

## Öffentliches Transparenzregister wirtschaftlich Berechtigter

Referentenentwurf eines Gesetzes zur Umsetzung der Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie [Richtlinie (EU) 2018/843] (20.5.2019)

DIE FAMILIENUNTERNEHMER unterstützen den Kampf der EU und der Bundesregierung gegen Geldwäsche, Steuerhinterziehungen sowie die Finanzierung der organisierten Kriminalität und des und Terrorismus. Ein wichtiges Element ist dabei die Identifikation von wirtschaftlich Berechtigten. Deshalb bedarf es in der Tat besserer Informationen über diese Personen, insbesondere derer, die sich womöglich Strohmännern bedienen. Wichtig ist auch ein effizienterer Austausch der nationalen Daten zwischen verschiedenen Staaten. Das im Sommer 2017 geschaffene und eingerichtete Transparenzregister wirtschaftlich Berechtigter, zu dem Behörden uneingeschränkter Zugang haben, kann hierfür nützlich sein. Auch die nun vorgesehene Vernetzung der Register innerhalb der EU vermag den Kampf gegen Geldwäsche weiter voranzutreiben, wenn gleichzeitig die entsprechenden Datenschutz-, Europa- und Grundrechte der wirtschaftlich Berechtigten gewahrt werden.

Bei allen Bestrebungen für mehr Transparenz dürfen jedoch die Rechte des wirtschaftlich Berechtigten nicht verletzt werden. Diese sind zum größten Teil redliche Familienunternehmer, deren Daten zu schützen sind. Allerdings erleichtert bereits das nach derzeitigem Stand betriebene Transparenzregister - mit einem Recht zur Einsichtnahme von Personen mit einem sogenannten berechtigtem Interesse - erhebliche Eingriffe in das Grundrecht auf informationelle Selbstbestimmung von Familienunternehmern.

Die Öffnung des Transparenzregisters für jedermann verletzt das Europarecht und die Grundrechte des Grundgesetzes. Diese Rechtsverstöße können nur vermieden werden, wenn von der Öffnung abgesehen wird. Es fehlt an jeglicher Verhältnismäßigkeit zwischen Transparenz und Persönlichkeitsrechten. Der Rechtsbruch würde nicht verhindert, aber reduziert, wenn Schutzrechte von Personen, die im Transparenzregister geführt werden, umfassend erweitert werden.

Die in § 23 Abs. 2 GwG bereits aufgezählten Straftaten – Betrug, erpresserischer Menschenraub, Geiselnahme, Erpressung oder räuberische Erpressung, eine strafbare Handlung gegen Leib oder Leben, Nötigung oder Bedrohung – veranschaulichen, wie groß die Gefahr für wirtschaftlich Berechtigte und deren Familienangehörige ist. Insofern sollte jedem wirtschaftlich Berechtigten ermöglicht werden, einen Antrag gem. § 23 Abs. 2 GWG darauf zu stellen, dass eine vollständige oder teilweise Beschränkung der Einsichtnahme vorgenommen wird. Dieser wird Familienunternehmern jedoch aus rechtlichen wie auch praktischen Gründen versagt. Ein analoges Verfahren zur Auskunftssperre wegen Gefährdung gem. § 51 BMG wäre eine zielführende Maßnahme.

## I. Die „5. EU-Geldwäscherichtlinie“ EU 2018/843

Obwohl die Änderungsrichtlinie zur Vierten EU-Geldwäscherichtlinie (EU) 2018/843 („5. EU-Geldwäscherichtlinie“) und der darin vorgesehene öffentliche Zugang gem. Artikel 1 Nummer 15 Buchstabe c zum Transparenzregister bereits rechtskräftig verabschiedet wurden, gehen DIE FAMILIENUNTERNEHMER davon aus, dass damit rechtswidriges Europarecht erlassen wurde. Denn die Europäische Menschenrechtskonvention (EMRK), die Grundrechtecharta (GRC) und das allgemeine europäische Datenschutzrecht verlangen, mit Daten angemessen umzugehen.

So regelt Art. 7 GRC das Recht jeder Person auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation. Des Weiteren schützt das Datenschutzgrundrecht nach Art. 8 GRC personenbezogene Daten des Einzelnen, die nach Treu und Glauben nur für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden dürfen. Art. 8 EMRK entspricht weitgehend Art. 7 und 8 GRC.

