Ransomware

Sind Lösegeldzahlungen bei Ransomware-Angriffen steuerlich abzugsfähig?

Steuerliche Folgen bei Opfern von Cybercrime

PETER BRÄUMANN / GEORG KOFLER / MICHAEL TUMPEL*)

Ein Aspekt der wachsenden Cyberkriminalität ist die digitale Erpressung durch sogenannte *„Ransomware“*: Dabei werden die Computersysteme des Opfers mit einem Schadprogramm infiziert. Dieses verschlüsselt anschließend die Nutzerdaten. Für deren Wiederherstellung wird die Bezahlung von *„Lösegeld“*, meist in Form von nicht nachzuverfolgenden *Bitcoins*, gefordert.[1]) Vielfach wird dieser Forderung Folge geleistet, um den Zugang zu den eigenen Daten zurückzuerlangen, die betrieblichen Abläufe wiederherzustellen und allenfalls auch die Veröffentlichung sensibler Informationen im Internet zu verhindern.[2]) Im Folgenden wird der Frage nachgegangen, ob diese Lösegeldzahlungen im unternehmerischen Bereich steuerlich abzugsfähig sind.

1. Wesentliche Voraussetzung: betriebliche Veranlassung

Der Begriff *„Ransomware“* enthält das englische Wort *ransom* für Lösegeld. In der bisherigen steuerrechtlichen Dogmatik wird das Schlagwort der Lösegeldzahlungen für gewöhnlich mit der Entführung natürlicher Personen in Verbindung gebracht. Auch wenn es sich dabei um Betriebsinhaber oder Gesellschafter handelt, scheidet ein Abzug derartiger Zahlungen als steuerliche Betriebsausgabe aus, weil das Motiv der Entführung in der Vermögenslage der Person liege und damit deren privaten Lebensbereich zuzuordnen sei. Prämien einer Lösegeldversicherung werden daher ebenso wenig als mögliche Betriebsausgaben betrachtet.[3]) Im Schrifttum wurde dazu aber einschränkend vertreten, dass im Falle von entführten bzw versicherten Arbeitnehmern der Abzug zustehen müsse, da eine betriebliche Veranlassung hier regelmäßig evident sei.[4]) Nach Ansicht der Finanzverwaltung in den EStR gehören die finanziellen Folgen einer Erpressung *„zwar in der Regel in den Bereich der privaten Lebensführung, jedoch sind betrieblich veranlasste Ausnahmen denkbar, zB Drohungen mit Geheimnisverrat an die Konkurrenz, Beschädigung oder Zerstörung von Wirtschaftsgütern, Vergiftung von durch den Betrieb erzeugten (bereits in Letztverbrauchermärkte gelangten) Lebensmitteln“*.[5])

*) MMag. Dr. Peter *Bräumann* ist Assistenzprofessor am Institut für betriebswirtschaftliche Steuerlehre der Johannes Kepler Universität Linz. Univ.-Prof. Dr. Michael *Tumpel* ist Vorstand dieses Instituts. Univ.-Prof. Dr. Georg *Kofler*, LL.M. ist Universitätsprofessor für internationales Steuerrecht an der Wirtschaftsuniversität Wien. Die Autoren sind Mitglieder des Law Lab des Linz Institute of Technology (LIT). Dieser Beitrag geht auf eine Anregung aus der Praxis zurück.

1) Siehe dazu etwa *Bundeskriminalamt*, Cybercrime Report 2020, Lagebericht über die Entwicklung von Cybercrime (2021) 14 ff.

2) In Deutschland wird geschätzt, dass knapp 40 % aller mit Ransomware erpressten Unternehmen das Lösegeld gezahlt haben (siehe *Meyer/Benzmüller/Simonis*, Werbeblocker als Schutz vor Schadsoftware, CR 2017, 274 [275]).

3) Siehe Rz 1594 EStR; BFH 30. 10. 1980, IV R 27/77; anders womöglich bei besonderer Gefährdungslage im Ausland, dazu *Wunderlich*, Steuerliche Behandlung von Lösegeldzahlungen und Prämien zu einer Entführungsrisikoversicherung, DStR 1996, 2003 (2003 ff).

4) Siehe zB *Kofler/Wurm* in *Doralt/Kirchmayr/Mayr/Zorn*, EStG (20. Lfg, 2018) § 20 Tz 163; Jakom/*Marschner*, EStG[14] (2021) § 4 Rz 330; *Wunderlich*, DStR 1996, 2003 (2004 f), der weiters für eine generelle Abzugsfähigkeit bei besonderer Gefährdungslage im Ausland eintritt.

5) Rz 1523 EStR.

Steuerlich ist daher im Ansatz zu unterscheiden, ob eine Erpressung und die darauf basierende Lösegeldzahlung die private oder die betriebliche Sphäre des Steuerpflichtigen betreffen, zumal von vornherein nur eine betriebliche Veranlassung zum Betriebsausgabenabzug nach § 4 EStG berechtigt. Wenn es sich – wie für Ransomware-Angriffe typisch[6]) – um ein infiziertes Computersystem eines Unternehmens handelt, wird uE an einer vollständigen betrieblichen Zuordnung nachweislich geleisteter Lösegeldzahlungen nicht gezweifelt werden können.[7]) Dies ist wohl mit der in den EStR als Beispiel für abzugsfähige Erpressungszahlungen genannten Situation der Drohung mit Beschädigung oder Zerstörung von Wirtschaftsgütern[8]) vergleichbar, werden doch das betroffene IT-System oder zumindest immaterielle Güter (Datenbestände) durch die Verschlüsselung unbrauchbar gemacht. Die grundsätzliche Eigenschaft der Lösegeldzahlung als Betriebsausgabe geht auch nicht dadurch verloren, dass das Unternehmen womöglich anders Abhilfe hätte schaffen können (Ersatzbeschaffungen, Rückgriff auf Sicherungen usw). Die Angemessenheit, Wirtschaftlichkeit, Zweckmäßigkeit und Notwendigkeit einer Ausgabe sind für deren Eigenschaft als Betriebsausgabe bei entsprechender betrieblicher Veranlassung schließlich irrelevant.[9])

Problematisch könnte sich allenfalls eine Zahlung für ein gemischt genutztes Computersystem (zB bei mobilen Geräten oder Computern in der Wohnung des Steuerpflichtigen) mit betrieblichen und privaten Daten erweisen. Da Computer und deren Zubehör nach der Judikatur des VwGH jedoch nicht dem sogenannten Aufteilungsverbot nach § 20 Abs 1 Z 2 lit a EStG unterliegen,[10]) ist die Lösegeldzahlung auch in derartigen Konstellationen zumindest im (notwendigenfalls zu schätzenden) Ausmaß der betrieblichen Veranlassung als Betriebsausgabe anzuerkennen.[11])

Bei festgestellter betrieblicher Veranlassung und damit grundsätzlicher Eigenschaft als Betriebsausgabe ist in weiterer Folge zu fragen, ob die Zahlung einem steuerlichen Abzugsverbot unterliegt. In den hier zu untersuchenden Fällen ist dabei insbesondere an zwei Abzugsverbote – § 20 Abs 1 Z 5 lit a EStG und § 162 BAO – zu denken, welche im Folgenden näher geprüft werden.

2. Abzugsverbot nach § 20 Abs 1 Z 5 lit a EStG?

2.1. Anwendungsvoraussetzungen

Nach § 20 Abs 1 Z 5 lit a EStG (bzw gleichlautend § 12 Abs 1 Z 4 lit a KStG) ist eine steuerliche Geltendmachung als Betriebsausgaben (oder Werbungskosten) unzulässig für *„Geld und Sachzuwendungen, deren Gewährung oder Annahme mit gerichtlicher*

---

[6]) In der Tat zeigen auch die Erfahrungen aus der Praxis, dass sich Ransomware-Angriffe offenbar vorwiegend gegen kleine und mittlere Unternehmen und weniger gegen Einzelpersonen richten, also – nicht zuletzt aufgrund einer *„zielgerichtete[n] Spezialisierung auf Unternehmen“* – ein Risikopotenzial für die österreichische Unternehmenslandschaft darstellen. Siehe *Bundeskriminalamt*, Cybercrime Report 2020, 15.

[7]) Ebenso *Heine*/*Trinks*, Steuerliche Folgen einer Erpressung für Täter und Opfer, NWB 2016, 2109 (2114 f), auch mit weiteren Überlegungen zu der Situation, dass sowohl betriebliche als auch berufliche Daten betroffen sind; *Wackerbeck*, Anwendbarkeit des § 160 AO bei Cyber-Erpressungen? NWB 2021, 1790 (1790).

