Stellungnahme

zum Maßnahmenpaket zur Bekämpfung von MwSt-Betrug, insbesondere zur Einführung bestimmter Anforderungen für Zahlungsdienstleister, KOM(2018)812, und zur Stärkung der Verwaltungszusammenarbeit bei der Betrugsbekämpfung, KOM(2018)813

Die DATEV eG ist das Softwarehaus und der IT-Dienstleister für Steuerberater, Wirtschaftsprüfer und Rechtsanwälte sowie deren zumeist mittelständische Mandanten. Das Unternehmen zählt mit über 7000 Mitarbeitern zu den größten IT-Dienstleistern und Softwarehäusern in Deutschland.

Das Leistungsspektrum der DATEV reicht von mehr als 200 PC-Programmen über Cloud-Dienste wie Online-Anwendungen, Datenverarbeitung und -archivierung im Rechenzentrum bis hin zu Outsourcingleistungen sowie Sicherheitsdienstleistungen. Beratungsleistungen und Angebote zur Wissensvermittlung runden das Angebot ab.

Über 40.000 Mitglieder unserer Genossenschaft erreichen wir über 2,5 Mio. KMUs, deren Daten bei uns im Auftrag verarbeitet werden.

DATEV entwickelte sich konsequent zu einem international agierenden Dienstleister, der heute auch im Ausland (Italien, Österreich, Tschechien/Slowakei, Polen, Ungarn, und Spanien) unterstützt.

Die Stellungnahme der DATEV eG erfolgt ausschließlich aus dem Blickwinkel des Unternehmens als berufsständischer IT-Dienstleister, insofern wird sie unabhängig von Stellungnahmen berufsständischer Organisationen wie Kammern und Verbänden abgegeben.

Transparenzregister-Nummer: 5027241291-41

DATEV eG begrüßt das Vorhaben der Europäischen Kommission, den Mehrwertsteuerbetrug im elektronischen Geschäftsverkehr zu reduzieren, und das Ziel, die Mehrwertsteuerausfälle für die Mitgliedstaaten zu verringern und damit zur Haushaltskonsolidierung in der EU und zu gerechten Wettbewerbsbedingungen für die ehrlichen Unternehmen in der EU beizutragen, die unter dem unfairen Wettbewerb durch Betrüger leiden.

Als IT-Dienstleister der rechts- und steuerberatenden sowie wirtschaftsprüfenden Berufe sehen wir unsere Rolle darin, die Prozesse unserer Kunden und deren Mandanten optimal zu unterstützen und gesetzliche Regelungen in praxisgerechte Lösungen und Prozesse umzusetzen. Aus dem Blickwinkel erfolgt unsere Einschätzung zum Maßnahmenpaket zur Bekämpfung von MwSt-Betrug vom 12.12.2018.

Die Zielsetzung, Mehrwertsteuerbetrug aufzudecken, kann durch die Vorschläge in der vorliegenden Form[1] nicht effektiv erreicht werden:

1. Der **Richtlinien-Vorschlag** KOM(2018)812 sieht vor, dass Zahlungsdienstleister über grenzüberschreitende eCommerce-Zahlungsvorgänge mit wirtschaftlichem Bezug detaillierte Aufzeichnungen führen.

   - Der **Anwendungsbereich** ist nicht ausreichend klar.
     - Es muss klargestellt werden, dass hier Zahlungsdienstleister im weiteren Sinne verpflichtet werden, so auch Payment Service Provider für Kreditkarten und Kryptowährungen etc..

       Der Verweis auf Art. 243a Abs. 1 PSD2 hinsichtlich der Definition Zahlungsdienstleister "importiert" die Probleme aus PSD2. Ob Zahlungsdienstleister, die nur Kryptowährungen anbieten, unter Art. 243a Abs. 1 fallen ist fraglich, da die PSD2 in ihrem Anwendungsbereich nicht bestimmt, welche Zahlungen mit welchem Geld unter die Richtlinie fallen.
     - Der Verweis auf die Definition des Zahlungsvorgangs in § 4 Nr. 5 der PSD2-Richtlinie reicht nicht aus. Im Fokus stehen bei B2C eCommerce Geschäften Fernzahlungsvorgänge, die in § 4 Nr. 6 PSD2 definiert werden. Zur Klarstellung sollten auch Kryptowährungen, die zunehmend im internationalen Zahlungsverkehr eingesetzt werden, ausdrücklich aufgenommen werden.
     - Auch ist unklar, ob bei einer verketteten Zahlung (PayPal-Kreditkarte-Girokonto) diese eine Transaktion von jedem an der Transaktion beteiligten Zahlungsdienstleistern gemeldet werden muss. Dies erscheint nicht sinnvoll.
   - Als **Schwellenwert** sind in Art. 243b Abs.2 (b) 25 Zahlungen/Quartal an denselben Zahlungsempfänger je Zahlungsdienstleister vorgesehen. Die Erreichung des Schwellenwerts kann bei Nutzung mehrerer Zahlungsdienstleister jedoch ggf. nicht festgestellt werden. Im Gegenteil, bei Betrugsabsicht kann die Splittung aktiv genutzt werden, um die Erhebung von Zahlungsdaten zu verhindern.

