95. Jahrgang / 10. Oktober 2020 / Nr. 29

SWK

Steuer- und WirtschaftsKartei

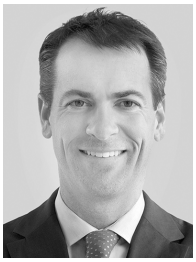
Linde
www.lindeverlag.at

Whistleblower-Richtlinie

Whistleblower: ein Segen für Unternehmen?

Inwiefern eine neue EU-Richtlinie neben Whistleblowern auch Unternehmen schützt

CHRISTOPHER SCHRANK / GREGOR KRISTÖFL*)



Die EU-Richtlinie zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden (kurz: Whistleblower-RL),[1]) wartet nur mehr auf die Transformation ins nationale Recht. Doch nicht nur für die Hinweisgeber selbst ist die Richtlinie interessant. Auch Unternehmen profitieren bei richtiger Implementierung von den Regelungen, weil durch entsprechende Hinweise Missstände früh erkannt und saniert werden können, bevor Behörden davon erfahren.

1. Was ist Whistleblowing?

Panama Papers, *Cambridge Analytica*, *Lux Leaks & Co* haben eine Sache gemein: Am Anfang der Enthüllungscausen standen immer *„Insider"*, die geheime Hinweise, Dokumente oder Berichte publik machten. Sogenannte *„Whistleblower"* (zu Deutsch auch *„Hinweisgeber"* bzw *„Enthüller"*) bringen aus geheimen oder zumindest geschützten Verhältnissen Missstände oder Verbrechen an die Öffentlichkeit und decken so Informationen auf, die sonst der Allgemeinheit verwehrt bleiben würden. Die oft fehlenden oder nur lückenhaft vorhandenen Schutzregelungen für Whistleblower schrecken aber vielfach davon ab, Missstände aufzudecken. Die persönlichen Folgen für Hinweisgeber sind teils beträchtlich, und einen monetären Anreiz, wie er im angloamerikanischen Raum vorgesehen ist, sucht man in Europa vergeblich. Auch die offizielle Empfehlung des Europarats aus dem Jahr 2014,[2]) nationale Regelungen zum Schutz von Whistleblowern umzusetzen, blieb weitgehend unbeachtet: Europaweit haben lediglich zehn Länder[3]) ein diesbezüglich umfassendes Gesetz. In den übrigen EU-Mitgliedstaaten sind die Informanten allenfalls nur teilweise geschützt, weil etwa der Schutz nur für bestimmte Sektoren gilt.

2. Ziel und Gegenstand der Whistleblower-RL

2.1. Allgemeines

Ab dem Jahr 2018 befasste sich auch das Europäische Parlament mit der Thematik, wobei im Oktober 2019 die EU-Richtlinie *„zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden"*, final beschlossen wurde. Die lange Dauer der Verhandlungen vom ersten Appell des Europarats im Jahr 2014 bis zum finalen Absegnen des Beschlusses durch den Rat der EU Ende 2019 spiegelt sich auch in der Zahl der Erwägungsgründe wider. So gehen den eigentlichen Normen der Richtlinie 110 Erwägungsgründe voran, die auch bereits erste Kommentierungen der neuen Regelungen beinhalten.

*) MMag. Dr. Christopher *Schrank* ist Partner der Brandl & Talos Rechtsanwälte GmbH. Gregor *Kristöfl* ist wissenschaftlicher Mitarbeiter der Brandl & Talos Rechtsanwälte GmbH.

1) Richtlinie (EU) 2019/1937 des Europäischen Parlaments und des Rates vom 23. 10. 2019 zum Schutz von Personen, die Verstöße gegen das Unionsrecht melden, ABl L 305 vom 26. 11. 2019, S 17.

2) Siehe dazu *Europarat*, Europarat fordert Staaten dringend zum Schutz von Whistleblowern und Journalisten auf, Pressemitteilung vom 2. 5. 2014, DC 055 (2014).

3) Frankreich, Ungarn, Irland, Italien, Litauen, Malta, Niederlande, Slowakei, Schweden und das Vereinigte Königreich.