[8]) Siehe wiederum Rz 1523 EStR.

[9]) Siehe zB Rz 1086 EStR mwN aus der Judikatur.

[10]) Siehe zB VwGH 27. 1. 2011, 2010/15/0197; dazu etwa *Kofler*/*Wurm* in *Doralt*/*Kirchmayr*/*Mayr*/*Zorn*, EStG (20. Lfg, 2018) § 20 Tz 22/1; Rz 1512 EStR.

[11]) Eine Berücksichtigung von privat veranlassten Lösegeldzahlungen als außergewöhnliche Belastung im Rahmen des § 34 EStG scheint aber nicht ausgeschlossen (siehe *Quantschnigg*/*Schuch*, Einkommensteuer-Handbuch [1993] § 34 Tz 38; *Fuchs*/*Unger* in *Hofstätter*/*Reichel*, Die Einkommensteuer [54. Lfg, 2013] § 34 Anh II Tz 37), wobei allerdings zudem zu berücksichtigen wäre, dass die im Folgenden dargestellten Abzugsverbote auch für außergewöhnliche Belastungen gelten (dazu § 20 Abs 3 EStG und Rz 837 LStR; aus dem Blickwinkel des § 20 Abs 1 Z 5 lit a iVm Abs 3 EStG daher eine Abzugsfähigkeit im Ergebnis verneinend *Fuchs* in *Doralt*/*Kirchmayr*/*Mayr*/*Zorn*, EStG [21. Lfg, 2020] § 34 Tz 78).

Strafe bedroht ist". Sollte diese Bestimmung auf Lösegeldzahlungen in Ransomware-Konstellationen zur Anwendung gelangen, wären diese trotz nachgewiesener betrieblicher Veranlassung steuerlich nicht abzugsfähig.

Auslöser für das Abzugsverbot sind nur gerichtlich strafbare Taten, nicht aber jene mit bloßer Verwaltungsstrafdrohung.[12]) Erfasst sind jedoch die Gewährung und Annahme, sodass für das Abzugsverbot nicht maßgeblich ist, ob das Verhalten des Zahlers oder aber auch nur jenes des Zahlungsempfängers der Strafbarkeit unterliegt.[13]) Der Täter muss auch nicht tatsächlich bestraft werden.[14]) Allerdings sind für das Abzugsverbot sämtliche Voraussetzungen einer Strafbarkeit (insbesondere auch die subjektive Tatseite oder Rechtfertigungsgründe) zu beachten, zumal ein nicht bloß wegen Verfolgungshindernissen (zB Verjährung) gefällter Freispruch in einem späteren tatsächlichen Verfahren die Abzugsfähigkeit wiederherstellen würde.[15]) Weiters sind vom Abzugsverbot des § 20 Abs 1 Z 5 lit a EStG nach Verwaltungspraxis[16]) und herrschender Ansicht im Schrifttum[17]) nur österreichische strafgesetzliche Bestimmungen erfasst, also Taten, die im Inland gerichtlich strafbar sind. Die dafür erforderliche Anknüpfung ergibt sich wiederum aus den §§ 62 ff StGB, wonach das österreichische Strafrecht für *„Taten, die im Inland begangen worden sind"*, gilt. Nach § 67 Abs 2 StGB gelten als Tatort sowohl der Handlungsort des Täters als auch der Erfolgsort der Tat gleichermaßen.

2.2. Anwendung wegen strafbarer Erpressung (§§ 142 f StGB)?

Die strafrechtliche Beurteilung der Ransomware-Kriminalität ist durchaus komplex. Im Wesentlichen wird hier zwischen der Infizierung des Computersystems und Verschlüsselung einerseits und der Geldforderung im Gegenzug zur Entsperrung andererseits zu unterscheiden sein. Ersteres wird als Datenbeschädigung (§ 126a StGB),[18]) Zweites von der – nicht unumstrittenen – herrschenden Ansicht und Rechtsprechung[19]) als echt

[12]) Siehe zB Rz 4840 EStR.

[13]) Siehe zB *Lachmayer* in *Renner/Strimitzer/Vock*, KStG (31. Lfg, 2018) § 12 Tz 53; *Achatz/Bieber* in *Achatz/Kirchmayr*, KStG (2011) § 12 Tz 82; *Althuber* in *Hofstätter/Reichel*, EStG (61. Lfg, 2016) § 20 Tz 12; *Kofler/Wurm* in *Doralt/Kirchmayr/Mayr/Zorn*, EStG (20. Lfg, 2018) § 20 Tz 130.

[14]) Siehe zB Rz 4846 EStR.

[15]) Siehe *Lachmayer* in *Renner/Strimitzer/Vock*, KStG (31. Lfg, 2018) § 12 Tz 49; *Kofler/Wurm* in *Doralt/Kirchmayr/Mayr/Zorn*, EStG (20. Lfg, 2018) § 20 Tz 132 f.

[16]) Rz 4840 EStR; ebenso bereits AÖF 1999/162.

[17]) Siehe zB *Quantschnigg/Schuch*, ESt-HB, § 20 Tz 34; *Kofler/Wurm* in *Doralt/Kirchmayr/Mayr/Zorn*, EStG (20. Lfg, 2018) § 20 Tz 127; *Achatz/Bieber* in *Achatz/Kirchmayr*, KStG, § 12 Tz 80; zweifelnd *Lachmayer* in *Renner/Strimitzer/Vock*, KStG (31. Lfg, 2018) § 12 Tz 54. Die Gegenauffassung leitet demgegenüber aus dem Zweck des § 20 Abs 1 Z 5 lit a EStG ab, dass das Abzugsverbot auch greift, wenn eine Handlung in Österreich nur mangels eines Anknüpfungspunkts an das Inland, dafür aber im Ausland strafbar ist (*Althuber* in *Hofstätter/Reichel*, EStG [61. Lfg, 2016] § 20 Tz 12; dazu auch *Huber*, Das neue Korruptionsstrafrecht aus Sicht des steuerlichen Abzugsverbots, SWK 10/2013, 525 [527]; siehe aus verfassungsrechtlichen Erwägungen auch *Walter*, Abzugsverbot von Schmiergeldern: Lücke und Gleichheitswidrigkeit, RdW 1999, 749 [749]).

[18]) Siehe nur *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht (2018) Rz 2.239.

[19]) Siehe mwN etwa *Reindl-Krauskopf*, Cyberstrafrecht im Wandel, ÖJZ 2015, 112 (112 f); *Reindl-Krauskopf*, Cyber Crime – Der digitalisierte Täter, ALJ 2017, 110 (115); *Reindl-Krauskopf/Salimi/Stricker*, IT-Strafrecht, Rz 2.148 und 2.240. Aus strafrechtlicher Sicht ist – ähnlich wie bei der *„Kunsterpressung"* (zB *„Raub der Saliera"*) – allerdings umstritten, ob für die Beurteilung des Schadens und damit das Vorliegen einer Erpressung eine Anrechenbarkeit der Sachrückgabe auf die abgenötigte Leistung zu erfolgen hat (siehe dazu weiters *Eder-Rieder* in *Höpfel/Ratz*, WK StGB[2] [2016] § 144 Rz 27 mwN): Die Rechtsprechung bejaht für Fälle der *„Kunsterpressung"* das Vorliegen von Erpressung nach § 144 StGB auf Basis des zivilrechtlichen Eigentumsbegriffs, zumal das Opfer das Eigentum an der gestohlenen Sache nicht verloren habe und damit der Forderung von Geld für deren Herausgabe keine entsprechende Gegenleistung des Täters gegenübersteht (OGH 6. 3. 2007, 11 Os 3/07m, JBl 2008, 198 [*Schmoller*]; siehe auch OGH 17. 8. 2010, 11 Os 54/10s). Die Gegenauffassung sieht hingegen den Vermögensschaden schon durch den vorangegangenen Diebstahl als eingetreten, sodass bei Rückgabe der Sache gegen Geld kein zusätzlicher Schaden entstehe, wenn das Lösegeld unter deren Wert liegt (so etwa *Flora* in *Leukauf/Steininger*, StGB [2020] § 144 Rz 9). Diese Meinungsdivergenz spiegelt sich auch bei der strafrechtlichen Diskussion von Ransomware wider (dazu ausführlich *Kahl/Stücklberger*, Strafrechtliche Implikationen des „WannaCry"-Angriffes, JSt 2018, 30 [31 ff]).

konkurrierende[20]) und daher zusätzlich strafbare Erpressung (§ 144 StGB) beurteilt. Der tatbestandliche Vermögensschaden der Erpressung tritt beim geschädigten Opfer, das die vermögensverschiebende Verfügung vornimmt, bei Ransomware-Angriffen also dem betroffenen Unternehmen in Österreich, ein. Damit liegt nach § 67 Abs 2 StGB ein nach österreichischem Recht strafbares Delikt vor.[21]) Wird die Geldforderung durch den Ransomware-Täter als Erpressung beurteilt, stellt sich daher die Folgefrage, ob damit eine Geldzuwendung, deren Annahme mit gerichtlicher Strafe bedroht ist, iSd Abzugsverbots nach § 20 Abs 1 Z 5 lit a EStG vorliegt.

