KPMG
cutting through complexity

Corporate Treasury News

KPMG IN DEUTSCHLAND

Ausgabe 49 – November 2015

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 künftig in unserem Newsletter kurz behandelt werden sollen, dann schreiben Sie uns: de-corporate-treasury@kpmg.com

Aktuelle Meldungen rund um das Finanz- & Treasury-Management finden Sie auf unserer Internetseite oder über Twitter: www.twitter.com/KPMG_DE_FTM

Mit besten Grüßen,

Prof. Dr. Christian Debus Carsten Jäkel

In dieser Ausgabe

Währungsmanagement – Steuerung der bilanziellen Fremdwährungsrisikoposition
Seite 2

Die Einführung von SWIFT im Unternehmen – welche Anbindung an SWIFT ist die richtige?
Seite 4

Was in Sachen REMIT als nächstes zu tun ist.
Seite 7

Veranstaltungen und Termine

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

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

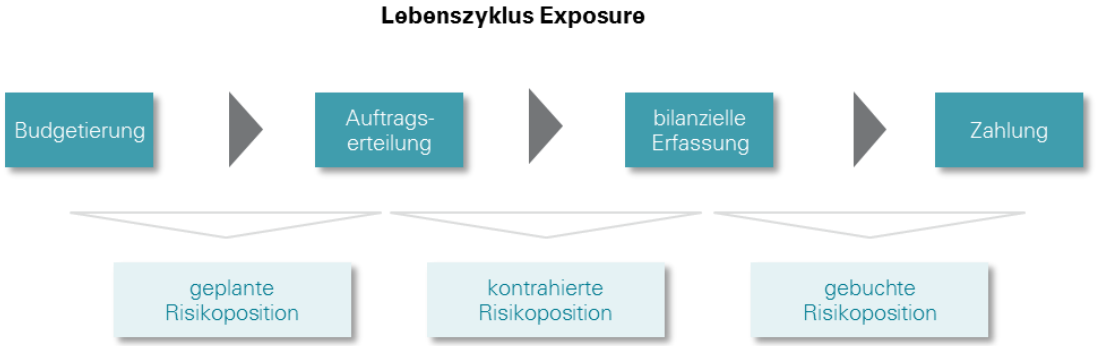
© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und "cutting through complexity" sind eingetragene Markenzeichen von KPMG International.

Währungsmanagement – Steuerung der bilanziellen Fremdwährungsrisikoposition

Nicht erklärbare Wechselkurseffekte trotz Währungssicherung sind ein häufiger Anlass für kritische Nachfragen des Management. Neben der unvollständigen Erfassung der Risikoposition sind deren im Zeitverlauf unterschiedliche und nicht hinreichend berücksichtigte Eigenschaften die wichtigsten Gründe hierfür.

Exposure-Lebenszyklus und Sichtbarkeit von Wechselkurseffekten

Risiken aus Fremdwährungspositionen folgen einem Lebenszyklus, dessen Beachtung wesentliche Bedeutung für die Gestaltung der Risikosicherungsstrategie hat. Der Lebenszyklus ergibt sich dabei aus der Zuordnung einer Risikoposition zu verschiedenen, zeitlich zu differenzierenden, Prozessschritten: Budgetierung, Auftragserteilung, bilanzielle Erfassung der Transaktion (in der Regel bei Lieferung oder Rechnungsstellung) und Zahlung. Ausgehend von diesen Schritten spricht man auch von geplanten, kontrahierten und bilanzierten bzw. gebuchten Risikopositionen.



© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft

Während sich der ökonomische Effekt von Wechselkursänderungen auf das Grundgeschäft über den gesamten Lebenszyklus erstreckt, ist in der Buchhaltung nur ein Teil dieses Effektes sichtbar. Denn solange die zugrunde liegende Transaktion nicht in der Bilanz erfasst wurde, verursacht sie auch keine Effekte in der Bilanz bzw. GuV. Sinkt also zum Beispiel bei einem Exportgeschäft zwischen Auftragskalkulation und der Einbuchung der Forderung der Wechselkurs, ist buchhalterisch noch kein Verlust realisiert. Vielmehr wird zunächst lediglich eine gegenüber der Planung betragsmäßig niedrigere Forderung als Umsatz erfasst. Diese Effekte aus Wechselkursveränderungen sind daher nicht aus dem Buchungsmaterial, sondern ausschließlich im Rahmen einer Nachkalkulation auf Basis der Kursentwicklung zu erkennen. Daher lässt sich das Wechselkursrisiko im Lebenszyklus bis zur bilanziellen Erfassung der Transaktion auch als kalkulatorisches Risiko bezeichnen, welches mit Fälligkeit der Risikoposition zahlungswirksam wird.