2.2. Anwendungsbereich

Die Europäische Kommission spricht in der Richtlinie explizit von *„gemeinsamen Mindeststandards“*, wobei der sachliche Anwendungsbereich der Richtlinie begrenzt ist. Nach Art 2 Whistleblower-RL greifen die Schutzvorschriften nämlich nur bei der Meldung von Verstößen gegen EU-Recht. Dazu zählen

- öffentliches Auftragswesen,
- Finanzdienstleistungen, Finanzprodukte und Finanzmärkte sowie Verhinderung von Geldwäsche und Terrorismusfinanzierung,
- Produktsicherheit und -konformität,
- Verkehrssicherheit,
- Umweltschutz,
- Strahlenschutz und kerntechnische Sicherheit,
- Lebensmittel- und Futtermittelsicherheit, Tiergesundheit und Tierschutz,
- öffentliche Gesundheit,
- Verbraucherschutz und
- Schutz der Privatsphäre und personenbezogener Daten sowie Sicherheit von Netz- und Informationssystemen.

Diesen Mindeststandard können die Mitgliedstaaten bei der Transformation ins nationale Recht jedoch nach Belieben erweitern.[4]) Ein Gebot der Vollharmonisierung gilt dabei insofern nicht, als die Richtlinie eine günstigere Behandlung durch die Mitgliedstaaten für zulässig erklärt (Art 25 Whistleblower-RL).[5]) UE wäre es aber sinnvoll, den Standard der Richtlinie auch auf das Melden von Verstößen gegen nationales Recht zu erstrecken und generell alle Meldungen von Strafrechtsverstößen zu erfassen.

In persönlicher Hinsicht gilt die Richtlinie für sämtliche Hinweisgeber, die im privaten oder im öffentlichen Sektor tätig sind und dort Informationen über Verstöße erlangt haben. Primär sind daher all jene Personen erfasst, die diese Informationen aus einem direkten beruflichen Kontext beziehen, wie zB Arbeitnehmer (einschließlich Beamte), Selbständige oder Praktikanten. Darüber hinaus werden – wie Art 4 Whistleblower-RL ausdrücklich festlegt – auch Personen außerhalb des konkreten Arbeitsverhältnisses geschützt, wie etwa Lieferanten oder auch Kollegen und Verwandte des Hinweisgebers. Konsequenterweise gilt die Richtlinie auch für Personen, deren Arbeitsverhältnis noch nicht begonnen hat (falls Informationen während der vorvertraglichen Verhandlungen erworben wurden) bzw inzwischen beendet wurde.

Um in den persönlichen Schutzbereich der Richtlinie zu fallen, müssen zusätzlich noch zwei weitere Voraussetzungen erfüllt sein:

- Gemäß Art 6 Abs 1 Whistleblower-RL hat der Hinweisgeber nur Anspruch auf Schutz, wenn hinreichend Grund zur Annahme besteht, dass die gemeldeten Informationen zum Zeitpunkt der Meldung der Wahrheit entsprachen (Stichwort Redlichkeit).[6]) Personen, die böswillig oder missbräuchlich irreführende bzw schlichtweg falsche Informationen melden, sollen daher nicht geschützt werden.

---

[4]) Vgl ErwGr 5 Whistleblower-RL: *„Die Mitgliedstaaten können entscheiden, den Anwendungsbereich der nationalen Bestimmungen auf andere Bereiche auszudehnen, um auf nationaler Ebene für einen umfassenden und kohärenten Rahmen für den Hinweisgeberschutz zu sorgen.“*

[5]) Vgl *Thüsing/Rombey*, Nachdenken über den Richtlinienvorschlag der EU-Kommission zum Schutz von Whistleblowern, NZG 2018, 1001.

[6]) Überhaupt zielt der Schutz der Richtlinie nicht nur auf das Melden bereits eingetretener, tatsächlicher Verstöße ab, sondern auch auf rein potenzielle Verstöße bzw solche, die *„sehr wahrscheinlich erfolgen werden“* (Art 5 Abs 2 Whistleblower-RL).

- Außerdem muss der Whistleblower – was für den Schutz der Unternehmen sehr wichtig ist – seine Meldung im richtigen Kanal in der richtigen Reihenfolge kundtun: In der Regel muss er zuerst über den innerbetrieblichen Weg melden, dann extern (behördlich), und erst danach kann er sich als *ultima ratio* an die Öffentlichkeit wenden.

