Corporate Treasury News

Aktuelle Entwicklungen und Trends im Bereich Treasury kompakt zusammengefasst

Ausgabe 52 | Februar 2016

Liebe Leserinnen und Leser,

wir freuen uns, Ihnen die neueste Ausgabe unserer Corporate Treasury News präsentieren zu können.

Wenn Sie Fragen oder Anregungen zu Themen haben, die hier kurz behandelt werden sollen, dann schreiben Sie uns: de-corporate-treasury@kpmg.com

Aktuelle Meldungen rund um das Finanz- & Treasury-Management finden Sie bei uns im Internet oder über Twitter: www.twitter.com/KPMG_DE_FTM

Mit besten Grüßen,

Prof. Dr. Christian Debus Carsten Jäkel

Veranstaltungen und Termine

In unseren kostenfreien Webinaren nehmen wir zu aktuellen Themen aus dem Bereich Finanz- und Treasury-Management Stellung und informieren Sie über Strategien und die konkrete Implementierung.

Wählen Sie sich online ein und nehmen Sie an unseren thematischen Expertenrunden teil:

24. März 2016, 16:00 Uhr
Risikofaktor Zahlungsverkehr – aktuelle Praxisbeispiele und Präventionsmaßnahmen zu Fraud und e-Crime

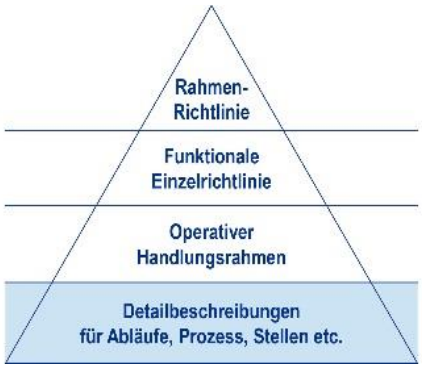
Von jedem Webinar fertigen wir einen Mitschnitt des Vortrages an. Sie finden ihn in unserem Webinar-Archiv.

Inhalt

Richtlinien - so aktuell wie die Zeitung von gestern?

Welches Unternehmen hat sie nicht: Richtlinien, Arbeitsanweisungen, Prozessbeschreibungen. In vielen Unternehmen gibt es organisatorische Handlungsrahmen in Hülle und Fülle. Unter Berücksichtigung all der Weiterentwicklungen und Veränderungen von IT und Prozessen in den letzten Jahren stellen sich vermehrt Unternehmen die Frage: Entsprechen die Richtlinien, Weisungen und Beschreibungen dem aktuellen in der Treasury-Organisation gelebten Prozess oder haben die Fortschritte den Handlungsrahmen bereits überholt?

Richtlinien thematisieren vor allem folgende Fragestellungen: Welche wesentlichen Ziele verfolgt das Treasury? Welche „Spielregeln" müssen stets eingehalten werden? Welche Aufgaben müssen abgedeckt werden? Wem werden die Kompetenzen zur Durchführung der Aufgaben zugeordnet und wie sind diese zu bearbeiten?



Darstellung: Aufbau eines Regelwerks

Richtlinien geben sowohl dem zentralen Treasury als auch den Tochtergesellschaften klare Weisungen vor und bilden idealerweise in den wesentlichen Ankerpunkten die Strategie und Aufgaben zu allen fachlichen Themen ab. Richtlinien dienen jedoch auch als eine revisionssichere Dokumentation und sollten sich am KonTraG, dem Leitfaden des Verbandes Deutscher Treasurer oder MaRisk orientieren. Funktionstrennung, Vier-Augen-Prinzip – Schlagwörter, welche in Richtlinien abzubilden sind.

Einmal geschrieben, für immer in der Schublade? Nicht selten geschieht genau das mit den oftmals mühsam erstellten „Meisterwerken". Um den Mitarbeitern im Treasury und den angrenzenden Abteilungen jedoch tatsächlich Orientierung zu geben, müssen diese Richtlinien auch regelmäßig adaptiert und an die Unternehmensanforderungen angepasst werden. Ändern sich Herausforderungen zum Beispiel durch Wachstum, Umstrukturierung in der Unternehmensorganisation oder Regulatorik, werden dadurch Prozesse geändert – dies muss sich auch in den Richtlinien wiederspiegeln. Haben Sie zum Beispiel Ihre Anforderungen an EMIR und darauf angepasste Prozesse bereits eingearbeitet?

