Für Ihre Kammermitteilungen **004/2019**

BStBK: Hinweise zur E-Mail-Kommunikation

Derzeit wünschen viele Mandanten und auch die Finanzverwaltung keinen verschlüsselten E-Mail-Verkehr. Aus berufsrechtlichen und datenschutzrechtlichen Gründen sollten Steuerberater grundsätzlich einen verschlüsselten Nachrichtenaustausch wählen. Hierbei ist zu beachten, dass man zwischen folgenden Verschlüsselungsarten im E-Mail-Verkehr unterscheiden muss:

Die Transportverschlüsselung

Im E-Mail-Verkehr ist als Standardverschlüsselung grundsätzlich die sog. Transportverschlüsselung (SSL/TLS-Verschlüsselung) vorgesehen. Sofern der Absender oder der Empfänger E-Mails mit Programmen wie Outlook oder die vom Handy-Hersteller vorinstallierten E-Mail-Anwendungen nutzt, sollte überprüft werden, dass stets SSL/TLS aktiviert ist. Sobald die Transportverschlüsselung auf beiden Seiten eingestellt ist, kann die E-Mail-Kommunikation von Beginn an ohne weitere Abstimmung verschlüsselt erfolgen. Die Transportverschlüsselung ist grundsätzlich eine Punkt-zu-Punkt-Verschlüsselung, die man sich wie einen Briefumschlag vorstellen kann. Der Inhalt wird bei der Übermittlung zwischen dem Absender und seinem E-Mail-Anbieter sowie zwischen zwei E-Mail-Anbietern untereinander und zwischen E-Mail-Anbieter und Empfänger verschlüsselt bzw. durch einen Briefumschlag geschützt. Allerdings wird die E-Mail beim E-Mailanbieter entschlüsselt, z. B. zur Prüfung (Spam, Viren, De-Mail-Metadaten) oder zur Kategorisierung. Dies ist insoweit unproblematisch, da für E-Mail-Anbieter in Deutschland das Fernmeldegeheimnis nach § 88 TKG gilt. Zusammenfassend bedeutet es, dass die Mails auf dem Internetweg geschützt sind – lediglich auf den Client-Rechnern und den E-Mail-Servern liegen sie unverschlüsselt vor.

Die Ende-zu-Ende-Verschlüsselung

Im Unterschied zur Transportverschlüsselung werden bei der Ende-zu-Ende-Verschlüsselung nicht die einzelnen Wege im Versandkanal verschlüsselt, sondern jede E-Mail wird vom Anfang bis zum Ende verschlüsselt. Nur Absender und Empfänger können

den Inhalt der E-Mail lesen, wenn sie den notwendigen Schlüssel haben. Eine Ende-zu-Ende-Verschlüsselung basiert auf einem der beiden technischen Standards S/MIME oder PGP bzw. GPG. Die beiden Standards sind untereinander nicht kompatibel. Dies bedeutet, beide Kommunikationspartner müssen den gleichen Standard nutzen.

Bei einer Ende-zu-Ende-Verschlüsselung haben es potentielle Angreifer sehr schwer, die E-Mails unterwegs abzufangen und zu manipulieren. Dennoch sind auch hier bereits Sicherheitslücken bekannt geworden (vgl. Pressemittelung der FH Münster vom 15. Mai 2018). Da der Anwender bei der Ende-zu-Ende-Verschlüsselung selbst aktiv werden muss, um die Technologie nutzen zu können, hat sich diese Technologie noch nicht flächendeckend durchgesetzt und wird von Mandanten teilweise abgelehnt.

Elektronischer Nachrichtenaustausch zwischen Steuerberater, Mandant und Dritten

Steuerberater unterliegen der berufsrechtlichen auch strafbewehrten Pflicht zur Verschwiegenheit. Unklar war bisher, welches Sicherheitsniveau bzw. welche Art der E-Mail-Verschlüsselung berufsrechtlich zulässig ist. Im Oktober 2018 hat die BStBK die *Hinweise für den Umgang mit personenbezogenen Daten durch Steuerberater und Steuerberatungsgesellschaften* zusammen mit dem DStV e.V. aktualisiert. Hierin wird im Hinblick auf die berufsrechtlichen Verschwiegenheitspflichten von Seiten der BStBK grundsätzlich eine verschlüsselte E-Mail-Kommunikation mit dem Mandanten empfohlen.

<u>Transportverschlüsselung ist ausreichend</u>

Eine Ende-zu-Ende-Verschlüsselung ist nicht erforderlich. Ausreichend ist nach den Hinweisen der BStBK die sog. „Transportverschlüsselung“. Diese Auffassung wird u. a. auch von Schöttle in BRAK Mitteilungen 3/2018 vertreten. Hierzu muss der Steuerberater sicherstellen, dass die E-Mail auf dem Transportweg verschlüsselt ist und sich die Server der E-Mail-Provider des Steuerberaters und des Mandanten in Deutschland befinden. Dies sollte sorgfältig mit dem Mandanten besprochen werden. Bei einem KMU-Mandat könnte beispielsweise darauf geachtet werden, dass von Seiten des Mandanten ein deutscher E-Mail-Provider für die Kommunikation mit dem Steuerberater genutzt wird. Viele deutsche E-Mail-Provider haben sich der Initiative E-Mail MADE IN GERMANY angeschlossen und bieten die Transportverschlüsselung und die Datenspeicherung in Deutschland nach den deutschen Daten-

schutzstandards standardmäßig an. Weitere Informationen findet man hierzu unter: www.e-mail-made-in-germany.de.