Auf die Wechselwirkung zwischen EU-Grundrechten und öffentlicher Ordnung sind auch schon die Gerichte aufmerksam geworden. In der Rechtssache „Digital Rights Ireland“<sup>1</sup> erkannte der EuGH, dass die Bekämpfung von internationalem Terrorismus und schwerer Kriminalität eine dem Gemeinwohl dienende Zielsetzung ist. Da jedoch die zum Erreichen dieser Zielsetzung erlassenen Rechtsakte einen Eingriff in die Grundrechte auf Privatsphäre und Datenschutz darstellen, ist es nach Auffassung des Gerichtshofs erforderlich, die Verhältnismäßigkeit solcher Maßnahmen zu prüfen. Auch EU-datenschutzrechtlich muss jede Verarbeitung personenbezogener Daten einem rechtmäßigen, festgelegten und genau umrissenen Zweck dienen, für das Erreichen dieses Zwecks erforderlich sein und zu ihm in einem angemessenen Verhältnis stehen.

Die Rechtfertigung der 5. EU-Geldwäscherichtlinie für einen öffentlichen Zugang zu den persönlichen Daten von Unternehmern speist sich aus dem Argument „mehr öffentliche Kontrolle“. Auf diese Weise könne ein Beitrag zur Bekämpfung des Missbrauchs von Gesellschaften und anderen juristischen Personen und ähnlichen Rechtsvereinbarungen für die Zwecke der Geldwäsche und der Terrorismusfinanzierung geleistet werden, als auch Ermittlungen erleichtert und Reputationseffekte bewirkt werden, da jedem, der Geschäfte abschließt, die Identität der wirtschaftlichen Eigentümer bekannt ist.

Die EU behauptet weiter: „Durch die verstärkte öffentliche Kontrolle wird ein Beitrag zur Verhinderung des Missbrauchs von juristischen Personen und Rechtsvereinbarungen einschließlich der Steuerumgehung geleistet.“<sup>2</sup> Das Transparenzregister soll also mehreren fiskalpolitischen Interessen dienen.

---

<sup>1</sup> EuGH, Urteil vom 8. April 2014, verbundene Rechtssachen C-293/12 und C-594/12, Digital Rights Ireland

<sup>2</sup> (EU) 2018/843 Absatz 35

Dabei ist nicht ersichtlich, inwiefern die Offenlegung von personenbezogenen Daten insbesondere gegenüber interessierten Laien für den zugrundeliegenden Regelungszweck der Bekämpfung des Geldwäscherisikos förderlich sein soll. Dieser Nutzen lässt sich nicht belegen. Er hat sich auch nicht in anderen Ländern, die ein öffentliches Register eingeführt haben, erwiesen. Denn im Grunde müsste es zur effektiven Geldwäschebekämpfung um die Aufdeckung von sogenannten „Strohmannbeteiligungen“ gehen, bei denen der formale Gesellschafter wirtschaftlich unbedeutend ist und sich dahinter ein wahrer wirtschaftlich Beteiligter verbirgt. Kriminell angelegte Strukturen werden andere Wege finden, als sich im deutschen Register offenlegen zu lassen.

Im Gegensatz zum Argument der „öffentlichen Kontrolle“ haben die Angaben über Vermögensverhältnisse, Beteiligungen oder Engagements über öffentliche, im Geschäftsverkehr relevante Dimension hinaus eine erhebliche private Dimension. Das Transparenzregister sammelt sensible Informationen über Vermögen, über wirtschaftliche Verhältnisse und auch über Strukturen von Unternehmen.

Dass entsprechende Daten nicht offengelegt werden sollen und der wirtschaftlich Berechtigte nicht öffentlich in Erscheinung treten will, kann dabei verschiedene, gut nachvollziehbare und auch legitime persönliche Gründe haben, die durchaus keinen Bezug zu kriminellen Handeln aufweisen: angefangen von einem Vereinsengagement mit politischen oder religiösem Bezug, über die vorweggenommene Regelung von Erbangelegenheiten, die der Erblasser bis zum Todesfall für sich behalten will, über die unternehmerische Tätigkeit einer Person, die wegen ihres „verbrannten“ oder in der Öffentlichkeit bekannten Namens im Hintergrund bleiben möchte, bis hin zu der Tatsache, dass Personen nicht als „vermögend“ oder „privilegiert“, sondern als Normalbürger in ihrer Umwelt wahrgenommen werden möchten – nicht nur weil sie dadurch angesichts der unzureichenden Ausnahmeregelungen zu Recht dem Risiko einer Straftat zum Opfer zu fallen, ausgesetzt werden, sondern weil Vermögen in der Gesellschaft nicht nur neidlos anerkannt wird. Hierzu zählen also beispielsweise auch die genannten Geheimhaltungsinteressen zwecks Vermeidung von Erb- und Pflichtteilsstreitigkeiten sowie mit Blick auf Konkurrenzunternehmen.