Die richtige Kommunikation ist nach Freigabe vom CFO sowohl bei Neuerstellung als auch bei Anpassungen das A und O. Ein Regelwerk erfüllt nur dann den Zweck, wenn es im Unternehmen auch gelebt wird. Dafür ist im Rahmen der Erstellung oder Anpassung der Richtlinien die angemessene Kommunikation an alle Tochtergesellschaften sowie Überwachung der Einhaltung der Richtlinien essenziell. Bereits im Vorfeld muss klar definiert sein, wer für diese Aufgaben die Verantwortung trägt.

Im Rahmen unserer Projekte sehen wir verschiedene Ansätze bei der internen Kommunikation an die Tochtergesellschaften. Manche Unternehmen stellen ihre Richtlinien ausschließlich im Intranet zur Verfügung und kommunizieren dies per Rundmail, andere wiederum halten webbasierte Trainings ab, um die wesentlichen Punkte verbal zu transportieren und Frage- und Antwortrunden anzubieten. Eine weitere Entwicklung ist die Bereitstellung in Form eines internen Nachlagewerks als Online-Lexikon, teilweise kombiniert mit regelmäßigen Schulungen bzw. Tests.

Wir empfehlen neben einer aktiven Kommunikation auch einen regelmäßigen Internal Audit, der nicht nur die Einhaltung der Richtlinien in allen relevanten Bereichen bzw. Gesellschaften beinhaltet, sondern auch den Inhalt derselben gemäß den Unternehmensprozessen überprüft. Nur so können alle Gesellschaften konzernweit an einem Strang ziehen und richtlinienkonform agieren.

Autorin: Yvonne Bamberger, Manager,
ybamberger@kpmg.com

FinfraG – der Countdown für die Schweizer Derivate-regulierung läuft

Welche Pflichten treffen kleine nichtfinanzielle Unternehmen (NFC-) mit Sitz in der Schweiz unter der neuen OTC-Derivateregulierung? Welches sind die Gemeinsamkeiten, welches die Hauptunterschiede zu EMIR? Was müssen deutsche Mutterunternehmen im Hinblick auf Schweizer Konzerntöchter beachten?

Am 1. Januar 2016 sind das Finanzmarktinfrastrukturgesetz (FinfraG) und die Finanzmarktinfrastrukturverordnung (FinfraV) in Kraft getreten. Während das FinfraG, ähnlich zur EMIR in der EU, die grundsätzlichen Vorgaben und Regelungen der Schweizer OTC-Derivateregulierung enthält, konkretisiert das FinfraV als „Level II"-Text die Bestimmungen im Gesetz.

Welche Geschäfte sind im Anwendungsbereich des FinfraG und wie wird die Clearingpflicht ermittelt?

Zur Ermittlung der relevanten Transaktionen müssen weltweit alle vollkonsolidierten Gruppengesellschaften auf Transaktionen untersucht werden, die gemäß dem FinfraG als Derivate gelten. Derivate sind definiert als Finanzkontrakte, deren Wert von einem oder mehreren Basiswerten abhängt und die kein Kassageschäft darstellen. Wie unter EMIR ist bei als Derivat bilanzierten Verträgen, also zum Beispiel klassischen Fremdwährungs- oder Zinsderivaten, damit in der Regel keine weitergehende Prüfung der Derivateeigenschaft notwendig.

Schwieriger ist die Klassifikation von physischen Warenlieferverträgen. Sobald solch ein Vertrag über eine Börse oder ein organisiertes Handelssystem (OTF) gehandelt wird oder nach Wahl einer Vertragspartei bar abgerechnet werden kann (also ein unbedingter Barausgleich möglich ist), ist er als Derivat unter FinfraG zu klassifizieren. Nur wenn alle Punkte verneint werden können, liegt kein regulierungspflichtiges Geschäft vor. Analog zu EMIR müssen Unternehmen daher alle Verträge konzernweit auf diese Kriterien hin überprüfen. Hierbei hat der Schweizer Gesetzgeber zwar auf der einen Seite die Komplexität gegenüber EMIR reduziert, indem er auf den komplexen Prüfungsschritt der sogenannten „anderen derivativen Finanzinstrumente" verzichtet hat, auf der anderen Seite ist mit dem Handel über OTFs ein Kriterium aufgenommen worden, das bis auf Weiteres eine Rechtsunsicherheit für Schweizer Unternehmen schafft. Denn weder in der Schweiz noch seitens des EU-Regulierers ESMA gibt es bislang eine Aufstellung solcher, als OTF klassifizierter, Handelssysteme.