2.3. Weiter Schutz: Verbot von Repressalien

Primäres Ziel der Richtlinie ist es, Hinweisgeber rechtlich abzusichern, wenn sie Missstände bzw Verbrechen melden, und ihnen Schutz vor unternehmensinternen Vergeltungsmaßnahmen oder Diskriminierungen zuzusichern. Damit Hinweisgeber vor etwaigen für sie nachteiligen Handlungen/Unterlassungen geschützt werden, verbietet Art 19 Whistleblower-RL in einer demonstrativen Aufzählung jede Art von Repressalien gegen Hinweisgeber – allein die Androhung solcher ist verboten. Als Beispiele werden etwa Suspendierungen, Kündigungen, Gehaltsminderungen, Diskriminierungen, Schädigungen, Disziplinarmaßnahmen oder auch die Versagung einer Beförderung als nicht zulässig erklärt. Zusätzlich ordnet die Whistleblower-RL als unterstützende Maßnahmen auch kostenfreie Rechtsberatung oder eine Beweislastumkehr im Gerichtsverfahren zu Lasten des Arbeitgebers an.

3. Meldekanäle

3.1. Dreistufiges Meldesystem

Die Mitgliedstaaten haben sicherzustellen, dass die Unternehmen und die Behörden Kanäle zur Übermittlung und Weiterverfolgung von Whistleblower-Meldungen einrichten. Diese Verpflichtung zur Implementierung von internen und externen Meldekanälen ist das Kernstück der Richtlinie. Um allerdings sicherzustellen, dass zuerst das betroffene Unternehmen über den mutmaßlichen Missstand aufgeklärt wird, ist in der Richtlinie gewissermaßen in letzter Sekunde ein *de facto* dreistufiges Meldesystem eingefügt worden: In erster Linie sind – sofern intern wirksam gegen den Verstoß vorgegangen werden kann und der Hinweisgeber keine Repressalien befürchten muss – innerbetriebliche Kanäle zur Meldung zu verwenden. Setzt das Unternehmen jedoch in der Folge keine geeigneten Maßnahmen, ist die Meldung an zuständige Behörden (die zu diesem Zweck ebenfalls Meldekanäle schaffen müssen) zu richten. An die Presse bzw die Öffentlichkeit (sogenannte *„Offenlegung“*, Art 15 Whistleblower-RL) dürfen sich Hinweisgeber nur als *ultima ratio* wenden – nämlich nur dann, wenn der Meldeversuch zuerst bei internen sowie bei externen Kanälen ergebnislos gescheitert ist. Darüber hinaus dürfen auch dann der Presse Informationen offengelegt werden, wenn der Verstoß eine unmittelbare oder offenkundige Gefährdung des öffentlichen Interesses darstellt bzw wenn Repressalien drohen. Allerdings – und insoweit wurde die Dreistufigkeit wieder etwas aufgeweicht – werden Hinweisgeber auch dann geschützt, wenn sie sich direkt an die zuständige externe Behörde wenden, ohne davor auf die Möglichkeiten der unternehmensinternen Meldekanäle zurückzugreifen.[7]) Es wäre daher wünschenswert, im Zuge der Umsetzung der Richtlinie das Stufenverhältnis stärker zu betonen.

3.2. Einrichtung der Meldekanäle

Interne Meldekanäle sind jedenfalls von allen Unternehmen mit mehr als 50 Beschäftigten einzurichten. Klein- und Kleinstunternehmen sind zwar nach der Richtlinie ausgenommen; die Mitgliedstaaten könnten jedoch auch ihnen vorschreiben, interne Meldekanäle einzurichten (zB aufgrund erheblicher Risiken, die sich aus ihrer Tätigkeit ergeben).[8]) Unternehmen mit Tätigkeit im Finanzdienstleistungssektor oder mit hoher

[7]) *Kapek/Popp*, Whistleblowing- und Geschäftsgeheimnisschutz, Compliance Praxis 2019, 38 (39).
[8]) Siehe ErwGr 48 Whistleblower-RL.

Anfälligkeit für Geldwäsche oder Terrorismusfinanzierung sind unabhängig von ihrer Größe zur Einrichtung der Kanäle verpflichtet.

Bezüglich der externen Kanäle müssen die Mitgliedstaaten bei der Umsetzung der Richtlinie die zuständigen Behörden benennen, die befugt sind, Meldungen über Verstöße entgegenzunehmen und geeignete Folgemaßnahmen zu ergreifen.

