55. Jahrgang / Oktober 2026 / Nr. 5

Der Gesellschafter

Zeitschrift für Gesellschafts- und Unternehmensrecht

Herausgegeben von
Nikolaus Arnold und Susanne Kalss

GesRZ

Manuel Steiner
Bemerkungen zur Kündigung in der GmbH

Eva Maria Baumgartner/Julia Auer-Mandahus
Zur Altersgrenze für Organe in einer Stiftungserklärung

Susanne Kalss
Führungsnachfolge und erbrechtliche Auswirkungen

Johannes Mitterecker
Wertabflussverbote bei M&A-Transaktionen

Aus der aktuellen Rechtsprechung
Entscheidungen von OGH und OLG
zum Gesellschafts- und Stiftungsrecht

Unternehmensrecht aktuell
Wichtige Gesetzesvorhaben im Überblick
Österreichische und europäische Finanzmarktaufsicht

Linde
www.lindeverlag.at

WiEReG 2027: Je mehr Daten, desto größer das Risiko

Das Register der wirtschaftlichen Eigentümer steht vor seinem bislang tiefgreifendsten Umbau. Den Anlass für die nunmehrige Neuordnung bildet das Geldwäschepaket der EU aus dem Jahr 2024. Die Verordnung (EU) 2024/1624 vom 31.5.2024 zur Verhinderung der Nutzung des Finanzsystems für Zwecke der Geldwäsche oder der Terrorismusfinanzierung, ABl L 2024/1624 vom 19.6.2024 (AMLR), regelt die Pflichten der Rechtsträger in Bezug auf ihr wirtschaftliches Eigentum erstmals unmittelbar anwendbar. Die Richtlinie (EU) 2024/1640 vom 31.5.2024, ABl L 2024/1640 vom 19.6.2024 (6. Geldwäsche-Richtlinie), enthält die Vorgaben für die Zentralregister. Der Nationalrat hat das Gesetz in der Fassung der Regierungsvorlage (RV 622 BlgNR 28. GP) unverändert beschlossen; die Befassung des Bundesrats und die Kundmachung stehen im Zeitpunkt der Drucklegung noch aus. Die Novelle des geltenden WiEReG (im Folgenden: WiEReG nF) soll mit 5.11.2026 in Kraft treten (§ 19 Abs 12 WiEReG nF). Mit 10.7.2027, dem Geltungsbeginn der AMLR, soll das WiEReG durch das Wirtschaftliche Eigentümer Registergesetz 2027 (WiEReG 2027) abgelöst werden (§§ 26 f WiEReG 2027; ErlRV 622 BlgNR 28. GP, 21).

§ 10 Abs 2 WiEReG nF enthält einen Katalog von zwölf Gruppen von Berechtigten, der im Wesentlichen Art 12 Abs 2 der 6. Geldwäsche-Richtlinie wiedergibt. Weitere Berechtigte kann der Bundesminister für Finanzen, wogegen durchaus verfassungsrechtliche Bedenken angebracht sind, durch Verordnung festlegen (ErlRV 622 BlgNR 28. GP, 3). Die Datenschutzbehörde (DSB) hat in der Begutachtung zum Ministerialentwurf zu Recht bezweifelt, ob eine solche Ermächtigung im Lichte der Rspr des VfGH zur Bestimmtheit von Eingriffsnormen (VfSlg 20.359/2019) ausreichend determiniert ist (*DSB*, Stellungnahme vom 21.4.2026, 2/SN-93/ME). Das beschlossene Gesetz hat den Wortlaut gegenüber dem Ministerialentwurf zwar an den bloß „fallweisen" Zugang nach Art 12 Abs 2 der 6. Geldwäsche-Richtlinie angeglichen, die Voraussetzungen, unter denen weitere Personenkreise Einsicht erhalten sollen, aber nicht näher bestimmt.