Die Vorschriften zur Berechnung der Clearingschwellen unter FinfraG sind eng an jene unter EMIR angelehnt. Es muss ein gleitender Durchschnitt der Nominalvolumina aller offenen OTC-Derivate, die in keinem Sicherungszusammenhang stehen, für einen Zeitraum von 30 Tagen für die verschiedenen Assetklassen berechnet werden. Ein Sicherungszusammenhang ist dann gegeben, wenn die Derivate zur Risikoreduzierung von Geschäfts- oder Liquiditätsrisiken abgeschlossen wurden. Neben Hedge Accounting gemäß IFRS ist auch Portfolio, Proxy- oder Makro-Hedging nach internationalen Standards, wie US GAAP und Swiss GAAP FER zulässig. Gruppeninterne Geschäfte, für die kein Sicherungszusammenhang nachgewiesen wird, sind bei der Berechnung ebenso zu berücksichtigen wie freiwillig geclearte Derivate. Die Höhe der Clearingschwelle pro Assetklasse ist ähnlich jener unter EMIR. Für Kredit- und Aktienderivate sind dies 1,1 Milliarden Schweizer Franken und für Zins-, Devisen-, Waren- und Sonstige Derivate 3,3 Milliarden Schweizer Franken.

Anders als nach EMIR ist eine Saldierung gegenläufiger Positionen mit identischem Basisinstrument, Währung und Fälligkeit auch dann zulässig, wenn es sich um Positionen mit unterschiedlichen Kontrahenten handelt. Zudem müssen Devisentermingeschäfte und Währungsswaps nicht mit in die Berechnung einbezogen werden, wenn diese Zug um Zug abgewickelt werden. Auch sind OTC-Derivate von finanziellen Gegenparteien, die in der Gruppe vollkonsolidiert werden (z.B. konzerninterner Banken oder Pensionskassen), bei der Schwellenbetrachtung zu berücksichtigen.

Welche Reportingpflichten treffen NFC-?

Grundsätzlich sind alle Gegenparteien unabhängig von ihrem Status sowie OTC und börsengehandelte externe und gruppeninterne Derivate (ETD) von der Meldepflicht betroffen. Die Meldung über Neuabschlüsse oder Änderungen an bestehenden Derivaten muss am folgenden Arbeitstag abgegeben werden.

Wie beim Dodd-Frank Act (DFA) besteht jedoch nur eine einseitige Meldepflicht. Derivate zwischen NFC- sind zudem grundsätzlich von der Meldepflicht ausgenommen. Somit müssen gruppeinterne Derivate in der Regel nicht gemeldet werden. Eine Backloading-Pflicht für bei Meldestart bereits ausgelaufene Derivate besteht nicht. Werden Derivate mit Gesellschaften eines höheren Status (wie z.B. Banken) abgeschlossen, ist immer die Gegenpartei (d.h. die Bank) meldepflichtig.

Eine Meldepflicht für NFC- besteht potenziell dann, wenn diese beispielsweise Derivate mit Nicht-Schweizer Banken abschließt, und die Bank weder unter FinfraG, noch unter einer als äquivalent anerkannten Regulierung meldet. Formale Äquivalenzentscheidungen seitens der Regulatoren stehen noch aus. Die Äquivalenz hinsichtlich der Meldepflicht ist nach aktueller Auslegung allerdings bereits dann gegeben, wenn die Meldeinhalte in einigen wesentlichen Punkten übereinstimmen. Damit würden die EMIR-Meldungen von in der EU ansässigen Banken die Meldepflicht erfüllen.

Welche Risikominderungstechniken müssen seitens NFC- eingehalten werden?