Historische Stoßrichtung dieses konstitutiven[22]) Abzugsverbots ist die Korruptionsbekämpfung, also insbesondere der Bereich der Schmier- bzw Bestechungsgelder.[23]) Allerdings ist umstritten, welche Straftatbestände tatsächlich betroffen sind. Seinem Wortlaut nach erfasst das Abzugsverbot zumindest jedes Delikt, bei dem die Zuwendung oder Annahme von Geld- oder Sachzuwendungen ausdrücklich Tatbestandselement der strafbaren Tat ist (zB bei der Bestechung nach § 307 StGB die Gewährung des Vermögensvorteils). Bei der Erpressung ist allerdings unklar, ob die Lösegeldzahlung selbst überhaupt (zumindest mittelbar) ein Tatbestandselement darstellt, weil in § 144 StGB nur der Vermögensschaden (*„einen anderen am Vermögen schädigt“*) als Teil des Tatbilds definiert ist, nicht aber die Gewährung oder Annahme der Zahlung als solche. Teile des älteren Schrifttums[24]) wie auch die Finanzverwaltung[25]) zählen Erpressung (§§ 144, 145 StGB) daher nicht zu jenen Tatbeständen, die vom Abzugsverbot betroffen sind. Das erscheint insofern stimmig, als umgekehrt die Subsumtion unter das Abzugsverbot wesentlich auf dem Element des Vermögensschadens beruht.[26]) Dieses Tatbestandselement würde sich aber etwa auch beim Betrug (§ 146 StGB) oder der Untreue (§ 153 StGB) finden, ohne dass bisher – soweit ersichtlich – die Abzugsfähigkeit beim Opfer in Frage gestellt worden wäre.[27])

Im jüngeren Schrifttum wird jedoch überwiegend[28]) und in der (nicht höchstgerichtlichen) Rechtsprechung zumindest einmal[29]) § 20 Abs 1 Z 5 lit a EStG weiter aufgefasst und dementsprechend dennoch davon ausgegangen, dass auch Lösegeld- und Schutzgeldzahlungen aufgrund einer Erpressung (oder etwa auch Geldzahlungen für die Bestimmung zu Straftaten) dem Grunde nach vom Abzugsverbot betroffen sind. Im Falle von Erpressungsopfern wird diese zunächst weite Auslegung im Schrifttum aber wieder eingeschränkt: Selbst wenn die Voraussetzungen des Abzugsverbots nach § 20 Abs 1 Z 5 lit a EStG *prima facie* erfüllt seien, wäre die Rechtsfolge eines Abzugsverbots oftmals unbefriedigend und auch vom Normzweck nicht gefordert. § 20 Abs 1 Z 5 lit a EStG möchte Zahlungen pönalisieren, mit denen sich der Zahler einen unrechten Vorteil verschafft, nicht aber Fälle, in denen das ehrliche Opfer etwa seinen Betrieb, seine Wirtschaftsgüter oder Betriebsgeheimnisse schützen möchte. Es scheint daher nahezu unstrittig, dass der Tatbestand des § 20 Abs 1 Z 5 lit a EStG in diesen Fällen teleologisch zu reduzieren ist,

[20]) Dazu etwa *Kahl*/*Stücklberger*, JSt 2018, 30 (33 f mwN).
[21]) Siehe zum Betrug etwa OGH 21. 10. 1987, 14 Os 122/87; 20. 12. 2011, 15 Os 106/11v; dazu auch *Salimi* in *Höpfel*/*Ratz*, WK StGB[2], § 67 Rz 30.
[22]) Siehe zum konstitutiven Charakter auch VwGH 7. 7. 2004, 2000/13/0173 (zu Schmiergeldzahlungen eines Vermittlers).
[23]) Dazu mwN etwa *Bieber*/*Kofler*, Korruptionstatbestände im Ertragsteuerrecht, Zak 2009, 187 (188).
[24]) Siehe zB *Quantschnigg*/*Schuch*, ESt-HB, § 20 Rz 35.
[25]) Siehe Rz 4843 EStR sowie wiederum Rz 1523 EStR.
[26]) Siehe auch *Kofler*/*Wurm* in *Doralt*/*Kirchmayr*/*Mayr*/*Zorn*, EStG (20. Lfg, 2018) § 20 Tz 128; *Heber*, Schmier-, Bestechungs- und Schutzgelder im Ertragsteuerrecht, ÖStZ 2010, 405 (407).
[27]) Vgl zB Rz 1689 EStR.
[28]) Siehe zB *Heber*, ÖStZ 2010, 405 (407 f); *Althuber* in *Hofstätter*/*Reichel*, EStG (61. Lfg, 2016) § 20 Tz 12; *Krafft* in *Wiesner*/*Grabner*/*Knechtl*/*Wanke*, EStG (26. Lfg, 2018) § 20 Anm 79 und 82; *Kofler*/*Wurm* in *Doralt*/*Kirchmayr*/*Mayr*/*Zorn*, EStG (20. Lfg, 2018) § 20 Tz 129; Jakom/*Peyerl*, EStG[14], § 20 Rz 86. Offen gelassen bei *Lachmayer* in *Renner*/*Strimitzer*/*Vock*, KStG (31. Lfg, 2018) § 12 Tz 53. Anderer Ansicht aber zB *Huber*, SWK 10/2013, 525 (527), und *Leitner*/*Brandl*/*Kert*, Handbuch Finanzstrafrecht[4] (2017) Rz 1596.
[29]) UFS 14. 3. 2008, RV/0639-W/08.

um die Lösegeldzahlungen des Opfers nicht unsachlich vom Abzug auszuschließen.[30]) Diese Ansicht deckt sich im Ergebnis mit der zuvor wiedergegebenen Verwaltungsmeinung: Die EStR zum Abzugsverbot des § 20 Abs 1 Z 5 lit a EStG erwähnen den Tatbestand der Erpressung nach §§ 144, 145 StGB nicht[31]) und sprechen an anderer Stelle sogar davon, dass Zahlungen von Erpressungsopfern bei betrieblicher Veranlassung als abzugsfähig anzusehen sind.[32])

In Erpressungssituationen führen somit beide Sichtweisen – Nichteinbeziehung in das Abzugsverbot oder aber zunächst Einbeziehung und anschließende abwägende teleologische Reduktion unter Beachtung des schutzwürdigen Opfers – zum selben Ergebnis. Das Abzugsverbot nach § 20 Abs 1 Z 5 lit a EStG kommt beim erpressten Lösegeldzahler nicht zur Anwendung. Diesem Zwischenergebnis steht uE auch die – vereinzelt gebliebene – Rechtsprechung nicht entgegen: So berief sich der (seinerzeitige) Unabhängige Finanzsenat (UFS) bei der Weitergabe von unterschlagenen Geldern an einen (angeblichen) Mitwisser zwar auf den im Raum stehenden Vorwurf der Erpressung (§ 144 StGB) und leitete daraus (ohne nähere Begründung) eine Anwendung des § 20 Abs 1 Z 5 lit a EStG ab. Eine nähere Auseinandersetzung mit der angesprochenen Frage fand aber nicht statt. Zudem wird auch deutlich, dass die gegenständliche Geldzahlung für den UFS ihre Ursache entweder im schuldhaften Verhalten des Betriebsinhabers als Täter hatte oder überhaupt den nichtabzugsfähigen Aufwendungen für die Lebensführung zuzuordnen war. Insgesamt war dieser Fall daher so gelagert, dass für das Erpressungsopfer eine teleologische Reduktion des § 20 Abs 1 Z 5 lit a EStG mangels Schutzwürdigkeit nicht angezeigt war, zumal der Erpressungsgrund in einer vorangegangenen strafbaren Handlung des Erpressten lag.[33])