Bei der Einrichtung der Meldekanäle müssen vorgegebene Standards eingehalten werden, um die Vertraulichkeit der entgegengenommenen Informationen zu wahren und die Identität des Hinweisgebers zu schützen. So ist sicherzustellen, dass nur befugte Mitarbeiter Zugriff auf die Meldekanäle haben.[9]) Für alle Mitarbeiter, die eingehende Meldungen bearbeiten oder sonst Zugang zu den gemeldeten Informationen haben (wie etwa Personen, die ausschließlich für die Entgegennahme von Meldungen oder für das Ergreifen von Folgemaßnahmen zuständig sind), gilt eine strenge Verschwiegenheitspflicht. Daneben gelten bei der Verarbeitung personenbezogener Daten in Verbindung mit dem Hinweisgebersystem die Bestimmungen der DSGVO.

Intern kann ein Meldekanal von einer dafür benannten Person oder auch einer Dienststelle betrieben werden. Welche Person innerhalb des Unternehmens am besten zur Entgegennahme von Meldungen geeignet ist, hängt – wie Erwägungsgrund 56 der Whistleblower-RL klarstellt – von der Struktur des Unternehmens ab. Gerade in kleineren Unternehmen kann diese Aufgabe durch einen Mitarbeiter in Doppelfunktion erfüllt werden, etwa den Leiter der Compliance- oder Personalabteilung, der auf direktem Weg der Unternehmensführung berichten kann.[10]) Dabei sollte die Wahl der zuständigen Person so gestaltet sein, dass Unabhängigkeit gewährleistet ist und Interessenkonflikte vermieden werden. Es ist aber auch zulässig, den internen Meldekanal an externe Dritte auszulagern, die aber natürlich ebenfalls die Unabhängigkeit, die Vertraulichkeit sowie den Datenschutz sicherstellen müssen. In Betracht kommen hier vor allem Rechtsanwaltskanzleien, die bereits von Gesetzes wegen die Erfordernisse der Vertraulichkeit und der Unabhängigkeit erfüllen und daher dazu prädestiniert sind, die Whistleblower-Meldung in Form eines persönlichen Gesprächs entgegenzunehmen. Dies hat im Vergleich zu schriftlichen oder fernmündlichen Meldekanälen den Vorteil, dass bei Unklarheiten sofort rückgefragt werden kann, was die Aufarbeitung des Sachverhalts in der Regel deutlich beschleunigt. Gemäß Erwägungsgrund 54 der Whistleblower-RL können aber auch sonstige Berater, externe Anbieter von Meldeplattformen sowie Gewerkschaftsvertreter oder Arbeitnehmervertreter zur Entgegennahme und Verarbeitung der Meldungen eingeteilt werden.

3.3. Technische Ausgestaltung und Rückmeldung

Bei der technischen Ausgestaltung des internen Meldekanals ist insbesondere darauf zu achten, dass die Meldungen in verschiedenen Formen erstattet werden können. Dazu gehören die schriftliche Meldungsübermittlung in digitaler Form oder auf Papier, die mündliche Meldungsübermittlung per aufgezeichnetem oder nicht aufgezeichnetem Telefongespräch sowie die physische Zusammenkunft mit der Person, die für die Entgegennahme von Meldungen in dem Unternehmen zuständig ist.[11])

Whistleblower dürfen sich auch ein entsprechendes Feedback des Unternehmens erwarten: So ist zunächst innerhalb von sieben Tagen der Eingang der Meldung zu bestätigen. In weiterer Folge ist dem Hinweisgeber innerhalb von drei Monaten eine in-

[9]) Art 9 Abs 1a Whistleblower-RL.

[10]) Potenzielle Mitarbeiter in Doppelfunktion wären laut ErwGr 56 Whistleblower-RL der Leiter der Compliance- oder Personalabteilung, ein Integritätsbeauftragter, ein Rechts- oder Datenschutzbeauftragter, ein Finanzvorstand, ein Auditverantwortlicher oder ein Vorstandsmitglied.