Die im FinfraG verankerten Risikominderungstechniken der Vertragsbestätigung, Portfolioabstimmung, Streitbeilegung und Portfoliokompression sind für externe und gruppeninterne, nicht geclearte OTC-Derivate einzuhalten. Weitere Übereinstimmungen mit EMIR sind neben den Bestätigungsfristen, dass vor dem Derivateabschluss mit dem jeweiligen Kontrahenten eine bilaterale Vereinbarung zur Einhaltung der Risikominderungstechniken getroffen werden und mindestens zweimal jährlich dokumentiert werden muss, ob eine Portfoliokomprimierung notwendig gewesen ist. Pflichten zur täglichen Bewertung der ausstehenden OTC-Kontrakte oder eine Handelsplatzpflicht, treffen NFC- darüber hinaus wie unter EMIR nicht.

Auf der anderen Seite muss für Derivateportfolios, bei denen eine andere NFC-Vertragspartei ist, kein Portfolioabgleich durchgeführt werden. Devisentermingeschäfte und Währungsswaps sind darüber hinaus grundsätzlich von den Risikominderungstechniken befreit.

Wann sind die Regelungen für NFC- verpflichtend umzusetzen?

Während die Reportingpflicht für NFC- und deren offener OTC-Derivate spätestens zwölf Monate nach der ersten Bewilligung oder Anerkennung eines Transaktionsregisters durch die FINMA erfüllt werden muss, tritt die Pflicht zur Meldung von börsengehandelten Derivaten (ETD) erst 18 Monate später in Kraft. Bislang ist kein Transaktionsregister in der Schweiz offiziell anerkannt, sodass die Meldepflicht für NFC- frühestens ab Mitte Februar 2017 in Kraft tritt.

Die Umsetzung der Risikominderungstechniken ist für NFC- ab dem 1. Juli 2017 und damit 18 Monate nach Inkrafttreten der FinfraV verpflichtend. Ein zentrales Clearing trifft, analog zur EMIR, nur große nicht finanzielle Gegenparteien (NFC+), sowie große finanzielle Gegenparteien (FC+). Eine Prüfungspflicht für NFC- in Bezug auf das FinfraG tritt ab 2017 in Kraft.

Autor: Christian Debus, Partner, cdebus@kpmg.com

e-Crime im Zahlungsverkehr – ein Aufruf zum Handeln

Ein Manager überweist 17 Millionen US-Dollar auf ausländische Konten, Lieferantenrechnungen werden an unbekannte Zahlungsempfänger umgeleitet und Cash Pools bedienen die Gier von betrügerischen Hackerbanden. Computerkriminalität macht auch vor dem Treasury keinen Halt mehr. Trotz solcher beunruhigenden Schlagzeilen nehmen wir zu diesem Thema bisher nur ein vergleichsweise geringes Bewusstsein in den Treasury-Abteilungen wahr. Alleine im Zahlungsverkehr gibt es eine Vielzahl von Risikofaktoren, die es zu analysieren und zu minimieren gilt, um Wirtschaftskriminalität zu verhindern. e-Crime ist daher längst nicht mehr nur ein Thema für die IT oder die Stammdatenverwaltung. Daher gilt auch für das Treasury: Es ist höchste Zeit zu handeln.

Man liest und hört es immer häufiger: Hackerbanden stehlen Kundendaten von den Servern teils großer, bekannter und bis dato als sicher geltenden Unternehmen. Dies ist noch weit weg von der Treasury-Abteilung. Aber sogenannte Fake President-Fälle (mehr dazu im weiteren Verlauf) stehen regelmäßig

in der Presse – es trifft große und kleine Unternehmen gleichermaßen. Spätestens hiermit ist e-Crime im Treasury angekommen. Und obwohl fast jeder von uns von diesen oder ähnlichen Vorfällen gehört hat, haben bisher nur wenige Treasury-Abteilungen präventive Maßnahmen dagegen ergriffen. Für das Treasury, aber vor allem auch für das gesamte Unternehmen, können Fake President-Fälle und andere Arten von e-Crime und Fraud im Treasury-Umfeld nicht nur zu immensen finanziellen Schäden führen, sondern auch zu Compliance-Risiken in Bezug auf Gesetzesverstöße.

Cyberkriminalität in Zukunft auch verstärkt Thema im Treasury

Eine vor Kurzem veröffentlichte KPMG-Studie mit dem Titel „Computerkriminalität in der deutschen Wirtschaft" zeigt, dass etwa 40 Prozent der Unternehmen in Deutschland in den letzten zwei Jahren von e-Crime betroffen waren. 89 Prozent der befragten Unternehmen schätzen das allgemeine Risiko aktuell als hoch bzw. sehr hoch ein und 70 Prozent gehen davon aus, dass das Risiko in den nächsten zwei Jahren weiter steigen wird. Unter dem Begriff der Cyberkriminalität bzw. dem Synonym e-Crime fallen unter anderem Delikte wie das Ausspähen und Abfangen von Daten, Verletzung von Urheberrechten, Computersabotage und die Manipulation von Konto- und Finanzdaten.