2.3. Anwendung wegen Beteiligung an einer kriminellen Vereinigung (§ 278 StGB)?

Aus der Perspektive der *„digitalen Erpressung“* wird einem Ransomware-Opfer im betrieblichen Bereich die Abzugsfähigkeit der Lösegeldzahlung nach § 20 Abs 1 Z 5 lit a EStG nicht zu versagen sein. Allerdings tritt durch die noch in Diskussion befindliche strafrechtliche Beurteilung von Ransomware-Fällen womöglich eine zusätzliche Dimension hinzu. Steht hinter dem Angriff eine kriminelle Vereinigung von zumindest drei Personen,[34]) ist nicht ausgeschlossen, dass die Lösegeldzahlung als Bereitstellung von Vermögenswerten und damit als Beteiligung an dieser Vereinigung nach § 278 Abs 3 Fall 3 StGB zu beurteilen ist.[35]) Folglich erfüllte das Opfer selbst den Straftatbestand nach Abs 1 leg cit zumindest hinsichtlich der objektiven Tatseite.[36]) Im Rahmen

[30]) Siehe zB *Heber*, ÖStZ 2010, 405 (407 f); *Althuber* in *Hofstätter/Reichel*, EStG (61. Lfg, 2016) § 20 Tz 12; *Lachmayer* in *Renner/Strimitzer/Vock*, KStG (31. Lfg, 2018) § 12 Tz 53; *Kofler/Wurm* in *Doralt/Kirchmayr/Mayr/Zorn*, EStG (20. Lfg, 2018) § 20 Tz 129 mwN; wohl auch Jakom/*Peyerl*, EStG[14], § 20 Rz 86; anderer Ansicht womöglich *Krafft* in *Wiesner/Grabner/Knechtl/Wanke*, EStG (26. Lfg, 2018) § 20 Anm 79.

[31]) Siehe Rz 4843 EStR.

[32]) Rz 1523 EStR.

[33]) Ebenso auch *Heber*, ÖStZ 2010, 405 (407 f).

[34]) § 278 Abs 2 StGB definiert eine kriminelle Vereinigung als einen auf längere Zeit angelegten Zusammenschluss von mehr als zwei Personen, der darauf ausgerichtet ist, dass von einem oder mehreren Mitgliedern der Vereinigung ua ein oder mehrere *„Verbrechen“* ausgeführt werden. Die in § 278 Abs 2 StGB erwähnten Verbrechen iSd § 17 Abs 1 StGB erfassen alle vorsätzlichen (strafbaren) Handlungen, die mit lebenslanger oder mit mehr als dreijähriger Freiheitsstrafe bedroht sind, also auch die Erpressung (§§ 144 f StGB) (dazu *Plöchl* in *Höpfel/Ratz*, WK StGB[2], § 278 Rz 20).

[35]) Bei Erfüllung der organisatorischen Voraussetzungen aufseiten des Empfängers der Lösegeldzahlung kommen auch die Strafbarkeiten nach §§ 278a und 278b StGB in Betracht, da diese auf die Tathandlungen in § 278 Abs 3 StGB verweisen.

[36]) Dazu ausführlich *Kahl/Stücklberger*, JSt 2018, 30 (33 f mwN). Siehe in diese Richtung auch zum deutschen Strafrecht *Salomon*, Cybercrime und Lösegeld – Strafbarkeit der Zahlung von Lösegeld als Reaktion auf Erpressungstrojaner, MMR 2016, 575 (575 ff), wonach eine Zahlung als Reaktion auf Erpressung im Cyberraum durchaus strafrechtliche Konsequenzen haben kann, auch wenn Strafverfolgungsbehörden derzeit in solchen Fällen noch keine Ermittlungen aufzunehmen scheinen. Auch

der Beteiligung an einer kriminellen Vereinigung nach § 278 StGB wäre das angegriffene Unternehmen damit selbst als Täter anzusehen; die tatbestandliche Vermögenszuwendung geht auch vom Inland aus und bildet damit eine nach § 67 Abs 2 StGB dem österreichischen Strafrecht unterliegende Tathandlung.[37])

Wenngleich die EStR dieses Delikt (und verwandte Delikte) noch nicht als Anwendungsfall des Abzugsverbots nennen,[38]) greifen die im steuerlichen Schrifttum entwickelten Argumente, dieses auf bestimmte Straftatbestände bzw den Täter zu beschränken – anders als im zuvor dargestellten Bereich der Erpressung – nicht. Da § 278 Abs 3 Fall 3 StGB ausdrücklich die Vermögenszuwendung als Tatbestandselement erfasst und der Erpresste hier nicht Opfer, sondern durch die materielle Förderung der kriminellen Vereinigung gleichsam Täter *„gegen den öffentlichen Frieden“*[39]) ist, scheint eine Nichtanwendung bzw teleologische Einschränkung des steuerlichen Abzugsverbots nach § 20 Abs 1 Z 5 lit a EStG bei diesem Delikt nicht geboten. Entscheidend für die steuerliche Beurteilung wird daher sein, ob tatsächlich eine Strafbarkeit nach § 278 StGB verwirklicht wird.

Im Rahmen einer steuerlichen Betrachtung kann diese dem Strafrecht zugehörige Frage nicht abschließend beantwortet werden. Allerdings scheinen in der laufenden Diskussion mehrere Anhaltspunkte dahingehend zu existieren, dass bei typischen Ransomware-Angriffen gegenwärtig nicht mit einer generellen Strafbarkeit der Lösegeldzahlungen und damit einer Anwendung des Abzugsverbots nach § 20 Abs 1 Z 5 lit a EStG zu rechnen ist. Erstens existiert im strafrechtlichen Schrifttum die Ansicht, § 278 StGB dahingehend teleologisch zu reduzieren, dass die *„Mitgliedschaft“* in der kriminellen Vereinigung eine über die konkrete Tathandlung hinausgehende Voraussetzung der Strafbarkeit sei, sodass eine bloß abgenötigte Zahlung den Tatbestand nicht erfülle (wenngleich die Rechtsprechung in die Gegenrichtung zu tendieren scheint).[40])

Zweitens fordert § 278 Abs 3 StGB auf subjektiver Tatseite bei der Beteiligung an einer kriminellen Vereinigung durch Bereitstellung von Informationen oder Vermögenswerten die Vorsatzform der Wissentlichkeit hinsichtlich der Vereinigung oder deren strafbarer Handlungen.[41]) Mit den Worten von § 5 Abs 3 StGB müsste der Lösegeldzahler die Förderung der kriminellen Vereinigung oder deren Taten also nicht bloß für möglich, sondern für gewiss halten. Da Ransomware-Angriffe typischerweise von gänzlich anonymen Tätern nur über digitalen Kontakt durchgeführt werden, wird das Opfer über die Anzahl der Täter und die weitere Verwendung der erpressten Gelder aber allenfalls mutmaßen können. Der gesetzlich geforderte subjektive Tatbestand des § 278 StGB wird daher wohl nicht erfüllt sein.[42])

Drittens ist zu bedenken, dass selbst bei Erfüllung des objektiven und subjektiven Tatbestands noch mögliche Rechtfertigungs- und Entschuldigungsgründe zu prüfen sind. Hier kommt vor allem der entschuldigende Notstand nach § 10 StGB in Betracht.[43]) Dabei ist im Wesentlichen abzuwägen, ob der durch die Zahlung bewirkte Eingriff in den

Plöchl in *Höpfel/Ratz*, WK StGB², § 278 Rz 38, zählt etwa erpresste Schutzgeldzahler zu den vom Tatbestand erfassten Personen.

37) Vgl *Salimi* in *Höpfel/Ratz*, WK StGB², § 67 Rz 80. Unter Umständen kommt bei Delikten aus dieser Gruppe auch eine Bestrafung von im Ausland begangenen Handlungen unter den Voraussetzungen des § 64 Abs 1 Z 9 StGB in Betracht.

38) Rz 4843 EStR.

39) So die Überschrift zum 20. Abschnitt des StGB.

40) Siehe die Analyse und Nachweise bei *Kahl/Stücklberger*, JSt 2018, 30 (35 f).

41) RIS-Justiz RS0124903; siehe auch *Plöchl* in *Höpfel/Ratz*, WK StGB², § 278 Rz 43.