Wird die Transaktion, zum Beispiel bei Rechnungstellung, bilanziell erfasst, kann sie ab diesem Zeitpunkt im Rahmen der Fremdwährungsfolgebewertung Ergebniseffekte verursachen, die sich dann buchhalterisch im Währungsergebnis niederschlagen (zum Thema Währungsergebnis siehe Newsletter 48 aus Oktober 2015). Sinkt beispielsweise der Kurs nach Einbuchung der Forderung weiter, kommt es am nächsten Bewertungsstichtag zu Währungsverlusten, die in der GuV zu erfassen sind. Es besteht also ein buchhalterisches Bewertungsrisiko bis zu dem Zeitpunkt der Zahlung, zu dem die Kurseffekte vollständig realisiert werden.

Doch wie kann die bilanzielle Risikoposition gesteuert werden und welche unterschiedlichen Anforderungen bestehen gegenüber der Sicherung geplanter oder kontrahierter Transaktionen?

© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und "cutting through complexity" sind eingetragene Markenzeichen von KPMG International.

Sicherungskonzept für bilanzielle Risikopositionen

In der Regel unterscheiden sich die Risikopositionen in den unterschiedlichen Lebenszyklusphasen in der Höhe ihrer Eintrittswahrscheinlichkeit. Während in der Budget- und Planungsphase ein höheres Maß an Unsicherheit besteht, treten bilanzierte Transaktionen mit sehr hoher Sicherheit ein. Diesem Umstand wird zum Beispiel durch unterschiedliche Sicherungsquoten oder -bandbreiten Rechnung getragen. Während längerfristig geplante Transaktionen mit einer geringeren Quote, je nach Eintrittswahrscheinlichkeit zum Beispiel zu 25 oder 50 %, gesichert werden, um der Unsicherheit Rechnung zu tragen, können bilanzierte Risikopositionen mit sehr hohen Sicherungsquoten von bis zu 100% gesichert werden. Grundlage dafür muss demnach eine entsprechende Strukturierung der Risikopositionen im Treasury System anhand des Lebenszyklusmodells sein, um bilanzielle Risikopositionen von anderen Risikopositionen abgrenzen zu können. Zudem sollte die Sicherungsstrategie entsprechend eine Anpassung der Sicherungsquote bei Bilanzwirksamkeit berücksichtigen.

Neben der Eintrittswahrscheinlichkeit nimmt bei bilanzierten Transaktionen in vielen Fällen auch die zeitliche Bestimmbarkeit der Fälligkeit der Transaktion zu, da diese zum Beispiel durch die Rechnungsstellung hinreichend präzisiert wurde. Daher ist gegebenenfalls neben einer notwendigen Erhöhung der Sicherungsquote auch die Anpassung der Fälligkeit des Sicherungsgeschäfts vorzunehmen. Durch nicht ausreichende Nachjustierung der Sicherungsgeschäfte in Bezug auf die konkreten Fälligkeitstermine der Risikopositionen entstehen Inkongruenzen, die eine häufige Ursache für unerwartete Effekte im Währungsergebnis darstellen.

Rollierender Ansatz im Sinne einer „Währungsbilanz"

Da insbesondere letztgenannte Anforderung zur Nachjustierung der Sicherungsposition einen entsprechenden Ressourceneinsatz im Front Office erforderlich macht, wird in der Praxis auch ein weiterer Steuerungsansatz für das bilanzielle Währungsrisiko diskutiert: die Steuerung im Sinne einer Währungsbilanz.