Letzteres betrifft dann auch das Treasury wo traditionell die Verwaltung der Bank- und Kontodaten, sowie die Abwicklung von Zahlungen beheimatet sind. Betrüger lassen sich auch hier immer wieder neue Szenarien einfallen, um sich persönlich am Eigentum der Firmen zu bereichern. Eine in der jüngeren Vergangenheit häufig angewandte Methode ist der sogenannte Fake President Fraud, auch als CEO Fraud bekannt. Er ähnelt stark dem allgemein geläufigen Enkeltrick – nur mit einer deutlich höheren Schadenssumme. Der Betrüger gibt sich dabei als Person des mittleren Managements, häufig auch als Vorstandsmitglied, aus und kontaktiert einen mit den Zahlungsprozessen vertrauten Mitarbeiter. Der Kontakt bleibt dabei unpersönlich und erfolgt meist nur über E-Mail oder Fax. Um den Mitarbeiter zu täuschen werden Absenderadresse, Signatur oder Brieflayout verblüffend echt gefälscht, zuweilen kommt die E-Mail sogar vom firmeneigenen Server. In dem Schreiben wird der Mitarbeiter dazu aufgefordert eine dringende Überweisung umgehend auf ein ausländisches Konto zu tätigen. Als Grund für den eiligen Geldtransfer wird oftmals eine strategische und geheime Vorstandsentscheidung oder ein streng vertrauliches Forschungs- und Entwicklungsprojekt genannt, welches unter keinen Umständen publik gemacht werden darf. Das Gefühl von sozialer Anerkennung („Der Vorstand hat ausgerechnet mich dazu auserwählt!") und der Druck der strengen Geheimhaltung veranlasst Angestellte dazu, diese Zahlungen ohne Absprache mit Kollegen oder dem direkten Vorgesetzten durchzuführen. Beispiele, bei denen Überweisungen in Höhe von sechs- oder siebenstelligen Beträgen getätigt wurden, gibt es viele. Besonders hart traf es 2015 einen US-Manager, der nach einer E-Mail seines angeblichen Chefs, 17 Millionen US-Dollar auf ein chinesisches Konto überwies. Auch bei deutschen Unternehmen nehmen wir eine starke Zunahme ähnlicher Fälle wahr.

Eine weiteres und häufig anzutreffendes Szenario ist jenes der „Payment Diversion". Während beim CEO Fraud versucht wird unter falschen Tatsachen eine Überweisung zu generieren, bleiben bei der Payment Diversion die originären Zahlungen unberührt. Der Trick dieser Methode besteht darin, den Weg des Geldes zu manipulieren. Die Betrüger geben sich dabei als Lieferant oder Geschäfts-partner des Unternehmens aus und informieren einen mit der Stammdatenverwaltung beauftragten Mitarbeiter formlos per E-Mail oder Fax, dass sich die Zahlungsinformationen geändert hätten. Sie bitten darum in Zukunft sämtlichen Zahlungsverkehr über die neue Bankverbindung abzuwickeln. Besonders raffinierte Täter kontaktieren die Person anschließend zusätzlich per Telefon, um sich über den Empfang des Änderungswunsches zu informieren. Durch diesen persönlichen Kontakt, die Tatsache, dass eine Änderung der Bankverbindung kein außergewöhnlicher Vorgang ist und dass es keine zusätzlichen auffälligen Kontobewegungen gibt, fällt es den Unternehmen schwer, diesen Trickbetrug schnell aufzudecken und die Täter zu identifizieren.