42) Auch bei *Plöchl* in *Höpfel/Ratz*, WK StGB², § 278 Rz 38, wird bei der Diskussion der möglichen Strafbarkeit etwa davon gesprochen, dass erpresste Schutzgeldzahler zumeist Kenntnis von der dahinter stehenden Organisation bzw deren sonstigen Taten haben werden. Dies kann im Falle von Ransomware-Angriffen wohl kaum vertreten werden.

43) Siehe *Plöchl* in *Höpfel/Ratz*, WK StGB², § 278 Rz 38.

öffentlichen Frieden (durch Förderung der kriminellen Vereinigung) nicht unverhältnismäßig schwerer wiegt als der Schaden, der dem vom Ransomware-Angriff betroffenen Unternehmen droht, und ob auch ein mit den rechtlich geschützten Werten verbundener Mensch als Maßstabsfigur kein anderes Verhalten gesetzt hätte. Insbesondere die Schwere des Angriffs, die Bedeutung der verschlüsselten Daten bzw nicht nutzbaren Infrastruktur, die Dringlichkeit der Wiederherstellung der Betriebsfähigkeit und die Tauglichkeit alternativer Pläne (zB Rückgriff auf Sicherungen) werden hierbei zu berücksichtigen sein. In vielen Fällen wird die Abwägung zugunsten des betroffenen Unternehmens ausfallen und eine Strafbarkeit daher mangels Schuld ausscheiden; letztlich ist aber entscheidend, welche Handlungen von der erwähnten Maßstabsfigur zu erwarten gewesen wären.[44])

Zusammenfassend besteht daher ein gewisses Risiko, dass die Lösegeldzahlung des Ransomware-Opfers den Straftatbestand des § 278 Abs 1 iVm Abs 3 Fall 3 StGB verwirklicht, da zumindest die objektive Tatseite nach dem Wortlaut dieser Bestimmung vielfach (bei entsprechender Personenmehrheit und weiteren verbotenen Handlungen auf Täterseite) erfüllt sein könnte. Die strafrechtliche Diskussion dahingehend ist aber noch nicht abgeschlossen; endgültige Klarheit wird wohl erst durch Judikatur zu dieser Frage herrschen. Von dieser Beurteilung hängt letztlich auch die steuerliche Abzugsfähigkeit ab. Allerdings scheint die erwähnte Strafbarkeit nach derzeitigem Wissensstand bei typischen (anonymen) Ransomware-Angriffen regelmäßig mangels Kenntnis der Organisation oder sonstigen Delikte auf Täterseite oder kraft entschuldigenden Notstands nach § 10 StGB (bei entsprechender Abwägung der Umstände des Einzelfalls) auszuscheiden. Daher ist aktuell nicht davon auszugehen, dass der Straftatbestand des § 278 Abs 1 iVm Abs 3 Fall 3 StGB im Regelfall einer Abzugsfähigkeit der Zahlung bei betrieblicher Veranlassung auf Grundlage des § 20 Abs 1 Z 5 lit a EStG im Wege stehen wird. Soweit ersichtlich wurde eine derartige Einschränkung der Abzugsfähigkeit auch im steuerlichen Schrifttum bislang noch nicht vertreten.

3. Abzugsverbot nach § 162 BAO mangels Empfängerbenennung?

Einer Abzugsfähigkeit des Lösegeldes bei digitalen Erpressungen könnte weiters der Empfängerbenennungstatbestand des § 162 BAO („*Schmiergeldparagraf*“[45])) entgegenstehen. § 162 Abs 1 BAO bestimmt, dass die Abgabenbehörde verlangen kann (Ermessen nach § 20 BAO[46])), *„daß der Abgabepflichtige die Gläubiger oder die Empfänger der abgesetzten Beträge genau bezeichnet“*. Bei Verweigerung der verlangten Angaben *„sind“* (zwingend) die beantragten Absetzungen nicht anzuerkennen (§ 162 Abs 2 BAO);[47]) sie sind auch nicht etwa im Schätzungsweg zu berücksichtigen.[48])

§ 162 BAO greift auch dann, wenn die Finanzverwaltung die geltend gemachten Abzugsposten dem Grunde nach nicht bezweifelt, sondern in freier Beweiswürdigung als zweifelsfrei erwiesen sieht.[49]) Zudem stellt die Rechtsprechung durchaus hohe Anforderungen an die Empfängerbenennung.[50]) So fordere diese Bestimmung *„die exakte*

[44]) Siehe *Kahl/Stücklberger*, JSt 2018, 30 (37 f mwN).
[45]) *Tanzer* in *Althuber/Tanzer/Unger*, BAO-Handbuch (2015) 460 f.
[46]) Dazu nur *Ritz*, BAO[6] (2017) § 162 Tz 2 mwN.
[47]) Rz 1115 EStR.
[48]) Siehe etwa VwGH 31. 1. 2001, 98/13/0156; 25. 4. 2013, 2013/15/0155; Rz 1110 EStR; siehe auch *Ritz*, BAO[6], § 162 Tz 3 mwN.
[49]) Dazu etwa VwGH 28. 5. 1997, 94/13/0230; 28. 10. 1997, 93/14/0073, 0099; 30. 9. 1998, 96/13/0017; ebenso Rz 1115 EStR.
[50]) Nach der Rechtsprechung kann etwa die Nennung bloß des Familiennamens (VwGH 25. 11. 1992, 89/13/0043), einer falschen (VwGH 30. 9. 1998, 96/13/0017) oder beliebigen Person (VwGH 17. 11. 1982, 81/13/0194, 82/13/0036, 0037), einer Firma in einer Steueroase (VwGH 13. 11. 1985, 84/13/0127) oder einer Briefkastengesellschaft (VwGH 11. 7. 1995, 91/13/0154, 0186; 28. 11. 2000, 97/14/0062), ohne die an diesen tatsächlich Beteiligten bekanntzugeben, die zwingende Versagung der Anerkennung

Empfängerbenennung in dem Sinne, dass es der zuständigen Abgabebehörde möglich gemacht wird, dass die Beträge beim Empfänger versteuert werden können".[51]) § 162 BAO stellt dabei nach herrschender Ansicht als *„formale Beweisregel"* eine Ausnahme vom Grundsatz der freien Beweiswürdigung dar.[52]) Insoweit geht § 162 BAO in der Praxis weit über jene Fälle hinaus, bei denen weder die Abzugsfähigkeit noch die Nichtabzugsfähigkeit mit letzter Gewissheit feststehen. Die von § 162 BAO intendierte Sicherung der Besteuerung beim Empfänger[53]) steht damit auch in einem gewissen Spannungsverhältnis zur tatsächlichen Berücksichtigung der materiellen Wahrheit,[54]) wird sie doch bei überbordender Handhabung zu einer *„Strafmaßnahme"*, mit der *„anstelle der Ermittlung der materiellen Wahrheit und im bewussten Gegensatz zu dieser dem – an sich ‚falschen' – Pflichtigen im abgekürzten Weg ein Steuernachteil angedroht und gegebenenfalls auch zugefügt wird"*.[55]) § 162 BAO und insbesondere die diesbezügliche Ermessensübung unterliegen allerdings Schranken. Benennungsverlangen dürfen insbesondere nicht offenbar unerfüllbar sein.[56])

Bei der typischen digitalen Erpressung mit Ransomware wird das Opfer naturgemäß den oder die Täter nicht benennen können, zielt doch die zunehmende technische Professionalisierung und die Lösegeldabwicklung über eine Kryptowährung gerade auf deren Anonymität ab. In der deutschen Diskussion zur Parallelnorm des § 160 dAO wird im Schrifttum durchaus die (strenge) Ansicht vertreten, dass die Finanzverwaltung auch in einer solchen Situation eine Empfängerbenennung rechtmäßig begehren und die Abzugsfähigkeit versagen darf, zumal die von der Rechtsprechung entwickelten Kriterien einer Unzumutbarkeit nicht erfüllt seien.[57]) Der Staat bzw die Allgemeinheit müsse sich *„an der wirtschaftlichen Entscheidung des Erpressten"*, wie er mit der Gefahr von Cyberattacken umgeht (also etwa durch Lösegeldzahlung), *„nicht mit einem Verzicht auf Steuereinnahmen beteiligen"*.[58])

An einem solch strengen Verständnis der Verhältnismäßigkeit darf freilich gezweifelt werden, zumal die deutsche Rechtsprechung die Ermessensfehlerhaftigkeit eines Benennungsverlangens zB bei Täuschungen über die Identität des Geschäftspartners,[59]) bei Lösegeldforderungen mit Morddrohung[60]) oder der Bedrohung der wirtschaftlichen Existenz des Steuerpflichtigen[61]) durchaus anerkannt hat. Es wird nicht verkannt, dass sich diese Fälle von jenen der digitalen Erpressung durchaus in wesentlichen Punkten unterscheiden, wird hier doch weder über die Identität der (ohnedies anonym agierenden) Täter getäuscht noch geht es um Leib und Leben, sondern lediglich um betriebliche Daten.[62]) Allerdings erscheint die Ransomware-Erpressung auch im Hinblick auf die Unzumutbarkeitsgrenze des § 160 dAO als Grenzfall, und die deutsche Rechtsprechung hatte sich – soweit ersichtlich – mit dieser Frage noch nicht explizit zu befassen.