Dabei werden im Sinne einer Bilanzaufstellung zu einem Stichtag die gebuchten aktivischen und passivischen Währungsrisikopositionen pro Währungspaar saldiert. Das daraus resultierende Nettoexposure bildet die Grundlage für einen kurzfristigen rollierenden Sicherungsansatz, mit einem Sicherungshorizont von beispielsweise 1-2 Monaten – unabhängig von den konkreten Fälligkeiten der einzelnen, gebuchten Risikopositionen. Im Rahmen einer regelmäßigen Neuberechnung der Währungsbilanz zum nächsten Betrachtungsstichtag erfolgt - unter Berücksichtigung der bestehenden Sicherungen - eine rollierende Anpassung der Sicherungspositionen. Dadurch kann sich der oben beschriebene Anpassungsaufwand der Einzeltransaktionen aufgrund von Ungenauigkeiten der Fälligkeiten reduzieren, da nur noch der Saldo der Währungsbilanz gesichert wird. Im Gegenzug lässt sich üblicherweise eine Reduzierung der Sicherungswirkung des Währungsmanagements in Bezug auf den gesicherten Kurs feststellen, da keine laufzeit-adäquate Kurssicherung erfolgt, sondern der Fokus auf einem Ausgleich der Effekte der bilanziellen Stichtagsbewertung liegt.

Fazit

Es bleibt festzuhalten, dass eine ausschließlich initiale Sicherung geplanter Transaktionen im Regelfall aufgrund des im Rahmen des Exposure-Lebenszyklus zunehmenden Informationsgehalts einer Risikoposition nicht ausreichend ist. Ebenfalls würde eine reine Sicherung der bilanziellen Risikopositionen das mögliche Währungsrisiko eines Grundgeschäfts nicht vollständig erfassen. Das Exposure muss über seinen gesamten Lebenszyklus analysiert und gesteuert werden. Der richtige Umgang mit dem bilanziellen Währungsrisiko stellt dabei einen elementaren Bestandteil bei der Reduzierung unerwünschter Währungsergebnisse dar.

Autor: Stephan Plein, Senior Manager, splein@kpmg.com

© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und "cutting through complexity" sind eingetragene Markenzeichen von KPMG International.

Die Einführung von SWIFT im Unternehmen – welche Anbindung an SWIFT ist die richtige?

Die seit mehr als 30 Jahren bestehende Genossenschaft SWIFT („Society for Worldwide Interbank Financial Telecommunication") sieht sich selbst nicht nur als Anbieter von Diensten, die einen sicheren und höchst zuverlässigen Austausch von Finanznachrichten zwischen registrierten Partnern über sichere Telekommunikationsnetze (das SWIFT-Netz) ermöglichen und standardisieren, sondern auch als Katalysator, um die Finanzwelt mit sinnvollen Ideen und Lösungen auf einer Plattform, dem SwiftNet, zusammenzubringen.

SWIFT verbindet schon seit Längerem nicht mehr nur Banken untereinander, sondern auch Nichtbanken mit Banken. Die Zusammenarbeit gliedert sich hierbei in Bereiche wie die Aufnahme von Geschäftsbeziehungen, den Austausch von standardisierten Finanznachrichten (FIN Messages) – zum Beispiel Bestätigungen und Zahlungen – sowie den interaktiven Austausch von Dateien auf xml-Basis (FileAct) oder Browse-Diensten (sicheres HTTP).

Entscheidet sich ein Unternehmen nun dafür, die Möglichkeiten dieser Plattform zu nutzen, stellen sich Fragen zum technischen Zugang: Ist bei der Einführung von SWIFT im Unternehmen der Aufbau einer komplett eigenen SWIFT-Infrastruktur im herkömmlichen Sinne unablässig, oder gibt es sinnvolle Alternativen? Welche Vor- und Nachteile müssen beachtet werden und welche Art der Anbindung unterstützt das eigene Geschäftsmodell am besten?

Warum überhaupt SWIFT nutzen?