Viel mehr noch, wenn der Datenzugriff tatsächlich zum Zwecke der Bekämpfung von Kriminalität erfolgen soll, müsste ein Anfangsverdacht vorliegen und die Strafverfolgungsorgane tätig werden. Aufgrund der Zielsetzung und der Publizität wird hingegen jeder wirtschaftlich Berechtigte unter Generalverdacht gestellt. Der öffentliche Zugang wird wohl eher allein zur Befriedung der Neugier ganz unterschiedlicher Kreise ausgenutzt werden.

Diese genannten Beweggründe der EU sind nicht mit der strikten Zweckbindung eines Eingriffs in die grundrechtlich geschützten Interessen von Datenschutz, Recht auf Familien- und Privatleben sowie das Recht auf unternehmerische Freiheit in Einklang zu bringen. Die Öffnung für jeden wird die in der Richtlinie ausdrücklich betonten Risiken der Betroffenen, Opfer eines Betrugs, einer Entführung, von Erpressung, Gewalt und Einschüchterung zu werden, erheblich erhöhen. Diese Risiken wiegen schwer. Die Öffnung für jedermann ist angesichts dieser dramatischen Gefahren nicht zu rechtfertigen.

Darüber hinaus ist der Grundrechtseingriff endgültig, denn Informationen, die einmal im Internet verfügbar sind, „erhält man nicht wieder zurück“.<sup>3</sup>

Auch der EU-Datenschutzbeauftragte kommt in seiner Stellungnahme vom 2. Februar 2017 zu einem ähnlichen Schluss, wenn er von einem „signifikanten und unnötigen Risiko für das individuelle Recht auf Privatsphäre und Datenschutz“ im Falle eines öffentlichen Registers spricht.<sup>4</sup> Die EU hörte dabei nicht auf seinen gutachterlichen Rat, den Zugang zu Informationen über den wirtschaftlichen Eigentümer unter anderem so zu gestalten, dass Zugang nur Stellen gewährt wird, die für die Durchsetzung des Rechts zuständig sind.

Darüber kann auch nicht das in der deutschen Gesetzesbegründung geführte Argument der *lex specialis* hinweghelfen: Der Richtliniengeber hat ein mögliches Konfliktpotential zwischen den Regelungen der Datenschutz-Grundverordnung und den Richtlinienvorgaben zum öffentlichen Zugang getroffen. Die Geldwäscherichtlinien betonen an verschiedenen Stellen, dass der Datenschutz eingehalten werden soll. Ohnehin ist fraglich, ob der europäische Normgeber von der Datenschutzgrundverordnung abweichende Regelungen treffen darf. Der Begriff der Grundverordnung betont eine besondere Verbindlichkeit der datenschutzrechtlichen Vorgaben. Aber selbst wenn von der Datenschutzgrundverordnung abweichende Regelungen getroffen werden könnten, sind diese sich jedenfalls am Grundrechtsrahmen, insbesondere an Art. 8 GRC, zu messen. Überdies können sich diese Vorgaben nicht über die vom EuGH in Sachen Vorratsdatenspeicherung statuierten Vorgaben hinwegsetzen, der insbesondere durch den EuGH in Sachen Digital Rights Ireland und Tele Sverige<sup>5</sup> konkretisiert wurde. Die Vorgaben der 5. EU-Geldwäscherichtlinie in Bezug auf das Transparenzregister werden dem dabei nicht gerecht.

### **Petition: Vorlage zum EuGH**

Die 5. EU-Geldwäscherichtlinie und der darin vorgesehene öffentliche Zugang zum Transparenzregister wirtschaftlich Berechtigter verstößt offensichtlich gegen Europarecht, in dem die Grundrechte nach Art. 7, 8 und 16 GRC verletzt werden. Dies ist ein Tiefpunkt der europäischen Rechtsetzung zu Lasten der für Europa so wichtigen Familienunternehmer. Dies hat weitreichende Folgen, denn es könnte eine Blaupause für weitere Aufweichungen der strengen Datenschutzstandards und Persönlichkeitsrechte im Zeitalter der Digitalisierung und weltweiten Vernetzung werden. Deutschland darf die 5. EU-Geldwäscherichtlinie daher nicht umsetzen. Der nationale Gesetzgeber sollte den Rechtsweg erwägen und die Richtlinie zur Prüfung vor den EuGH bringen.

## II. Umsetzung in Deutschland

### **Datenschutz und verfassungsrechtliche Bedenken**

Allen Mitgliedsstaaten ist eine Frist bis zum 10.01.2020 gesetzt worden, die 5. EU-Geldwäscherichtlinie und den öffentlichen Zugang zum Transparenzregister umzusetzen.