---

nicht verhindern (siehe auch Rz 1116 EStR). Ebenso wenig stellt die Namhaftmachung einer nicht existenten GmbH bzw deren nicht ausforschbarer Kontaktperson eine hinreichende Empfängerbenennung dar (VwGH 8. 6. 1988, 84/13/0069).

[51]) So BFG 18. 6. 2018, RV/7103208/2013.

[52]) Siehe nur *Ritz*, BAO[6], § 162 Tz 12 mwN.

[53]) So zB VwGH 2. 3. 1993, 91/14/0144; 28. 5. 1997, 94/13/0230; Rz 1110 EStR.

[54]) Kritisch daher zB *Holzinger*, Empfängerbenennung als überragendes Prinzip des Steuerrechts? SWK 32/2013, 1413 (1413 ff), und *Balas/Kotschnigg*, Verfassungsrechtliche Bedenken gegen § 162 BAO, SWK 3/2017, 160 (160 ff); siehe dazu auch *Ritz*, BAO[6], § 162 Tz 5.

[55]) *Tanzer* in *Althuber/Tanzer/Unger*, BAO-HB, 461 f.

[56]) Siehe etwa VwGH 31. 1. 2001, 98/13/0156; 25. 4. 2013, 2013/15/0155.

[57]) So ausführlich *Wackerbeck*, NWB 2021, 1790 (1790 ff); wohl auch *Heine/Trinks*, NWB 2016, 2109 (2115).

[58]) So *Wackerbeck*, NWB 2021, 1790 (1794), mit dem Hinweis, dass auch Presseunternehmen trotz des bestehenden Auskunftsverweigerungsrechts für Zahlungen an Informanten etc ausdrücklich von § 160 dAO erfasst sind (§ 102 Abs 1 Nr 4 HS 2 dAO; siehe dazu auch BFH 15. 1. 1998, IV R 81/96).

[59]) BFH 13. 12. 2016, X B 23/16; 4. 4. 1996, IV R 55/94.

[60]) FG Hessen 12. 3. 1981, IX 9/78.

[61]) Siehe zum Erwerb von Betriebsmitteln am Schwarzmarkt BFH 23. 2. 1951, IV 81/50 S; 16. 7. 1957, I 316/56 U.

[62]) Dazu differenzierend *Wackerbeck*, NWB 2021, 1790 (1790 ff).

Hingegen geht die bisherige deutsche Literatur zB für – die nicht als Betriebsausgaben abzugsfähigen[63]) – Lösegeldzahlungen im Fall der Entführung des Betriebsinhabers von einer Abzugsmöglichkeit als außergewöhnliche Belastung nach § 33 dEStG aus, ohne dass – der auch für Ausgaben nach § 33 dEStG anwendbare[64]) – § 160 dAO einer Anerkennung entgegenstünde.[65])

Die Befürworter der Anwendung einer Empfängerbenennung in Cybercrime-Fällen gehen von der Prämisse aus, dass eine Identitätsfeststellung der Täter sowie ein Weiterlaufen des Geschäftsbetriebs – wenn auch unter erschwerten Voraussetzungen – dem Grunde nach möglich seien und die Opfer sich daher mehr oder weniger freiwillig für die Leistung des Lösegeldes als Reaktion auf ein gewöhnliches Geschäftsrisiko entschieden.[66]) Wenngleich es sich hierbei um Abwägungsfragen handelt, können diese Argumente uE im Falle von professionell organisierten Ransomware-Angriffen kaum verfangen, da eine Identifikation der potenziell weltweit ansässigen und digital verschleierten Täter in der Realität auch mit hohem Aufwand quasi ausgeschlossen scheint und viele Geschäftszweige ohne Zugriff auf ihren digitalen Datenbestand und ihre IT-Systeme schlicht nicht mehr operieren können. Auch die These, die Öffentlichkeit müsse sich nicht mittels Abzugs von der Steuerbemessungsgrundlage an der offenbar als suboptimal beurteilten Entscheidung der Lösegeldzahlung beteiligen, überzeugt nicht. In Deutschland genügt (wie auch nach österreichischem Recht) für die Eigenschaft einer Zahlung als steuerliche Betriebsausgabe deren betriebliche Veranlassung; der Steuerpflichtige kann dabei aber frei entscheiden, wie er seine Mittel einsetzt, ohne dass die Höhe der Aufwendungen, deren Notwendigkeit, Üblichkeit oder Zweckmäßigkeit eine steuerliche Anerkennung vereitelt.[67])

Für die österreichische Rechtslage ist uE jedenfalls eine demgegenüber weitere Sichtweise geboten. Denn im Unterschied zu § 160 dAO, der darauf abstellt, dass der Steuerpflichtige dem Verlangen nach Empfängerbenennung *„nicht nachkommt“*, spricht § 162 Abs 1 BAO davon, dass der Steuerpflichtige die *„verlangten Angaben verweigert“*. Die Angabe *„verweigern“* heißt aber, dass Umstände, die bekannt sind oder die vom Befragten gemessen an seinem Wissen und den ihm zugänglichen Erkenntnisquellen festgestellt werden können, dem Fragenden nicht bekanntgegeben werden. In diesem Sinne dürfen dem Steuerpflichtigen daher keine offenbar unerfüllbaren Aufträge zum Nachweis der Empfänger erteilt werden. *„Offenbar unerfüllbar“* sind derartige Aufträge nach der Rechtsprechung (nur) dann, wenn eine unverschuldete, tatsächliche Unmöglichkeit, die Empfänger der geltend gemachten Betriebsausgaben namhaft zu machen, vorliegt.[68]) Zudem darf es *„nicht in der Macht des Steuerpflichtigen gestanden sein, die tatsächlichen Umstände, die ihn an der Bezeichnung der Empfänger hindern, abzuwenden“.* [69]) Hat aber der Abgabepflichtige bestehende zumutbare Beweisvorsorgepflichten nicht verletzt, so kann die Rechtsfolge des § 162 Abs 2 BAO nicht eintreten, wenn der Steuerpflichtige bei Unmöglichkeit der Bekanntgabe mangels Wissens und Feststellbarkeit die Namen der Empfänger nicht mitteilt. Eine Unmöglichkeit zur Empfängerbenennung kann solcherart etwa bei Diebstahl[70]) oder unverschuldetem Verlust von Unterlagen vorliegen.[71])

---

[63]) Siehe zB BFH 30. 10. 1980, IV R 27/77 (zur analogen Sichtweise im österreichischen Steuerrecht, zumal das Entführungsmotiv in der Kapitalkraft und Vermögenslage der Person liegt, siehe etwa *Kofler/Wurm* in *Doralt/Kirchmayr/Mayr/Zorn*, EStG (20. Lfg, 2018) § 20 Tz 129 mwN).
[64]) *Gercke* in *Koenig*, AO[4] (2021) § 160 Rn 18.
[65]) So ausdrücklich zB *Loschelder* in *Schmidt*, EStG[40] (2021) § 33 Rn 90 (unter *„Lösegeld“*).
[66]) So *Wackerbeck*, NWB 2021, 1790 (1793).
[67]) Siehe zB *Hey* in *Tipke/Lang*, Steuerrecht[23] (2018) § 8 Rz 231.
[68]) Siehe etwa VwGH 31. 1. 2001, 98/13/0156; 25. 4. 2013, 2013/15/0155.
[69]) VwGH 22. 11. 2012, 2008/15/0265; 25. 4. 2013, 2013/15/0155.
[70]) Rz 1113 EStR.
[71]) VwGH 19. 2. 1965, 0044/64; siehe auch Rz 1113 EStR.