Heute sind mehr als 10.000 Banken und Unternehmen in über 200 Ländern an SWIFT angebunden. Der überwiegende Teil ist in Europa sowie dem Mittleren Osten und Afrika angesiedelt (per August 2015 rund 66% der Teilnehmer), der Anteil asiatischer liegt bei ca. 13% und der Anteil amerikanischer Firmen bei rund 21%. Im Durchschnitt werden jeden Monat bis zu 500 Millionen Nachrichten ausgetauscht. Trotz dieser hohen Anzahl an Teilnehmern und der Menge an Nachrichten, die im SWIFT-Netzwerk ausgetauscht werden, hat SWIFT eine äußerst hohe Verfügbarkeit und Stabilität zu verzeichnen.

SWIFT löst – bezogen auf die FIN-Standards und die Zugangskanäle zu Banken - für viele Unternehmen das Problem unterschiedlicher Formate im Bereich Zahlungsverkehr und ist daher eine Möglichkeit zur Prozess- sowie Formatharmonisierung und somit zur Kostensenkung im diesem Bereich.

Neben implementierten Industriestandards wie IP-Konnektivität (Secure IP), VPN (Virtual Private Network)/IP Protection und PKI (Public Key Infrastructure) gibt es bei SWIFT auch eine strikte Aufgabenteilung durch entsprechende Zertifikate, Benutzerprofile und -rollen (RBAC - Role-Based Access Control) und die Einrichtung von Security Officers. Verschiedene Queues ermöglichen ein 4-Augen-Prinzip und die Aufgabentrennung nach zum Beispiel Erstellung, Verifikation, Autorisierung und Versand. Die Verschlüsselung auf drei möglichen Ebenen (Applikations-, Messaging- und Netzwerkebene) bildet somit eine sehr sichere Grundlage des Austausches von Nachrichten.

Was ist nun der optimale Zugang zu SWIFT?

Die hauseigene SWIFT-Landschaft

Wählt man den herkömmlichen Weg einer eigenen Infrastruktur mit selbst betriebenen hardwaretechnischen Komponenten und Netzwerkzugängen, müssen darauf Anwendungen betrieben werden, die von SWIFT bereitgestellt werden. Hierzu zählen im Wesentlichen SwiftAllianceAccess/Entry (SAA/SAE), SwiftAllianceGateway (SAG)

© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und "cutting through complexity" sind eingetragene Markenzeichen von KPMG International.

sowie SwiftAccord[1] , der Online Operations Manager O2M (Verwaltung von Sicherheitszertifikaten) und die Web Platform, die inzwischen allesamt webbasiert administriert und zugänglich gemacht werden.

Das Herzstück jeder Installation bildet SAA/SAE. Dort werden Geschäftspartner (MessagePartners) und eigene Entities/Gesellschaften (über Logical Terminals) eingerichtet und deren Beziehungen untereinander verwaltet (Beziehungsmanagement RMA) sowie das Routing und Reporting (Message Management) vorgenommen. SAG ist die Verbindung zum SwiftNet („Concentrator of traffic") und regelt unter anderem auch die Sicherheit durch spezielle Hard- und Software und geeignete Verschlüsselungsverfahren. Accord dient als Plattform für das Echtzeit-Matching von Confirmations (Bestätigungen), während die Web Platform die oben genannten Applikationen verwaltet und strukturiert.

Je nach geplantem Datenvolumen, den gebuchten Services, der Kategorie des Supports (Silber, Gold, etc.) und der Anzahl der anzubindenden Legaleinheiten des Unternehmens ergeben sich daraus aufsummierende Lizenz- und Servicegebühren. Unter diesen Gesichtspunkten kann eine Einführung von SWIFT - unter der Prämisse eine eigene Infrastruktur einsetzen zu wollen - jedoch schnell sehr kostspielig werden. Nicht selten bemängeln zudem Unternehmen, die diesen Weg gewählt haben, dass alle Vorgaben zum Betrieb des technischen Gateways von SWIFT kommen und recht starr sind. Beispiele hierfür sind Pflichtupdates, die mit kurzen Vorlaufsfristen eingespielt werden müssen, neue Standards, die jährlich systemweit eingepflegt werden müssen oder auch die feste Vorgabe der Netzbetreiber für die technische Anbindung an das SWIFT-Netzwerk.