[11]) *Groß/Platzer*, Richtlinie der EU zur Stärkung des Schutzes von Hinweisgebern ante portas, NZA 2018, 913 (914); siehe dazu auch Art 9 Abs 2 sowie Art 12 Abs 2 Whistleblower-RL.

haltliche Rückmeldung über die geplanten oder bereits ergriffenen Folgemaßnahmen und deren Gründe zu geben. In hinreichend begründeten Fällen kann die externe Behörde den Zeitrahmen sogar auf sechs Monate erhöhen, etwa wenn die Komplexität des Gegenstands der Meldung eine langwierige Untersuchung benötigt. Wird einer Meldung nicht rechtzeitig nachgekommen, können sich die Hinweisgeber gemäß dem dreistufigen System an die nächste zuständige Ebene wenden: Wurde eine interne Meldung missachtet, können die Behörden informiert werden; wurde eine externe Meldung missachtet, können sich die Hinweisgeber an die Öffentlichkeit wenden (Art 15 Abs 1 lit a Whistleblower-RL). Sofern die zuständige Stelle Meldungen von Hinweisgebern behindert oder zu behindern versucht hat, muss sie auch mit Sanktionen rechnen (Art 23 Abs 1 lit a Whistleblower-RL).

4. Whistleblowing als Chance zur Sanierung von Verstößen

Vielfach sehen Unternehmen die verpflichtende Einrichtung von Whistleblower-Systemen als bloße finanzielle oder organisatorische Last. Allerdings bieten funktionierende und zuverlässige innerbetriebliche Kanäle auch ganz wesentliche Vorteile: Mithilfe der ersten internen Anlaufstelle hat ein Unternehmen nämlich die Möglichkeit, potenziell rechtswidriges Verhalten im Betrieb möglichst früh zu erkennen und zu „sanieren", bevor die Behörden alarmiert werden oder Informationen an die Öffentlichkeit gelangen.

Im Strafrecht können viele Delikte (wie etwa Betrug oder Untreue) durch die sogenannte *„Tätige Reue"* (§ 167 StGB) saniert werden. Danach erlischt die Strafbarkeit, wenn der Schaden rechtzeitig, freiwillig und vollständig wiedergutgemacht wird – Sanktionen, Strafzahlungen oder Image-Schäden bleiben dem Unternehmen so erspart. Doch selbst wenn es nach dem Gesetz keine Möglichkeit zur Sanierung von Strafrechtsverstößen gibt (wie etwa im Bereich der Korruptionsdelikte), kann die Whistleblower-Meldung jedenfalls dazu beitragen, den Sachverhalt aufzuklären und das Begehen zukünftiger ähnlicher Taten zu verhindern, was jedenfalls die Verbandsgeldbuße reduziert.[12]) Neben der Tätigen Reue kommt im Strafrecht auch der *„Rücktritt vom Versuch"* nach § 16 StGB in Betracht, wonach die Strafbarkeit wegen Versuchs oder Beteiligung entfällt. Dabei zu beachten ist aber die dafür verlangte Freiwilligkeit. Im Bereich des Finanzstrafrechts kommt als Sanierungsmöglichkeit die Selbstanzeige infrage, durch die sich der Abgabepflichtige die Straffreiheit sichern kann. Durch frühzeitige Informationen der Hinweisgeber können Unternehmen somit etwaige Missstände unternehmensintern ausbessern, adäquate Maßnahmen setzen bzw durch Inanspruchnahme genannter gesetzlicher Bestimmungen einer Haftung oder Rufschädigung entgehen.

5. Blick in die Zukunft

Spätestens nach Ablauf der Umsetzungsfrist wird erstmals ein EU-weit gemeinsamer und umfassender Mindestschutz für Whistleblower gewährt sein. Was jedenfalls noch aussteht, national geregelt zu werden, sind die konkreten Rechtsfolgen bei Verstößen gegen eben diese unionsrechtlichen Auflagen, weil diese von der Richtlinie nur abstrakt definiert werden: Einerseits müssen wirksame und angemessene Sanktionen für natürliche und juristische Personen festgelegt werden, die zB Meldungen behindern oder Repressalien ergreifen. Andererseits müssen auch abschreckende Sanktionen für die Hinweisgeber selbst normiert werden, wenn diese etwa wissentlich falsche Informationen melden oder gleich an die Öffentlichkeit gehen. Die entsprechenden nationalen Vorschriften müssen prinzipiell bis zum Dezember 2021 in Kraft treten – diejenigen betreffend die Einrichtungspflicht interner Kanäle bei juristischen Personen mit bis zu 249 Arbeitnehmern jedoch erst bis zum 17. 12. 2023.