Geändert wird auch die Speicherdauer. Während die Daten eines wirtschaftlichen Eigentümers bisher zehn Jahre nach dem Ende seines wirtschaftlichen Eigentums nicht mehr zugänglich waren, werden sie künftig erst zehn Jahre nach der Beendigung des Rechtsträgers gelöscht (§ 7 Abs 3 WiEReG nF; § 9 Abs 7 WiEReG 2027). Die Materialien verweisen dafür lediglich auf nicht näher bezeichnete internationale Vorgaben (ErlRV 622 BlgNR 28. GP, 3). Art 10 Abs 20 der 6. Geldwäsche-Richtlinie knüpft zwar ebenfalls an die Beendigung des Rechtsträgers an, sieht aber vor, dass die Angaben fünf Jahre nach der Auflösung zugänglich bleiben. Eine weitere Aufbewahrung für höchstens fünf Jahre ist nur in konkreten Fällen zulässig, wenn deren Erforderlichkeit und Verhältnismäßigkeit festgestellt wurde; danach sind die personenbezogenen Daten zu löschen. Mit einer unterschiedslosen Speicherung für zehn Jahre ist das nur schwer vereinbar. Bezeichnenderweise ordnet § 18 Abs 13 WiEReG 2027, der nach den Materialien gerade Art 10 Abs 20 der 6. Geldwäsche-Richtlinie umsetzt (ErlRV 622 BlgNR 28. GP, 19), an, dass die übrigen Daten fünf Jahre nach der Beendigung des Rechtsträgers aufzubewahren und danach alle personenbezogenen Daten zu löschen sind. Wie sich dies zu § 9 Abs 7 WiEReG 2027 verhält, lässt das Gesetz offen. Der EuGH hat für Gesellschaftsregister zwar ein allgemeines Recht auf Löschung nach Zeitablauf verneint, die Prüfung der Frage der Löschung im Einzelfall aber den Mitgliedstaaten übertragen (EuGH 9.3.2017, Rs C-398/15, *Manni*). Für das Register der wirtschaftlichen Eigentümer hat der Unionsgesetzgeber die Löschung dagegen selbst vorgesehen.

Das WiEReG 2027 übernimmt sodann die Systematik der AMLR. Bei natürlichen Personen ohne Wohnsitz im Inland sind wie schon bisher Nummer und Art eines Ausweisdokuments zu melden und eine Kopie des Ausweisdokuments zu übermitteln (§ 6 Abs 1 Z 1 lit a WiEReG 2027; vgl ErlRV 622 BlgNR 28. GP, 16). Neu ist, dass bei Personen mit Wohnsitz im Inland Nummer, Art, Status und Gültigkeitsdauer des Ausweisdokuments automatisiert aus der Zentralen Evidenz nach § 22b Abs 4 PassG übernommen und laufend aktuell gehalten werden (§ 9 Abs 5 WiEReG 2027). Das Compliance-Package bleibt erhalten (§ 7 WiEReG 2027). Die Registerbehörde kann von Rechtsträgern Urkunden und Unterlagen verlangen, nunmehr auch solche zur Überprüfung der Mittelherkunft (§ 18 Abs 5 WiEReG 2027; ErlRV 622 BlgNR 28. GP, 18). Legt der Rechtsträger bei begründeten Hinweisen auf eine Sanktionssituation nicht binnen vier Wochen Nachweise für deren Nichtbestehen vor, ist dies im Register anzumerken (§ 10 Abs 3 WiEReG 2027). Die Anmerkung hat zwar keine unmittelbaren Rechtswirkungen (§ 10 Abs 6 WiEReG 2027), nach den Materialien, die ausdrücklich von einer Beweislastumkehr sprechen, aber *„nachteilige Auswirkungen im Geschäftsverkehr mit Verpflichteten"* (ErlRV 622 BlgNR 28. GP, 13); einer Beschwerde gegen den auf Antrag zu erlassenden Bescheid kommt keine aufschiebende Wirkung zu (§ 10 Abs 4 WiEReG 2027). Neu ist schließlich die Nachschau (§ 19 WiEReG 2027). Die Registerbehörde kann die Finanzpolizei beauftragen, Betriebsstätten und eingetragene Niederlassungen zu betreten und dies nach vorheriger Androhung mit unmittelbarer verwaltungsbehördlicher Befehls- und Zwangsgewalt durchzusetzen; dabei gelten Verhältnismäßigkeitsschranken und für Trustees aus rechtsberatenden Berufen besondere Schutzvorkehrungen (§ 19 Abs 3 und 6 WiEReG 2027). Die Nachschau ist bereits vor einem begründeten Verdacht möglich, Vorbild ist § 50 GSpG (ErlRV 622 BlgNR 28. GP, 19 f).