<sup>3</sup> vgl. Müller Transparenz auf allen Ebenen, NZWiSt 2017, 87

<sup>4</sup> [https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2017/17-02-02\\_Opinion\\_AML\\_EN.pdf](https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2017/17-02-02_Opinion_AML_EN.pdf)

<sup>5</sup> EuGH, Urteil vom 21.12.2016, verbundene Rechtssache C-203/15 und C-698/15 (Tele2 Sverige u.a.).

Dieser wird nun in § 23 Abs. 1 Nr. 3 GWG-E geregelt. Die Umsetzung muss sich dabei auch am deutschen Verfassungsrecht und Datenschutz messen lassen und vereinbar sein.

Dies erscheint höchst zweifelhaft. Denn bereits im Jahr 1983 hat das Bundesverfassungsgericht in einer Entscheidung - das "Recht auf informationelle Selbstbestimmung", um den Schutz der Privatsphäre - gerade vor dem Hintergrund moderner Datenverarbeitung - zu wahren.<sup>6</sup> Es verleiht dem Einzelnen das Grundrecht, grundsätzlich selbst zu bestimmen, wann und in welchem Umfang er persönliche Lebenssachverhalte preisgeben möchte. Das Recht auf informationelle Selbstbestimmung ist Bestandteil des allgemeinen Persönlichkeitsrechts, das durch Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG geschützt wird. Es genießt daher Verfassungsrang und ist wesentliche Ausprägung der Menschenwürde und der allgemeinen Handlungsfreiheit.

Wie auf europäischer Ebene, sind Einschränkungen dieses Rechts nur im überwiegenden Allgemeininteresse zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muss. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.

Bereits der derzeit gestaffelte Zugang zum Transparenzregister mit dem Begriff des berechtigten Interesses sind so weitreichend, dass auch irgendwie gearteter Bezug zu den Vortaten der Geldwäsche ausreicht. Aufgrund der vielen Relativierungen in der Gesetzbegründung („insbesondere“/ „etwa“) ist für wirtschaftlich Berechtigte daher zum jetzigen Zeitpunkt kaum übersehbar, wer auf ihre Daten Zugriff hat.

Das Regel-Ausnahme-Verhältnis wird durch einen öffentlichen Zugang nun vollends umgekehrt: Verdachtsmomente im Hinblick auf Geldwäsche, auffällige Konzernstrukturen oder der Einsatz von Briefkastenfirmen sind nicht erforderlich. Alle persönlichen Daten der wirtschaftlich Berechtigten würden vielmehr auf dem Präsentierteller ausgestellt werden.

Nichts Anderes gilt, wenn die Daten bereits in anderen Registern zugänglich sind. Denn die elektronische Zusammenfassung der bereits veröffentlichten Daten aus u.a. dem Handelsregister bewirken eine erhebliche eigene grundrechtliche Betroffenheit, weil neue Möglichkeiten der Datenverarbeitung geschaffen werden.<sup>7</sup> Die sich stetig erweiternde Technik setzt zahlreiche Daten „intelligent“ wie Mosaiksteine zusammen, um genaue Bilder der Betroffenen zu zeichnen. Diese Daten sind im Wettbewerb maßgeblich, insbesondere wenn ein Unternehmer in andere Branchen investiert, sein Geschäftsmodell verändert. Vielmehr noch, die erhebliche grundrechtliche Betroffenheit wird durch die modernen Verarbeitungs- und Verknüpfungsmöglichkeiten von Daten gesteigert. Profile, wie sie Unternehmen wie Google oder Amazon von Nutzern erstellen, veranschaulichen die Gefahren eindrucksvoll. Solche genauen Strukturen rechtsverbindlich zu ermöglichen widerspricht dem Schutzauftrag der öffentlichen Hand.

<sup>6</sup> BVerfGE 65,1 [41]

<sup>7</sup> BVerfG vom 21.06.2016 – 2 BvR 637/09

Der im Recht auf informationelle Selbstbestimmung innewohnende Anspruch, dass jedes Individuum entscheiden kann, welche Informationen es wem gegenüber wie preisgeben möchte, läuft nunmehr ins Leere.

Die öffentliche Hand darf nicht – hier laufen die Erwägungen parallel zum europäischen Recht – genaue öffentliche Bilder von Unternehmen ermöglichen. Es ist ihr untersagt, die ausdrücklich benannten erheblichen Gefahren der Betroffenen, Opfer eines Betrugs, einer Entführung, von Erpressung, Gewalt und Einschüchterung zu werden, dramatisch zu erhöhen. Zu einer durch das Transparenzregister angeleiteten Entführung darf es von vornherein nicht kommen. Das Register will die Kriminalität bekämpfen. In einer Öffnung für jedermann würde es dieser aber dienen.