Auch De-Mail nutzt grundsätzlich eine Transportverschlüsselung und ist per Gesetz als „sicher“ eingestuft (vgl. § 130a Abs. 4 ZPO). Grundlegender Unterschied zwischen einer einfachen transportverschlüsselten E-Mail und einer De-Mail ist die Tatsache, dass bei De-Mail der Absender und der Empfänger vorher verifiziert und somit eindeutig zugeordnet werden können. Auch in § 87a AO ist geregelt, dass bei der Übermittlung von Daten, die dem Steuergeheimnis unterliegen, ein geeignetes Verfahren zur Verschlüsselung zu verwenden ist. Die kurzzeitige automatisierte Entschlüsselung, die beim Versenden einer De-Mail-Nachricht durch den akkreditierten Dienstanbieter zum Zweck der Überprüfung auf Schadsoftware und zur Weiterleitung an den Adressaten der De-Mail-Nachricht erfolgt (Transportverschlüsselung), verstößt nicht gegen dieses Verschlüsselungsgebot. Somit steht der Versendung von E-Mails, die mit einer Transportverschlüsselung versehen sind, das Berufs- und Steuergeheimnis nicht entgegen.

Um das Sicherheitsniveau zu erhöhen, können E-Mail-Anhänge zusätzlich mit einem Passwort geschützt werden oder E-Mails mit einer Ende-zu-Ende-Verschlüsselung übermittelt werden. Dies sollte individuell beurteilt werden. Dabei ist der Schutzbedarf der übermittelten Daten zu berücksichtigen.

Einwilligung des Mandanten in einen unverschlüsselten E-Mail-Verkehr ist berufsrechtlich zulässig

Grundsätzlich ist eine verschlüsselte E-Mail-Kommunikation mit dem Mandanten vorzuziehen. Wenn der Mandant dies jedoch ausdrücklich wünscht, ist auch eine unverschlüsselte E-Mail-Kommunikation berufsrechtlich zulässig. Der Mandant sollte dann auf die Gefahren einer unverschlüsselten E-Mail-Kommunikation hingewiesen werden. Wenn es sich um sensible Daten bzw. Dokumente handelt (z. B. Jahresabschluss, Steuererklärung, betriebswirtschaftliche Auswertungen) ist es erforderlich, dass sich der Steuerberater beim Mandanten bezüglich dieser Daten bzw. Dokumente die konkrete Einwilligung zum unverschlüsselten Versand einholt.

Es ist zu empfehlen, dass bei Abschluss des Mandatsvertrages die Wege und Regeln der elektronischen Kommunikation mit dem Mandanten vereinbart werden. Bei Daten Dritter (z. B. Unterlagen zur Lohnbuchhaltung, Daten des Ehepartners) kann der Verzicht auf die E-Mail-Verschlüsselung grundsätzlich nur vom Dritten selbst eingeholt werden. Daher sollte in der Vereinbarung erläutert werden, dass die Zustimmung des Mandanten nicht für Daten Dritter gilt. **Eine Mustervereinbarung ist diesem Dokument beigefügt.**

Hinweise zum Datenschutz

Unter den Datenschutzaufsichtsbehörden besteht derzeit keine einheitliche und klare Auffassung darüber, welches Sicherheitsniveau bzw. welche Art der E-Mail-Verschlüsselung datenschutzrechtlich zulässig ist. Der Hamburgische Landesdatenschutzbeaufauftragte führt zu dieser Frage aus, dass aus datenschutzrechtlicher Sicht eine Ende-zu-Ende-Verschlüsselung zu bevorzugen sei. Dabei ist jedoch auch eine Abwägung zwischen Schutzbedarf auf der einen und der Aufwand auf der anderen Seite zu treffen. Am Ende kommt dieser zur Erkenntnis, dass aber auch auf die Nutzung von De-Mail, welche den Einsatz von Transportverschlüsselung garantiert, zurückgegriffen werden kann.

Zu der Frage, ob datenschutzrechtlich ein Verzicht auf die Verschlüsselung möglich ist, wird überwiegend die Auffassung vertreten, dass ein Verzicht auf Standards der Datensicherheit möglich ist, da ein Betroffener freiwillig bestimmen kann, wie weit er den Schutz des informationellen Selbstbestimmungsrecht zieht (vgl. VG Berlin 24. Mai 2011, Az. 1 K 133/10, Potthoff, NWB 2018, S. 287 vgl. 2b) datenschutzrechtliche Beurteilung).