Zumindest bei internationalen Konzernen mit vielen Tochterunternehmen weltweit wird die Verwaltung der Geschäftspartner und eigener Einheiten schnell kompliziert und aufwendig. Ein- und ausgehende SWIFT-Nachrichten wie Zahlungsaufträge und Kontoauszüge müssen durch viele verschiedene Queues auf unterschiedliche logische Einheiten ausgesteuert werden. Fehlermeldungen sind in diesem Zusammenhang oft kryptisch und schwer zu finden. Bei einer zurückgewiesenen Nachricht (zum Beispiel fehlerhafter Zahlungsauftrag) erhält man einen NAK-Text („Not AcKnowledged") als Code, der in diesbezüglichen Beschreibungen zwar nachrecherchiert werden kann, in der Praxis aber oft nicht genau den tatsächlichen Fehler beschreibt oder gar nicht zu finden ist.

Aus Administrationssicht machen folglich die vielen Einzelanwendungen, ein hoher Monitoring- und Administrationsaufwand sowie ein komplexes Routing den Support anspruchsvoll und zeitintensiv. Man sollte hier auf gut geschultes Personal zurückgreifen können, dessen Einarbeitung jedoch durchaus längere Zeit in Anspruch nehmen kann.

Alternative Anbindungen an SWIFT

Scheut man als Unternehmen die beschriebene komplexe Administration einer eigenen SWIFT-Infrastruktur, bleibt die Tür zu SWIFT dennoch nicht verschlossen. Denn glücklicherweise gibt es Alternativen und viele Corporates sind in der jüngeren Vergangenheit dazu übergegangen, die Dienste eines Service-Bureaus (SSB) in Anspruch zu nehmen oder SWIFT Alliance Lite2 zu nutzen.

Die Wahl eines SSB hat den Vorteil, dass Unternehmen die komplette technische Anbindung an SWIFT, den Betrieb der Zugangskomponenten sowie ausgewählte Services, wie zum Beispiel Formatkonvertierungen, als kostengünstiges Gesamtpaket eines Drittanbieters nutzen können. Zum einen kann dadurch der erstmalige Zugang zu SWIFT wesentlich schneller und effizienter eingerichtet werden, zum anderen können Kosten gespart werden. Die eigene Infrastruktur und internes Know-how werden auf ein Minimum reduziert, da das Service-Bureau den Betrieb und die Verwaltung der Umgebung übernimmt. Zudem sorgt ein SSB für Aktualität und Sicherheit hinsichtlich des Technologiestandards und zukünftiger Updates. Ein Nachteil aus Sicht der Unternehmen ist das Risiko, welches durch die Ausgliederung sensibler Daten an einen Dritten hervorgerufen wird und je nach Prozessdesign auch eine fehlende end-to-end Verschlüsselung. Neben Sicherheitsaspekten ist ferner darauf zu achten, dass das SSB Hochverfügbarkeit, redundante Server, Notfallpläne etc. gewährleistet.

Die angebotenen Dienste der SSBs sind je nach Anbieter unterschiedlich ausgeprägt. Von der schlichten Bereitstellung von Transfer-Services über eine vollumfänglich administrierte Outsourcing-Lösung, bis hin zum Angebot hauseigene Formate automatisiert in SWIFT-Formate umzuwandeln, gibt es hier vielerlei Abstufungen und Möglichkeiten zu jeweils unterschiedlichen Preismodellen. Dem tatsächlichen Einführungsprojekt ist daher unbe-

[1] Bezüglich SwiftAccord sei erwähnt, dass dieser Dienst am 31.10.2017 eingestellt wird. SWIFT verspricht zwar Hilfe und Unterstützung in der Auswahl und Implementierung einer neuen Lösung, registrierte Kunden von Accord sollten sich jedoch rechtzeitig Gedanken machen, welche Konsequenzen eine Ablösung von Accord in ihrem Unternehmen haben wird.

© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und "cutting through complexity" sind eingetragene Markenzeichen von KPMG International.

dingt ein strukturierter Auswahlprozess für den Dienstanbieter auf der Basis der individuellen Anforderungen vorzuschalten.