Diese Bedenken wurden ausführlich im Rahmen der Gesetzgebung zur Umsetzung der 4. EU-Geldwäscherichtlinie von Sachverständigen vorgetragen und führten entsprechend zu dem beschränkten Zugang zum Register mit einem „berechtigten Interesse“. Auch die Bundesbeauftragte für den Datenschutz äußerte sich besorgt. Diese Argumente werden durch die Datenschutzgrundverordnung erheblich gestärkt.

## **Petition: Öffentlichen Zugang nicht umsetzen**

Die Öffnung des Transparenzregisters für jedermann verletzt die Grundrechte des Grundgesetzes, der EU-Grundrechtcharta und der EMRK. Diese Rechtsverstöße können nur vermieden werden, wenn von der Öffnung abgesehen wird.

## III. Mangelnde Schutzrechte

Der Rechtsbruch auf europäischer und nationaler Ebene würde zwar nicht verhindert, aber in seiner Intensität reduziert, wenn Schutzmaßnahmen und –rechte von wirtschaftlich Berechtigten im Transparenzregister umfassend erweitert werden.

### **1. Voraussetzungen für Schutzantrag gem. § 23 Abs. 2 GWG entschärfen**

Wirtschaftlich Berechtigte haben gem. § 23 Abs. 2 GWG die Möglichkeit eine Beschränkung der Einsichtnahme ihrer Daten zu beantragen, wenn ein schutzwürdiges Interesse aufgrund der Gefahr, Opfer einer Straftat zu werden besteht. Hierzu zählen Betrug, Entführung, Erpressung, Gewalt oder Einschüchterung. Die 5. EU-Geldwäscherichtlinie erweitert den Straftatkatalog um Schutzgelderpressung und Schikane, welches nicht ausdrücklich in dem vorliegenden Gesetzentwurf Erwähnung findet.

Obwohl die aufgezählten Straftaten veranschaulichen, welcher Gefahr sich der Familienunternehmer und seine Familienangehörigen aussetzen, wenn ihre personenbezogenen Daten öffentlich sind, wird ihnen der Schutzantrag in der Praxis versagt. Ungeklärt ist nämlich weiterhin, wie der genannte „wichtige Grund“ hinreichend

nachgewiesen werden soll und welches Ermessen der registerführenden Stelle – einem privatrechtsförmigen Träger als Beliehenen – zugebilligt wird.

So ist höchst fragwürdig, wann und wie einem Unternehmer der Nachweis schutzwürdigen Interesses gelingen soll. Denn eine konkrete Gefahr wird man nur belegen können, wenn man bereits Opfer einer Straftat geworden ist. So wird der wirtschaftlich Berechtigte in aller Regel keine Kenntnis von Tatsachen einer gegen ihn gerichteten Straftat erhalten, bevor ein potentieller Straftäter die Daten eingesehen hat. Das veranschaulichen auch aktuelle Zahlen: Bis zum 8. Oktober 2018 wurden 444 Anträge aufgrund schutzwürdigen Interesses gestellt, aber nur 32 rechtskräftig stattgegeben, 19 abgelehnt und 28 durch den Antragsteller zurückgenommen. Unklar ist bei den stattgegebenen Anträgen es sich allein um schutzwürdiges Interesse aufgrund von Minderjährigkeit handelt.

Hinsichtlich der Beurteilung eines Schutzantrags und dessen praktische Voraussetzung besteht insofern weiterhin erheblicher Klärungs- und Ausführungsbedarf.

Wenig hilfreich ist dabei, dass nun in der Gesetzesbegründung genannte Beispiel für eine Gefährdungssituation und einem entsprechenden Schutzbedürfnis bei „Vorliegen einer Sicherheitseinstufung vom LKA“.<sup>8</sup> Zunächst ist dieser Verweis irreführend, da nach Rücksprache mit einigen Landeskriminalämtern diese gar nicht für eine solche Sicherheitseinstufung zuständig wären, sondern die örtliche zuständige Polizeibehörde. Des Weiteren wird auch solch eine Prüfung nur bei akuter Gefährdungslage oder bereits erfolgter Bedrohung möglich sein. Dem Unternehmer wird also jegliche Präventivmaßnahme zur Beschränkung der Einsicht seiner Daten im Transparenzregister versagt.

Auch wenn der wirtschaftlich Berechtigte erfolgreich seine Daten beschränken könnte, müsste er zudem alle drei Jahre einen neuen Antrag stellen. Des Weiteren sind die Daten weiterhin auch Behörden und Verpflichteten anlasslos einsehbar.