Elektronischer Nachrichtenaustausch zwischen Steuerberater und Finanzamt

Das Finanzamt muss nach § 87a Abs. 1 Satz 3 AO grundsätzlich eine Verschlüsselung verwenden, wenn es Daten auf elektronischem Wege versendet, die dem Steuergeheimnis nach § 30 AO unterliegen. Eine Verschlüsselung seitens des Finanzamts ist nicht erforderlich, soweit nur allgemeine Auskünfte erteilt oder z. B. Formulare versendet werden. Vom Steuerpflichtigen an das Finanzamt zu übermittelnde Daten werden von der Vorschrift jedoch nicht erfasst. Derzeit hat sich die Finanzverwaltung in den einzelnen Bundesländern zum Umgang mit E-Mails unterschiedlich aufgestellt.

Verschlüsselte E-Mails werden grundsätzlich nicht zugelassen. Insgesamt hat sich die Finanzverwaltung bislang gegen eine E-Mail Kommunikation mit dem Steuerpflichtigen oder dem Steuerberater entschieden und hat einen eigenen Weg für die Kommunikation mit dem Steuerpflichtigen und dem Steuerberater entwickelt. Mit ELSTER, welches auch über den Eric-Client an die Steuerberatersoftware angebunden ist, soll eine sichere und bei allen Finanzämtern einheitliche Kommunikationsmöglichkeit geschaffen werden. Folgende Standard-Kommunikationsszenarien vom Steuerpflichtigen/Steuerberater zum Finanzamt sind bereits heute in ELSTER vorgesehen:

- Einspruch gegen einen Steuerbescheid,
- Antrag auf Fristverlängerung für die Abgabe der Steuererklärung,
- Antrag auf Anpassung von Vorauszahlungen,
- eine Mitteilung an das Finanzamt („Sonstige Nachricht“),
- steuerliche Anmeldung.

Weitere strukturierte Nachrichten wie z. B. der digitale Verwaltungsakt über ELSTER sollen folgen. Auch die digitale Übersendung von Anhängen und Belegen soll in den nächsten Jahren möglich sein. Die Finanzverwaltung strebt die umfassende digitale Kommunikation zwischen Finanzamt und Steuerpflichtigen/Steuerberater über ELSTER an.

Ausblick

Der Entwicklungsstand der Technik und die tatsächliche Verfahrensweise im Umgang mit E-Mails sollten weiter beobachtet werden. Daraus können sich in Zukunft neue oder andere Anforderungen an die datenschutzgerechte und berufsrechtlich zulässige Nutzung von E-Mails ergeben.

7. Februar 2019
Be/Ze

Verteiler:
Präsidenten
Steuerberaterkammern

Anlage

Regelungen zur elektronischen Kommunikation
zwischen Auftraggeber und Auftragnehmer

Der Auftraggeber wünscht eine Korrespondenz

☐ per SMS
☐ per E-Mail
☐ per Telefax

1. E-Mail Kommunikation

Wird im Rahmen der elektronischen Kommunikation zwischen Auftraggeber und Auftragnehmer oder sonstigen Dritten (z. B. Kreditinstituten) die Übermittlung von Daten nicht durch eine geeignete Verschlüsselung geschützt, besteht die grundsätzliche Gefahr, dass Daten von Dritten abgefangen und gelesen werden können.

In Kenntnis dieser Gefahr wünscht der Auftraggeber die Korrespondenz per E-Mail an folgende E-Mail-Adresse:

_____

UNGESICHERTE KOMMUNIKATION

☐ ohne weitere Sicherungsmaßnahmen

GESICHERTE KOMMUNIKATION

☐ passwortschützt
☐ unter Einsatz einer Transportverschlüsselung
In diesem Fall stellt der Auftraggeber sicher, dass er E-Mails transportverschlüsselt empfangen kann.
☐ unter Einsatz einer Ende zu Ende Verschlüsselung

2. Regelung zu sensiblen Daten

Der Auftragnehmer darf Jahresabschlüsse, Steuererklärungen, betriebswirtschaftliche Auswertungen, _____ an den Auftraggeber und an Dritte, mit denen der Auftraggeber in Geschäftsbeziehung steht (z. B. Kreditinstitute)

☐ passwortgeschützt
☐ unter Einsatz einer Transportverschlüsselung
☐ unter Einsatz einer Ende zu Ende Verschlüsselung
☐ unter Einsatz einer Cloud-Plattform
☐ unverschlüsselt

versenden oder von diesen empfangen, wenn die Übermittlung oder der Empfang vom Auftrag umfasst ist.

3. Regelungen zu Daten von Dritten

Sind Daten Dritter betroffen (z. B. im Lohnbereich, ggf. Daten des Ehepartners) erfolgt kein unverschlüsselter Versand. Die Daten werden dem Auftraggeber wie folgt zur Verfügung gestellt:

☐ passwortgeschützt
☐ unter Einsatz einer Transportverschlüsselung
☐ unter Einsatz einer Ende zu Ende Verschlüsselung
☐ unter Einsatz einer Cloud-Plattform
☐ Postweg

Der Auftraggeber kann diese Einwilligung jederzeit widerrufen.

Unterschrift des Auftraggebers: _____