Schlagabtausch zwischen Treasury und IT um Verantwortung zur Abwehr möglicher Angriffe

Das Ausmaß einer solchen Gefährdung scheint bisher aber noch nicht zu allen Treasury-Abteilungen durchgedrungen zu sein. Auch Cash Pools sind ein besonders lohnenswertes Ziel: Jedes an den Cash Pool angeschlossene Konto hat Zugriff auf die Liquidität des gesamten Cash Pools und stellt somit einen potenziellen Angriffspunkt dar. Aus unserer Projekterfahrung heraus ist die Liste möglicher Einfallstore deutlich länger, als viele Treasurer denken. Einige der Risiken sind glücklicherweise bisher noch nicht von Angreifern erkannt worden und wir möchten an dieser Stelle auch keine Gebrauchsanleitung für mögliche Cyberattacken bereitstellen. Vielmehr möchten wir Treasury-Abteilungen für das Thema sensibilisieren, um sich mehr Gedanken zur Abwehr solcher Angriffe zu machen.

Bevor nun die Überlegung getroffen wird, welche möglichen Schutzmaßnahmen man einleiten kann, sollte man die unterschiedlichen Angriffspunkte abgleichen, um mögliche Risikoquellen zu identifizieren. Hier stößt man häufig bereits auf das *erste* große Problem: Wer treibt das Thema im Unternehmen überhaupt? Meist sind die Verantwortlichkeiten im Unternehmen noch nicht klar verteilt oder kommuniziert worden. Für die Treasury-Abteilung allerdings sind die Verantwortlichen schnell gefunden: die IT-Mitarbeiter. In den Augen vieler Treasurer suchen sich Betrüger den Weg über die Computersysteme und sollten daher primär von der IT geschützt werden. Die IT wiederum spielt den Ball zurück und begründet die Pflicht des Treasury darin, dass die IT nicht das Prozesswissen besitzt, um den Zahlungsverkehr angemessen vor Angriffen zu schützen. Beide Standpunkte für sich gesehen mögen durchaus schlüssig klingen, bringen das Unternehmen im Kampf gegen e-Crime allerdings keinen Schritt vorwärts. Es ist daher essenziell, dass die Verantwortlichkeiten klar definiert werden.

Hierbei kann die Antwort nur lauten, dass das Treasury die Gesamtverantwortung für die Sicherung der Liquidität und damit auch für die Sicherung des Zahlungsverkehrs übernimmt. Selbstverständlich kann eine ganzheitliche Betrachtung und ein ausreichender Schutz vor Wirtschaftskriminalität nur durch die zusätzliche Unterstützung der IT erreicht werden. Diese muss jedoch im Zweifel aktiv vom Treasury eingefordert werden. Das Beispiel des Fake President Fraud zeigt jedoch auch, dass sich das Treasury nicht nur auf die IT verlassen sollte und eine einseitige Betrachtung von Sicherheitsmängeln keinen wirksamen Schutz bietet. Eine ganzheitliche Betrachtung der Prozesse im Zusammenhang mit der IT Security ist deshalb unabdingbar. Durch die Identifikation vorhandener Risikofaktoren und erste Veränderungen der eigenen Strukturen und Abläufe im Unternehmen kann die Gefahr, selbst Opfer eines Cyberangriffs zu werden, bereits erheblich minimiert werden. Darüber hinaus sollten Treasury und IT gemeinsame Maßnahmen ergreifen, um das Risiko weiter einzugrenzen und finanzielle Schäden und Reputationsverluste zu vermeiden.

Mehr zum Thema e-Crime im Treasury erfahren Sie in unserem Webinar „Risikofaktor Zahlungsverkehr – aktuelle Praxisbeispiele und Präventionsmaßnahmen zu Fraud und e-Crime“ am 24. März 2016 um 16:00 Uhr. Für dieses Webinar begrüßen wir Michael Sauermann, Partner bei KPMG im Bereich Forensic, der uns aus der täglichen Praxis forensischer Untersuchungen im Bereich e-Crime und Zahlungsverkehr berichten wird.

Autor: Thomas Mehlkopf, Manager,
tmehlkopf@kpmg.com

Impressum

Herausgeber

KPMG AG
Wirtschaftsprüfungsgesellschaft
THE SQUAIRE, Am Flughafen
60549 Frankfurt

Redaktion

Prof. Dr. Christian Debus (V.i.S.d.P.)
Partner, Finance Advisory
T + 49 69 9587-4264
cdebus@kpmg.com

Carsten Jäkel
Partner, Finance Advisory
T + 49 221 2073-1522
cjaekel@kpmg.com

Newsletter kostenlos abonnieren
www.kpmg.de/newsletter/subscribe.aspx

www.kpmg.de

www.kpmg.de/socialmedia