Das datenschutzrechtliche Regel-Ausnahme-Verhältnis, nach dem Daten zu schützen sind, nur in besonderen Fällen anderen zugänglich und nur in absoluten Ausnahmefällen entgegen dem Willen des Betroffenen öffentlich gemacht werden, wird ausgehebelt. Dies ist mit der Vorgabe des EuGH in Sachen Vorratsdatenspeicherung, dass ein Zugriff auf personenbezogene Daten als Grundrechtseingriff auf das Notwendigste beschränkt sein muss, nicht vereinbar.<sup>9</sup>

Das Nachweisen eines schutzwürdigen Interesses gem. § 23 Abs. 2 GWG muss insofern erheblich vereinfacht werden um wirtschaftlich Berechtigten überhaupt die realistische Möglichkeit zu geben ihre personenbezogenen Daten vor Dritten zu schützen. Für eine großzügigere Ausnahmeregelung zu Gunsten des wirtschaftlichen Berechtigten spricht dabei schon, dass dessen schutzwürdigen Interessen ganz konkret im Einzelfall dargelegt werden müssen, das Einsichtnahmeinteresse von Jedermann dagegen vollkommen abstrakt und entsprechend wenig schutzwürdig ist. Wenn also niedrige Anforderungen an die

<sup>8</sup> Seite 91 des Gesetzentwurfs

<sup>9</sup> siehe Müller, Transparenz auf allen Ebenen, NZWiSt 2017, 87

Einsichtnahmen gestellt werden, sollten konsequenterweise auch geringe Voraussetzungen für die Darlegung eines schutzwürdigen Interesses gelten. Dies dürfte bei Familienunternehmern oder Begünstigten von Familienstiftungen regelmäßig schon dann der Fall sein, wenn aus dem Transparenzregisterauszug der Eindruck entstehen könnte, dass der wirtschaftlich Berechtigte über erhebliches Vermögen verfügt.

### **Petition: Auskunftssperre wegen Gefährdung gem. § 51 BMG als Beispiel für Schutzantrag gem. § 23 Abs. 2 GWG**

Als analoges Verfahren könnte die für Melderegister genutzte Auskunftssperre wegen Gefährdung gem. § 51 BMG (Bundesmeldegesetz) dienen. Eine solche bewirkt, dass einem Antrag auf Melderegisterauskunft zunächst nicht stattgegeben wird. Vielmehr erfolgt erst eine Anhörung des betroffenen Einwohners. Stellt sich bei dieser Anhörung heraus, dass eine Gefahr für den betroffenen Einwohner nicht ausgeschlossen werden kann, ist eine Melderegisterauskunft nicht zulässig und muss unterbleiben.

Der Gesetzesbegründung zu Nummer 20, Buchstabe a, Doppelbuchstabe bb, Absatz 2 (Seite 91), sollte folglich geändert werden: „Ein Schutzantrag nach § 23 Absatz 2 GwG ist erst bei Vorliegen konkreter Anhaltspunkte (z.B. Vorliegen einer Sicherheitseinstufung vom LKA oder Vorliegen einer Auskunftssperre wegen Gefährdung gem. § 51 BMG) möglich, sodass die Registrierungspflicht auch aus präventiven Gründen erforderlich ist.“

### **2. Meldungen in anderen Registern ausblenden**

In diesem Zuge sollte § 23 Abs. 2 S. 1 GWG ersatzlos gestrichen werden, nach dem ein schutzwürdiges Interesse grundsätzlich ausgeschlossen ist, wenn sich die Daten bereits aus einem anderen öffentlichen Register ergeben. Denn dies könnte wiederum gegen Datenschutzgrundsätze bzw. das Gebot der informationellen Selbstbestimmung verstoßen, da die Daten in den anderen Registern oftmals zu einem anderen Zweck eingeholt und veröffentlicht wurden. Nun entsteht eine Doppelung der Daten für einen anderen Zweck und Empfängerkreis.

So ist gerade das Handelsregister, auf das hier Bezug genommen wird, von Wesen und Zwecksetzung ein zwingend anderes als das Transparenzregister. Hier geht es nämlich um das Rechtsschutzbedürfnis des Einzelnen, der durch alltägliche Rechtsgeschäfte jederzeit in die Situation kommen kann, auf diese Auskunft zugreifen zu müssen. Kaufleute haben im Gegenzug regelmäßig ein Interesse daran, diese Daten zu pflegen und im Geschäftsverkehr aufzutreten. Das Informationsbedürfnis wird insofern aus dem Handelsregister bereits erfüllt. Dies wird zudem dadurch noch stärker deutlich, dass dem Transparenzregister ausdrücklich kein öffentlicher Glaube zugestanden wird und die Pflicht auf Richtigkeit vom Staat auf die wirtschaftlichen Berechtigten abgewälzt wird.