Den Steuerpflichtigen trifft im Fall der Ransomware-Erpressung wohl auch kein Verschulden, Geschäftsbeziehungen nicht im Sinne einer Beweisvorsorge so gestaltet zu haben, dass die Person des Empfängers bzw Gläubigers namhaft gemacht werden kann.[72]) Es erschiene hier geradezu zynisch, dem Steuerpflichtigen vorzuwerfen, er habe die bewusste Nichtfeststellung der Identität des Täters zu verantworten.[73]) § 162 BAO stellt außerdem nur auf das Verschulden an der Nichtbenennung (zB durch mangelnde Dokumentation) und nicht etwa darauf ab, ob die ursächliche Schädigung (zB durch höhere IT-Sicherheit) verhindert hätte werden können. Darin liegt auch ein wesentlicher Unterschied etwa zu typischen Betrugsfällen in der Baubranche, bei denen die Rechtsprechung von der Anwendbarkeit des § 162 BAO ausgeht.[74]) So differenzierte etwa unlängst das BFG danach, dass der Übeltäter (etwa bei einem Diebstahl) *„in der Regel nicht greifbar ist“*, wohingegen beim fraglichen Betrug der Täter gegenüber der Steuerpflichtigen *„sehr wohl körperlich in Erscheinung trat und Geld von ihr in Empfang nehmen konnte“*.[75]) Auch dies spricht letztlich dafür, dass bei erwiesener Erpressung und betrieblich veranlasster Lösegeldzahlung ein Benennungsbegehren nach § 162 BAO ermessensfehlerhaft wäre und der Betriebsausgabenabzug schon aus diesem Grund nicht versagt werden darf.

Hinzu tritt folgende Überlegung: Der primäre Zweck des § 162 BAO liegt darin, die Besteuerung beim Empfänger sicherzustellen.[76]) § 162 BAO beruht nach der Rechtsprechung *„auf dem Grundsatz, dass das, was bei dem einen Abgabepflichtigen abzusetzen ist, bei dem anderen versteuert werden muss, wenn nicht steuerpflichtige Einnahmen unversteuert bleiben sollen“*.[77]) Allerdings ist die Anwendung des § 162 BAO dann nicht ausgeschlossen, wenn (bloß) behauptet wird, die Zahlungen seien beim Empfänger nicht steuerpflichtig.[78]) Ergibt jedoch das Ermittlungsverfahren, dass *„der wirkliche Empfänger der Zahlungen im Inland nicht steuerpflichtig ist“*, kann auf eine Empfängerbenennung nach § 162 BAO verzichtet werden.[79]) Auch nach der Verwaltungspraxis kann auf ein Benennungsbegehren bei unzweifelhaften betrieblichen Aufwendungen verzichtet werden, wenn sichergestellt ist, *„dass der wirkliche Empfänger der Zahlungen im Inland nicht steuerpflichtig ist“*.[80]) In diesem Sinne wird auch von der herrschenden Ansicht zu deutschen Parallelvorschrift des § 160 dAO ein Benennungsverlangen zB dann für unzulässig erachtet, wenn der Empfänger mit an Sicherheit grenzender Wahrscheinlichkeit nicht im Inland steuerpflichtig ist oder ein Steuerausfall aufseiten des Empfängers sonst ausscheidet.[81]) Unklar ist allerdings, ob es eine Rolle spielt (oder spielen soll), dass Österreich gegenüber dem Staat des (vermuteten) Empfängers zur Amtshilfe verpflichtet ist.[82]) Insgesamt scheint ein solcher Nachweis der steuerlichen Irrelevanz im Inland aber ohnehin schwer erbringbar: Der Umstand, dass der tatsächliche

---

[72]) Zu dieser Anforderung etwa VwGH 2. 3. 1993, 91/14/0144; 28. 5. 1997, 94/13/0230; 28. 10. 1997, 93/14/0073, 0099; siehe auch Rz 1117 EStR.

[73]) In diese Richtung aber *Wackerbeck*, NWB 2021, 1790 (1792).

[74]) BFG 10. 12. 2020, RV/7103693/2017; dazu auch *Hatzenbichler*, § 162 BAO: Unterlassung von Handlungen zur Identifizierung des betrügerischen Geschäftspartners, BFGjournal 2021, 151 (151 ff).

[75]) BFG 10. 12. 2020, RV/7103693/2017 (außerordentliche Revision von VwGH 7. 6. 2021, Ra 2021/13/0025, abgelehnt).

[76]) Siehe zB VwGH 2. 3. 1993, 91/14/0144; 28. 5. 1997, 94/13/0230; Rz 1110 EStR.

[77]) VwGH 25. 4. 2013, 2013/15/0155.

[78]) Rz 1109 EStR; siehe auch VwGH 14. 5. 1974, 0284/73; 25. 5. 2004, 2001/15/0019, ecolex 2004/426, 894 (*Kofler*/*Postl*).

[79]) VwGH 30. 6. 2010, 2007/13/0067 (zu einem möglicherweise in Russland ansässigen Zahlungsempfänger); ebenso BFG 10. 12. 2020, RV/7103693/2017; siehe zB auch *Ritz*, BAO[6], § 162 Tz 8 mwN; anders aber möglicherweise VwGH 25. 5. 2004, 2001/15/0019, ecolex 2004/426, 894 (*Kofler*/*Postl*), wo der VwGH dem Argument, dass auch im Falle, dass tatsächlich ein österreichischer Unternehmer Zahlungsempfänger gewesen wäre, jener mit diesen Einkünften aus ungarischen Betriebsstätten in Ungarn und nicht in Österreich steuerpflichtig wäre, entgegenhielt, *„dass § 162 BAO auf eine konkrete Steuerpflicht des Empfängers der abgesetzten Beträge nicht abstellt“*.

[80]) Rz 1125 EStR (zu Auslandsprovisionen).

[81]) *Rüsken* in *Klein*, AO[15] (2020) § 160 Rn 12; *Gercke* in *Koenig*, AO[4], § 160 Rn 30.

[82]) Siehe aber die Forderung von *Doralt*, § 162 BAO: Keine Empfängernennung bei Empfänger im Ausland? RdW 2013, 298 (298), der § 162 BAO auch dann anwenden möchte, wenn der vom Steuerpflichtigen

Empfänger keiner inländischen Steuerpflicht unterliegt, lässt sich ohne dessen Kenntnis kaum zweifelsfrei feststellen,[83]) zumal selbst ausländische Personen im Inland steuerpflichtig sein können.[84]) Ist die Abgabenbehörde aber nach dem Beweisverfahren davon überzeugt, dass der oder die anonymen Empfänger (zB die Hacker bei einer Ransomware-Erpressung) im Inland mit dem Lösegeld keinesfalls steuerpflichtig sind (und allenfalls auch eine Amtshilfe an das Ausland mangels Konkretisierbarkeit der Täter ins Leere laufen würde), scheint ein Begehren nach Empfängerbenennung auch in diesem Lichte unverhältnismäßig und damit ermessensfehlerhaft.

Im Bereich des § 162 BAO wird der Finanzverwaltung in Ransomware-Fällen durchaus ein gewisser Ermessensspielraum zukommen. Sollten etwa stichhaltige Anhaltspunkte dahingehend bestehen, dass zB der Täter im Inland ansässig ist oder von einem sorgfältigen Geschäftsmann mit vertretbaren Mitteln auszuforschen gewesen wäre, kann – analog der zuvor angesprochenen Meinung im deutschen Schrifttum – nicht von einer Unmöglichkeit der Empfängerbenennung gesprochen werden. Dies kann allerdings uE allenfalls als Korrektiv für besonders gelagerte Fälle dienen (wenn zB der begründete Verdacht eines Zusammenwirkens des Unternehmens mit den vermeintlichen Tätern zur Reduktion des steuerpflichtigen Gewinns besteht). In den hier angesprochenen typischen Situationen von Ransomware-Angriffen auf Betriebe wird die Ermessensentscheidung jedoch gegen eine Anwendung des § 162 BAO ausfallen müssen, da es dem Unternehmen unverschuldet unmöglich ist, die Täter zu benennen. Von entscheidender Bedeutung wird jedoch sein, die Vorgänge möglichst genau und schlüssig nachvollziehbar zu dokumentieren und belegen zu können. Die erwähnte Unmöglichkeit kann nämlich wohl nur geltend gemacht werden, wenn am tatsächlichen Vorliegen eines professionellen Ransomware-Angriffs und der speziell darauf erfolgten Zahlung kein Zweifel besteht.

