DATEV-Cloud – auch bei sensiblen Daten.



Der DATEV Copilot macht es möglich!

Kostenfreie Lizenz jetzt im DATEV-Shop bestellen:
www.datev.de/shop/90431