### **3. Rechtsbehelfe explizit regeln**

Obwohl die 5. EU-Geldwäscherichtlinie keine Änderungen hinsichtlich des Schutzes vorstellt, wird auf das Widerspruchsverfahren eingegangen: „Die Mitgliedstaaten stellen



sicher, dass diese Ausnahmen nach eingehender Bewertung der außergewöhnlichen Natur der Umstände gewährt werden. Rechte auf eine verwaltungsrechtliche Prüfung des Beschlusses über die Ausnahme und auf einen wirksamen Rechtsbehelf werden gewährt.“

Diese EU-Vorgabe findet im Gesetzentwurf keine Erwähnung. Dabei sollte explizit das Recht und Verfahren auf eine verwaltungsrechtliche Prüfung des Beschlusses über den Schutzantrag gem. § 23 Abs. 2 GWG sowie der wirksame Rechtsbehelf klar definiert werden. Auch dies würde die Schutzrechte des wirtschaftlichen Berechtigten aufwerten.

#### **4. Suchanfragen protokollieren, Gebühren und Registrierungspflicht beibehalten**

Um Missbrauchsgefahren zu minimieren, sind technische und organisatorische Maßnahmen für das Betreiben des Transparenzregisters und dem öffentlichen Zugang unumgänglich. Derzeit ist deshalb für die Einsichtnahme eine Registrierung mit einer E-Mail-Adresse und einem Nachweisdokument bezüglich der Person, der Institution, der Berufskategorie oder Gesellschaftsart notwendig. Natürliche Personen müssen an dieser Stelle obligatorisch zum Beispiel die Kopie des Personalausweises oder Reisepasses zur Identifizierung vorlegen. Es kann nur nach einzelnen Rechtseinheiten gesucht werden, nicht nach Privatpersonen oder ganzen Datensätzen. Pro Antrag wird eine Gebühr von 4,50 Euro erhoben.

Es bedarf auch weiterhin der Verifikation einer E-Mail-Adresse, indem ein Bestätigungslink versendet wird, der Angabe der Personalausweisnummer der Einsicht nehmenden Person und bei Unternehmen, die Einsicht nehmen würden, zusätzlich die Umsatzsteuer-identifikationsnummer abgefragt wird. Damit wird die Einsichtnahme in das Transparenzregister unter Vorspiegelung einer falschen Identität und so spätere Straftatenaufklärung erschwert. Zielführender wäre noch eine amtliche Identitätsprüfung, wenn man sich als Interessierter in das Register einloggt. Somit wird die Gefahr von „Fake Accounts“ reduziert.

Jede Suchanfrage sollte außerdem weiterhin protokolliert werden, um nachzuvollziehen, wer welche Daten eingesehen hat. Dies ist auch für mögliche spätere Strafverfolgungszwecke und Beweisführung nützlich, sollten die eingesehenen Daten missbraucht werden.

#### **5. Technische Voraussetzungen gesetzlich fixieren**

Entscheidend ist auch die strikte technische Umsetzung, nur nach der Organisation in dem Register gem. § 20 Abs. 1 GWG suchen zu können und nicht nach Namen oder anderen Merkmalen der natürlichen Personen. Denn ansonsten ergäben sich andere und weitaus umfassendere Einblicke in die Vermögenslage von Einzelpersonen und – aus Sicht eines Familienunternehmens – in die Vermögensverhältnisse der Unternehmerfamilie.

Insofern wäre auch eine ausdrückliche Klarstellung im Gesetz hilfreich, dass die Datensätze des Transparenzregisters in ihrer Gesamtheit nicht zum Download zur Verfügung stehen oder über automatisierte Abfragen über Programmierschnittstellen (API) bereitgestellt werden, einschließlich der hiermit einhergehenden Auswertungsmöglichkeiten.