[1] KOM(2018)812, KOM(2018)813.

- Art. 243d Abs. 1 sieht die **Speicherung von Informationen**, u.a. Namen/Unternehmensbezeichnung, USt-ID, IBAN/BIC Zahlungskonto, Adresse, vor. Diese sind für die Bekämpfung von Umsatzsteuerbetrug nicht valide genug.
    - Die Namensangabe durch den Zahler kann ungenau sein.
    - Auch die USt-ID kann den Zweck nicht erfüllen, da die USt-ID nur für eine eingeschränkte Gruppe von Zahlungsempfängern als Merkmal herangezogen werden kann. Privatpersonen verfügen in ihrer Eigenschaft als Zahlungsempfänger grundsätzlich nicht über eine USt-ID. Auch nicht jedes Unternehmen, da die USt –ID nicht automatisch vergeben wird und separat beantragt werden muss.
    - Der Länderbezug der IBAN/BIC ist nicht verlässlich genug und lässt auch Spielraum für bewusste Umgehungen.

      Im vorgesehenen Verfahren wird anhand der Kontoinformationen (IBAN/BIC) sowohl auf den Ort des Zahlers als auch auf den Ort des Zahlungsempfängers rückgeschlossen. Bei Verwendung eines z.B. nicht im Ansässigkeitsstaat des Zahlers/Zahlungsempfängers befindlichen Kontos funktioniert das angedachte Verfahren nicht. (Eine BIC gibt nicht unbedingt Auskunft über den Ort, an dem die MwSt angefallen ist.) Zudem kann z.B. bei Zahlungen über PayPal keine Zuordnung über die IBAN erfolgen, da E-Mail-Adressen verwendet werden. Auch durch „Konstrukte" wie z.B. Alipay (China) und barzahlen.de kann eine Systemumgehung erreicht werden. Durch das Bezahlen an der Kasse gibt es keine zwingende Verbindung mehr zu einem Zahlungsdienstleister bzw. zu einer nationalen IBAN.

  Vor dem Hintergrund des in Zukunft zu erwartenden steigenden Einsatzes von Kryptowährungen im internationalen Zahlungsverkehr, sollten Regelungen zum Umgang mit selbigen berücksichtigt werden, da hier die im Rahmen des Richtlinienvorschlags genannten zu speichernden Informationen nicht vorliegen.

- Durch hohes Invest von Wirtschaft und Banken sind die qualitativ hochwertigen **Standards NextGenPSD2 und XS2A (Access to Account)** erarbeitet worden. Diese könnten die **notwendigen Daten und deren sicheren Transfer sehr viel besser** abdecken, als die derzeit vorgesehene Aufzählung der zu übermittelnden Daten. Daher sollten die Richtlinie und Verordnung auf den Standard setzen. Er sollte für diese Zwecke um die weiteren notwendigen Anforderungen wie z.B. einer Lieferadresse ergänzt werden.

2. Der **Verordnungs-Vorschlag** (KOM(2018)813) zur Verwaltungszusammenarbeit enthält Bestimmungen zur Erhebung und Auswertung der Daten im Hinblick auf die Betrugsaufdeckung über ein neues zentrales elektronisches System (CESOP) durch Eurofisc-Beamte. Diese **überzeugen nicht**:

   Wegen der Unterschiedlichkeit der über die jeweiligen umsatzsteuerlichen Meldeverfahren u.a. (M)OSS, Zusammenfassende Meldung (ZM) (hier: Lieferadresse) und an CESOP (u.a. IBAN) zu meldenden Daten werden beim Abgleich auch in Fällen, in denen kein Betrug vorliegt, Abweichungen festgestellt werden. Vor dem Hintergrund der Erfahrung von DATEV um die Herausforderungen bei einem Matching stellen wir den Erfolg des vorgeschlagenen Systems in Frage.

   Vorgesehen ist in Art. 24b Abs. 2, 24e (d) die Erhebung der Daten durch den Mitgliedstaat beim Zahlungsdienstleister über ein festzulegendes EU-weit einheitliches elektronisches

Standardformular. Wie bereits erwähnt, decken die Standards NextGenPSD2 und XS2A die notwendigen Daten und Transfers sehr viel besser ab, als die derzeit vorgesehene Aufzählung der zu übermittelnden Daten und sollte – erweitert um die Lieferadresse – genutzt werden.

Die Vorschläge der EU-Kommission scheinen nicht geeignet, um signifikant zur Betrugsbekämpfung beizutragen und sollten daher nicht verabschiedet werden.

Grundsätzlich zeigt sich hier der in der digitalen Wirtschaft - auch in anderen Kontexten - erhebliche Bedarf an digitalen Identitäten für Wirtschaftsteilnehmer. Es sollte daher zügig eine **digitale EU-weite WirtschaftsID** geschaffen werden.