[12]) Vgl § 5 Abs 3 Z 3 und 5 VbVG.

Auf den Punkt gebracht

Die Whistleblower-RL gewährt erstmals EU-weit einen gemeinsamen und umfassenden Mindestschutz für Whistleblower. Der sachliche Anwendungsbereich der Richtlinie ist auf die Meldung von Verstößen gegen EU-Recht begrenzt. In persönlicher Hinsicht gilt die Richtlinie für sämtliche Hinweisgeber, die im privaten oder im öffentlichen Sektor tätig sind und dort Informationen über Verstöße erlangt haben. Zusätzlich hat der Hinweisgeber redlich zu sein und die Meldung im richtigen Kanal in der richtigen Reihenfolge kundzutun.

Kernstück der Richtlinie ist die Verpflichtung zur Implementierung von internen und externen Meldekanälen zur Übermittlung und Weiterverfolgung von Whistleblower-Meldungen. In erster Linie sind innerbetriebliche Kanäle zur Meldung zu verwenden. Setzt das Unternehmen in der Folge keine geeigneten Maßnahmen, ist die Meldung an die zuständigen Behörden zu richten. An die Presse bzw die Öffentlichkeit dürfen sich Hinweisgeber nur als *ultima ratio* wenden.

Pauschale Vorratsdatenspeicherung laut EuGH nicht zulässig

Entscheidung: EuGH 6. 10. 2020, *La Quadrature du Net ua*, C-511/18.

Norm: Art 15 Abs 1 RL 2002/58/EG.

In einer Entscheidung vom 6. 10. 2020 hat der EuGH zur Vorratsdatenspeicherung folgende Aussagen getroffen: Eine flächendeckende und pauschale Speicherung von Internet- und Telefonverbindungsdaten ist nicht zulässig; Ausnahmen sind aber möglich – so dürfen Mitgliedstaaten zur Bekämpfung schwerer Kriminalität und im Fall einer Bedrohung der nationalen Sicherheit Vorratsdatenspeicherung anordnen.

Konkret beschäftigte sich der EuGH im vorliegenden Urteil mit den nationalen Regelungen in Belgien, Frankreich und Großbritannien. Bereits im Jahr 2016 hatte der EuGH die anlasslose Speicherung von Telefon- und Internetdaten für unzulässig erklärt. Diese Rechtsprechung wurde nun im Wesentlichen bestätigt, allerdings wurden Ausnahmeregeln festgelegt, da die Mitgliedstaaten moniert hatten, dass es die Strafverfolgung, Gefahrenabwehr und die Bekämpfung von Terror erschwere, wenn sie keinen Zugriff auf Internet- und Telefondaten von verdächtigen Personen nehmen dürften. Weiters hatten die Mitgliedstaaten argumentiert, dass es allein ihre Sache sei, für Sicherheit in ihrem jeweiligen Hoheitsgebiet zu sorgen – dies umfasse auch alle Maßnahmen, die die Regierungen für erforderlich hielten.

Dieser Ansicht widersprach der EuGH zwar, dennoch gestattet er den Mitgliedstaaten nun, zur Bekämpfung und Abwehr schwerer Straftaten die vorübergehende allgemeine Speicherung von Telefon- und Internetdaten anzuordnen. Das müsse sich allerdings auf den unbedingt erforderlichen Zeitraum beschränken und von Gerichten bzw unabhängigen Behörden überprüft werden. Droht somit etwa ernsthaft und nachweisbar ein Terroranschlag, dürfen Kontakt- und Standortdaten gespeichert und eingesehen werden oder IP-Adressen von Internetprovidern herausverlangt werden – dies allerdings nur so lange wie unbedingt erforderlich; darüber hinaus müsse der Grundrechtseingriff von einem Richter genehmigt werden.

Das Urteil des EuGH erklärt formal nur die Vorratsdatenspeicherungen in Belgien, Frankreich und Großbritannien für unvereinbar mit EU-Recht. So steht etwa eine Entscheidung zur Frage der deutschen Vorratsdatenspeicherung, vorgelegt vom Bundesverwaltungsgericht Leipzig, noch aus.