## 6. Datenverarbeitung und Nutzung definieren und eingrenzen

Die EU-Richtlinie und der vorliegende Gesetzentwurf enthalten keinerlei Vorgaben zur weiteren Nutzung der Daten durch die Öffentlichkeit. Damit wird dem sogenannten „Crawling“ Tür und Tor geöffnet, in dem Daten aus dem Transparenzregister abgegriffen werden können und ohne notwendige Rechtsgrundlage auf anderen Portalen weiterverarbeitet und – ohne jegliche Schutzrechte des Betroffenen zu wahren - angeboten werden. Denn die personenbezogenen Daten haben erheblichen wirtschaftlichen Wert, so dass eine missbräuchliche Weiterverwendung als sehr naheliegend erscheint, welches insbesondere zu Wettbewerbsnachteilen von Familienunternehmen führen kann. Insofern ist zwingend gesetzgeberisches Handeln gefragt um zu klären, was mit den erlangten Daten (nicht) gemacht werden darf. Wichtig wäre auch der Hinweis, die Daten dürfen nicht frei und ohne jede Zweckbindung weiterverarbeitet werden.

## 7. Auskunftsrecht von wirtschaftlich Berechtigten einführen

Es ist unverständlich, warum es der registerführenden Stelle gem. § 23 Abs. 2 Satz 2 GWG-E sogar untersagt wird, den Gesellschaften mitteilen zu können, wer Einsicht in die Angaben genommen hat. Die EU-Richtlinie sieht gem. Artikel 1 Nummer 15 Buchstabe e eine solche Untersagung nur für zuständige Behörden und zentrale Meldestellen, aber gerade nicht für die Öffentlichkeit vor, wie es nun in der Gesetzesbegründung genannt wird. Damit wird wieder ein entscheidendes Schutz- und Datenschutzrecht des wirtschaftlich Berechtigten untergraben, denn es wird ihm verboten, herauszufinden, wer Einsicht in seine Daten genommen hat.

Gerade vor dem Hintergrund der mangelnden Verhältnismäßigkeit von Transparenz und Datenschutz wäre genau das Gegenteil nötig. Wenn bereits die Einsichtnehmenden registriert werden und Suchanfragen protokolliert, wäre es ein Leichtes, diese dem wirtschaftlich Berechtigten mindestens auf Anfrage (wenn nicht sogar automatisch) im Sinne der DSGVO zur Verfügung zu stellen.

## 8. Naming and shaming eindämmen

Ein Verstoß gegen die Mitteilungspflichten ist als Ordnungswidrigkeit bußgeldbewehrt. Die Geldbuße beträgt bis zu 1 Mio. Euro oder das Zweifache des aus dem Verstoß gezogenen wirtschaftlichen Vorteils, wenn es sich um einen schwerwiegenden, wiederholten oder systematischen Verstoß handelt. Gegenüber bestimmten Verpflichteten kann in diesen Fällen eine Geldbuße bis zu 5 Mio. Euro oder 10 Prozent des Jahresumsatzes verhängt werden. In den übrigen Fällen kann ein Bußgeld von bis zu 100.000 Euro verhängt werden. Diese Sanktionen sind nicht verhältnismäßig.

Diese Sanktionen werden öffentlich bekannt gemacht. In dieser Bekanntmachung sind Art und Charakter des Verstoßes und die für den Verstoß verantwortlichen Personen zu

benennen. Damit werden das staatliche Informationshandeln und die Gläsernmachung des Unternehmers unternehmerfeindlich abgerundet.

Die Geldbußen sollten auf die Mindestvorgaben der EU-Richtlinie zurückgestuft werden. Auch die Pranger Wirkung im Rahmen der Veröffentlichung von Bußgeldbescheiden sollte in diesem Zusammenhang relativiert werden. Die Bußgeldverfahren und Veröffentlichungen sollten sich weiterhin nur gegen die verpflichteten juristischen Personen richten.

## **9. Nationale Register nur bei einheitlichem Datenschutzstandard innerhalb der EU vernetzen**

Die nationalen Register in allen EU Mitgliedstaaten verursachen bereits ohne die zusätzliche öffentliche Transparenz einen immensen Austausch von persönlichen Daten. In Deutschland gibt es immer noch Zweifel an den nötigen Sicherheitsmaßnahmen der Registerbehörde, um die Daten ausreichend vor Missbrauch zu schützen oder um zu vermeiden, dass die falschen Daten übermittelt werden, bevor ein solcher Austausch überhaupt erfolgen sollte. Bevor es also zu einer angestrebten Vernetzung kommt, müssen diese Bedenken ausgeräumt werden.

Auch über die Grenzen hinweg scheint es noch viel größeren Umsetzungsbedarf zu geben, bevor überhaupt eine Verknüpfung der nationalen Register angedacht werden sollte. So sind in 20 Mitgliedstaaten die Register zu wirtschaftlich Berechtigten noch nicht eingeführt worden.<sup>10</sup> Damit ist auch unklar, wie dort Datenschutzstandards gewahrt werden sollen und Missbrauch vermieden.

---

<sup>10</sup> BT Drucksache 19/5354