Alliance Lite2 ist dagegen eine von der SWIFT-Organisation eigens entwickelte schlanke, internet-basierte Lösung, die eine direkte Kommunikation mit SWIFT ohne Drittanbieter ermöglicht und ohne komplexe eigene Infrastruktur im Unternehmen auskommt. Zwar muss ein Unternehmen immer noch eigene Komponenten (Server, Netzwerk) ausfallsicher bereitstellen und darauf von SWIFT zur Verfügung gestellte Zugangssoftware betreiben. Die Komplexität und die seitens SWIFT gestellten Anforderungen an die Umgebung sind jedoch um ein Vielfaches geringer als im Vergleich zur „klassischen" SWIFT-Infrastruktur. So kann beispielsweise die technische Anbindung über das Internet per abgesicherter VPN-Verbindung erfolgen und erfordert demnach keine Standleitung über einen dedizierten Telekommunikationsanbieter. Dies spart Kosten, Zeit und Verwaltungsaufwand. Mithin eine Alternative für Unternehmen, die sich das vergleichsweise überschaubare Maß an technischer Administration zutrauen und keine Zusatzdienste eines SWIFT Service-Bureaus benötigen.

Fazit

Im konkreten Kontext eines multinationalen Unternehmens auf der Suche nach Sicherheit, Standardisierung und Zuverlässigkeit in der Bankenkommunikation ist SWIFT mitunter alternativlos. Bei der Einführung müssen die künftigen SWIFT-Nutzer jedoch abwägen, ob eine eigene SWIFT-Infrastruktur noch sinnvoll ist oder nicht eher die Inanspruchnahme der Dienste eines Service-Bureaus bzw. Alliance Lite2 in Frage kommen.

Beim Aufbau eines eigenen SWIFT-Gateways muss man sich über die Kosten und Aufwände, sowie die entsprechenden exklusiven Schulungen (nur direkt bei SWIFT erhältlich) der Mitarbeiter im Klaren sein. Eigene Mitarbeiter benötigen hierfür eine relativ lange Einarbeitungszeit und ein tiefes Verständnis der SWIFT-Welt und -Terminologie. Dies gilt gleichermaßen für die Lösung Alliance Lite2 von SWIFT, obgleich hierbei Kosten, Equipment und Aufwand erheblich reduziert werden können.

Die Entscheidung ist daher mitnichten einfach und eindeutig, denn es gilt unterschiedliche Entscheidungsparameter abzuwägen. Grundlage hierfür ist die eingehende Analyse auch und insbesondere der unterschiedlichen SSBs und ihrer angebotenen Dienste sowie der weiteren SWIFT-Alternativen.

Autor: Tobias Riehle, Manager, triehle@kpmg.com

Was in Sachen REMIT als nächstes zu tun ist.

Die am 7. Januar 2015 in Kraft getretene Durchführungsverordnung zu REMIT (EG 1348/2014) definiert die Meldeverpflichtungen zu Transaktionen beim Strom- und Gashandel. Während die Meldungen für sogenannten OMPs (organised market places) bereits am 7. Oktober 2015 gestartet sind, heißt dies nicht, dass Marktteilnehmer mit weiteren Aktivitäten bis zur Meldung von bilateralen Geschäften, die ab dem 7. April 2016 beginnt, warten können.

Inwieweit neben den naturgemäß meldepflichtigen Energieversorgungsunternehmen auch Industrie- und Handelsunternehmen meldepflichtige Marktteilnehmer sind, sollte in einer individuellen Betroffenheitsanalyse festgestellt werden, denn eine Vielzahl von Unternehmen wird den Regelungen der REMIT unterliegen.

Die Durchführungsverordnung sieht vor, dass Geschäfte, die ab dem 7. Oktober 2015 auf OMPs getätigt werden, auch von OMPs gemeldet werden sollen. Eine Liste aller OMPs wird von ACER auf ihrer Website zur Verfügung gestellt. Marktteilnehmer sollten für die Meldung von OMP-Geschäften ein sogenanntes „Reporting Agreement" mit dem jeweiligen OMP abschließen. Allerdings sind beim Handel auf OMPs auch sogenannte Backloading-Verträge zu beachten. Dies sind Verträge, die vor dem 7. Oktober 2015 auf einem OMP abgeschlossen wurden, aber (teilweise) nach dem 7. Oktober 2015 erfüllt werden. Zu beachten ist hier, dass die Meldungen dieser Verträge in der Regel nicht von OMPs übernommen werden, sodass der Marktteilnehmer selbst bei der Meldung

© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International"), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und "cutting through complexity" sind eingetragene Markenzeichen von KPMG International.

dieser Verträge aktiv werden muss. ACER sieht vor, dass alle Backloading-Verträge auf OMPs bis zum 5. Januar 2016 (7. Oktober 2015 plus 90 Tage) gemeldet worden sein sollen. An die zu meldenden Daten gelten nicht die gleichen Anforderungen wie für übliche Meldungen, sondern eine „Minimalanforderung“: in der Regel sind zu Transaktionen nur Daten zu melden, die dem Marktteilnehmer bereits vorliegen.

Um zu entscheiden, ob eine Meldung zu erfolgen hat oder nicht, ist bei den bilateralen Verträgen eine Unterscheidung zwischen Standard und Nicht-Standardverträgen vorzunehmen. Dafür müssen im Vorfeld meldepflichtige Verträge identifiziert und klassifiziert (Standard-/Nicht-Standardvertrag, Rahmenvertrag, Ausführung eines Rahmenvertrags, Endkundenvertrag, Gruppengeschäft, Option, Swap, etc.) werden. Der wesentliche Aufwand bei der Umsetzung der Durchführungsverordnung besteht in der Anreicherung der zu meldenden Daten. Bereits vorhandene Daten müssen identifiziert werden und nicht vorhandene Daten müssen angelegt werden. Gerade diese melderelevanten Daten liegen in Industrie- und Handelsunternehmen nicht oder nicht vollständig in elektronischer Form vor. Die Bereitstellung melderelevanter Daten und Klassifizierung der Vertragsarten muss allerdings bis zum 7. April 2016 abgeschlossen sein, denn dann beginnt die Meldeverpflichtung für bilaterale Geschäfte.

Bilaterale Meldungen können auch an einen anderen Marktteilnehmer oder an einen dritten Dienstleister delegiert werden. Das Entgelt des Dienstleisters orientiert sich im Wesentlichen an der Anzahl der abzugebenden Meldungen und am Implementierungsaufwand der Meldesoftware, der wiederum von der Datenlage beim Marktteilnehmer abhängt.

Eine Backloading-Regelung gibt es auch für bilaterale Verträge. Verträge, die vor dem 7. April 2016 abgeschlossen wurden, aber nach dem 7. April 2016 (teilweise) erfüllt werden, müssen bis zum 6. Juli 2016 (7. April 2016 plus 90 Tage) gemeldet worden sein. An die Daten gilt hier die gleiche Minimalanforderung.

Um auf die Anforderungen von REMIT vorbereitet zu sein und eine effiziente, rechtzeitige, vollständige und korrekte Meldung sicherzustellen, sollten die Projekte jetzt bereits in einem fortgeschrittenen Stadium sein. Falls dies nicht der Fall ist, sollte umgehend mit der Umsetzung begonnen werden.

Autor: Bardia Nadjmabadi, Senior Manager, bnadjmabadi@kpmg.com

Impressum

Herausgeber

KPMG AG
Wirtschaftsprüfungsgesellschaft
THE SQUAIRE, Am Flughafen
60549 Frankfurt am Main

www.kpmg.de

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

Die enthaltenen Informationen sind allgemeiner Natur und nicht auf die spezielle Situation einer Einzelperson oder einer juristischen Person ausgerichtet. Obwohl wir uns bemühen, zuverlässige und aktuelle Informationen zu liefern, können wir nicht garantieren, dass diese Informationen so zutreffend sind wie zum Zeitpunkt ihres Eingangs oder dass sie auch in Zukunft so zutreffend sein werden. Niemand sollte aufgrund dieser Informationen handeln ohne geeigneten fachlichen Rat und ohne gründliche Analyse der betreffenden Situation.

© 2015 KPMG AG Wirtschaftsprüfungsgesellschaft, ein Mitglied des KPMG-Netzwerks unabhängiger Mitgliedsfirmen, die KPMG International Cooperative („KPMG International“), einer juristischen Person schweizerischen Rechts, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG, das Logo und "cutting through complexity" sind eingetragene Markenzeichen von KPMG International.