4. Steuerzuschlag nach § 22 Abs 3 KStG bei Körperschaften?

Seit dem Betrugsbekämpfungsgesetz 2010[85]) besteht für Körperschaften zusätzlich ein *„Zuschlag in Höhe von 25 % von jenen Beträgen […], bei denen der Abgabepflichtige auf Verlangen der Abgabenbehörde die Gläubiger oder Empfänger der Beträge nicht genau bezeichnet“* (§ 22 Abs 3 KStG). Diese Regelung soll ausweislich der Gesetzesmaterialien dem Ausgleich einer fehlenden Besteuerungsebene, die durch die Nichtnennung des Zahlungsempfängers verursacht wird, dienen und hat überdies die Zielsetzung, Korruption und Geldwäsche entgegenzuwirken.[86]) Wenngleich § 22 Abs 3 KStG – anders als noch die Fassung im Begutachtungsentwurf[87]) – nicht formal an § 162 BAO anknüpft, war dieser *„bei der Schaffung der Regelung des § 22 Abs 3 KStG zweifelsfrei ein Orientierungspunkt für den Gesetzgeber“*.[88])

Allerdings besteht der Zuschlag zur Körperschaftsteuer unabhängig vom Vorliegen der Anspruchsvoraussetzungen des § 162 BAO;[89]) er ist insbesondere auch dann festzu-

nicht genannte Empfänger möglicherweise in einem Staat steuerpflichtig ist, gegenüber dem Österreich zur Amtshilfe verpflichtet ist oder – insbesondere aus Gründen der Gegenseitigkeit – daran interessiert sein muss. In diese Richtung auch *Tanzer* in *Althuber/Tanzer/Unger*, BAO-HB, 459, und *Dziurdź* in *Lang/Rust/Schuch/Staringer*, KStG^2 (2016) § 22 Rz 39.

[83]) Siehe auch VwGH 28. 6. 2000, 95/13/0182; 28. 5. 2009, 2008/15/0046.

[84]) Etwa aufgrund der beschränkten Steuerpflicht im Inland; siehe VwGH 27. 3. 1956, 0292/55, VwSlg 1396 F/1956.

[85]) BGBl I 2010/105.

[86]) Siehe ErlRV 875 BlgNR 24. GP, 7. Siehe zu einer Darstellung und Analyse der Kritik etwa *Blasina* in *Renner/Strimitzer/Vock*, KStG (32. Lfg, 2019) § 22 Tz 21 ff mwN.

[87]) Dazu *Blasina* in *Renner/Strimitzer/Vock*, KStG (32. Lfg, 2019) § 22 Tz 16.

[88]) Siehe VwGH 14. 9. 2017, Ro 2016/15/0004, GES 2017, 444 (*Renner*).

[89]) VwGH 14. 9. 2017, Ro 2016/15/0004, GES 2017, 444 (*Renner*); BFG 10. 12. 2020, RV/7103693/2017; *Dziurdź* in *Lang/Rust/Schuch/Staringer*, KStG^2, § 22 Rz 26.

setzen, wenn eine Aufforderung nach § 162 BAO unterbleibt (zB aus Ermessensüberlegungen) oder wenn die fraglichen Beträge gar nicht steuerlich als Betriebsausgaben geltend gemacht wurden.[90]) Umgekehrt wird der Zuschlag nach § 22 Abs 3 KStG in jenen Fällen parallel zum Tragen kommen, bei denen auch die Versagung des Betriebsausgabenabzugs nach § 162 Abs 2 BAO zur Anwendung kommt.[91])

Während die Rechtsfolge des Zuschlags bei mangelnder Bezeichnung der *„Gläubiger oder Empfänger der Beträge“* zwingend ist, liegt es im Ermessen der Abgabenbehörde, ob überhaupt die Gläubiger- oder Empfängerbenennung verlangt wird.[92]) Allerdings kann die Ermessensübung durchaus von jener bei § 162 BAO abweichen.[93]) So wäre etwa – im Lichte der Bekämpfung von Korruption und Geldwäsche[94]) – womöglich ein Abstellen auf eine konkrete oder gar inländische Steuerpflicht des Empfängers nicht geboten.[95]) Allerdings gilt für das *„Verlangen der Abgabenbehörde“* nach Empfängerbenennung auch bei § 22 Abs 3 KStG, dass es nicht offenbar unerfüllbar sein darf.[96])

Im Hinblick auf Ransomware-Erpressungen werden dieselben Wertungsmaßstäbe wie bei § 162 BAO heranzuziehen sein, sodass die unverschuldete Nichtbenennung des anonymen Erpressers bzw der anonymen Erpresser gleichermaßen nicht zu einem Zuschlag führen darf.

Auf den Punkt gebracht

Die von Unternehmen als Opfer von Ransomware-Angriffen an den oder die Täter bezahlten Lösegelder sind uE als steuerlich abzugsfähige Betriebsausgaben zu qualifizieren. Die Angemessenheit, Wirtschaftlichkeit, Zweckmäßigkeit und Notwendigkeit der Lösegeldzahlung spielen bei gegebener betrieblicher Veranlassung keine weitere Rolle. Das Abzugsverbot nach § 20 Abs 1 Z 5 lit a EStG für Geld- und Sachzuwendungen, deren Gewährung oder Annahme mit gerichtlicher Strafe bedroht ist, gelangt auf die Opfer einer strafbaren Erpressung (§ 144 StGB) nicht zur Anwendung. Ein Anwendungsfall dieses Abzugsverbots könnte jedoch bestehen, wenn die Leistung des Lösegelds als Beteiligung an einer kriminellen Vereinigung (§ 278 StGB) durch Vermögenszuwendung an selbige zu beurteilen ist. Wenngleich die strafrechtliche Debatte diesbezüglich noch nicht abgeschlossen ist, scheinen in typischen Ransomware-Fällen gute Gründe gegen eine solche Strafbarkeit zu sprechen, zumal im Rahmen des Abzugsverbots auch die subjektive Tatseite und etwaige strafrechtliche Rechtfertigungs- und Entschuldigungsgründe zu berücksichtigen sind.

Bei hinreichender Nachweisbarkeit des Zahlungsgrundes und Zahlungsflusses werden im Regelfall auch die Empfängerbenennung nach § 162 BAO oder ein KöSt-Zuschlag nach § 22 Abs 3 KStG nicht zur Anwendung gelangen, da dem Steuerpflichtigen die Nennung eines professionell agierenden Täters, der seine Identität verschleiert und zu dem keinerlei weitere Beziehung besteht, ohne eigenes Verschulden unzumutbar sein wird. Widrigenfalls würde ein Ermessensfehler vorliegen.

[90]) VwGH 14. 9. 2017, Ro 2016/15/0004, GES 2017, 444 (*Renner*); siehe auch *Lachmayer*/*Renner*, Nichtbenennung der Empfänger von Aufwendungen, RdW 2016, 67 (69); *Ritz*, BAO[6], § 162 Tz 20.
[91]) So *Lachmayer*/*Renner*, RdW 2016, 67 (70); siehe auch *Kirchmayr* in *Achatz*/*Kirchmayr*, KStG, § 22 Tz 10; *Blasina* in *Renner*/*Strimitzer*/*Vock*, KStG (32. Lfg, 2019) § 22 Tz 16.
[92]) *Kirchmayr* in *Achatz*/*Kirchmayr*, KStG, § 22 Tz 10; *Dziurdź* in *Lang*/*Rust*/*Schuch*/*Staringer*, KStG[2], § 22 Rz 37; *Blasina* in *Renner*/*Strimitzer*/*Vock*, KStG (32. Lfg, 2019) § 22 Tz 20 f; anders wohl *Lachmayer*/*Renner*, RdW 2016, 67 (70).
[93]) *Dziurdź* in *Lang*/*Rust*/*Schuch*/*Staringer*, KStG[2], § 22 Rz 37.
[94]) Siehe zu dieser Zielsetzung des § 22 Abs 3 KStG etwa ErlRV 875 BlgNR 24. GP, 7.
[95]) So *Dziurdź* in *Lang*/*Rust*/*Schuch*/*Staringer*, KStG[2], § 22 Rz 39.
[96]) Ausführlich und zur Parallelität mit § 162 BAO *Dziurdź* in *Lang*/*Rust*/*Schuch*/*Staringer*, KStG[2], § 22 Rz 38.