Die Speicherung der Ausweisnummer, die Einsicht in historische Daten und die Nachschaubefugnis als solche sind unionsrechtlich vorgegeben (Art 62 Abs 1 Unterabs 2 AMLR; Art 12 Abs 1 Unterabs 2 und Art 10 Abs 11 der 6. Geldwäsche-Richtlinie). Das bedeutet freilich noch nicht, dass sie auch grundrechtskonform sind. Bemerkenswert, wenn auch in Hinblick auf die Historie früherer Prüfungen nachvollziehbar, ist, dass der österreichische Gesetzgeber in wesentlichen Bereichen erheblich über das Unionsrecht hinausgeht. Die Empfehlungen 24 und 25 der FATF sollen *„vollinhaltlich umgesetzt werden, auch wenn*

dies bedeutet, dass über die Mindeststandards der 6. Geldwäsche-Richtlinie und Verordnung hinausgehende Vorschriften beibehalten oder erlassen werden müssen" (ErlRV 622 BlgNR 28. GP, 1). Der Österreichische Rechtsanwaltskammertag (ÖRAK) hat dieses Vorhaben als *„deutlich überschießend"* bezeichnet und gefordert, dass eine Überschreitung der unionsrechtlichen Regelungen ausreichend begründet wird; ein pauschaler Verweis auf Empfehlungen einer Task Force genüge nicht (*ÖRAK*, Stellungnahme vom 27.4.2026, 15/SN-93/ME). Diesem Programm folgen die flankierenden Sorgfaltspflichten der Rechtsträger (§ 3 WiEReG 2027; ErlRV 622 BlgNR 28. GP, 9) und die Pflicht der rechtlichen und wirtschaftlichen Eigentümer, auch Informationen bereitzustellen, die nach den Materialien *„über die Mindestanforderungen der Verordnung (EU) 2024/1624 hinausgehen"* (§ 4 WiEReG 2027; ErlRV 622 BlgNR 28. GP, 10). Beibehalten wird ferner die Pflicht, nach der jährlichen Überprüfung auch bei unveränderten Verhältnissen eine Bestätigungsmeldung abzugeben, die die Materialien nicht mit dem Unionsrecht, sondern mit dem andernfalls erforderlichen Personalaufwand der Registerbehörde begründen (§ 3 Abs 5 WiEReG 2027; ErlRV 622 BlgNR 28. GP, 10).

Das Register enthält schon heute nicht nur Stammdaten und Angaben zum wirtschaftlichen Eigentum, sondern bei Personen ohne Wohnsitz im Inland auch Ausweiskopien und, soweit Compliance-Packages übermittelt werden, die für die Feststellung und Überprüfung der wirtschaftlichen Eigentümer erforderlichen Dokumente. Bei Privatstiftungen zählen dazu die Stiftungsurkunde, die Stiftungszusatzurkunde und alle weiteren Nachweise, die für die Feststellung und Überprüfung aller Begünstigten notwendig sind (§ 5a WiEReG; § 7 Abs 1 Z 1 lit e WiEReG 2027). Die Stiftungszusatzurkunde, die nach § 10 Abs 2 PSG gerade nicht in die Urkundensammlung des Firmenbuchgerichts aufgenommen wird, liegt damit in einem zentralen Register, aus dem Verpflichtete die Dokumente eines gültigen Compliance-Packages einsehen und herunterladen können, sofern dieses nicht nur auf Anfrage zur Verfügung gestellt wird (§ 12 Abs 7 und 8 WiEReG 2027). Das WiEReG 2027 führt diese Dokumentensammlung fort und erweitert den Datenbestand um die laufend aktualisierten Ausweisdaten der Personen mit Wohnsitz im Inland, enthält allerdings auch Schutzvorkehrungen: Die mit einem Compliance-Package übermittelten Dokumente sind fünf Jahre nach ihrer Übermittlung zu löschen (§ 7 Abs 6 WiEReG 2027), bei berechtigten Gründen kann statt einer Urkunde ein vollständiger Aktenvermerk übermittelt werden (§ 7 Abs 3 WiEReG 2027) und die Zugriffsrechte sind abgestuft. Personen mit berechtigtem Interesse erhalten weder Ausweisdaten noch Ausweiskopien und keinen Zugang zu Compliance-Packages (§ 14 Abs 5 WiEReG 2027). Immerhin verlangt § 17 Abs 1 WiEReG 2027 bei Unstimmigkeitsmeldungen, anders als noch der Ministerialentwurf, keine Dokumente mehr; die Wirtschaftskammer hatte gerade mit Blick auf Stiftungs(zusatz)urkunden Bedenken erhoben (*WKÖ*, Stellungnahme vom 20.4.2026, 7/SN-93/ME, 4 f). Eine Datenschutz-Folgenabschätzung halten die Erläuterungen unter Berufung auf den Ausnahmegrund DSFA-A06 für nicht erforderlich, weil keine Daten iSd Art 9 und 10 DSGVO verarbeitet werden sollen (ErlRV 622 BlgNR 28. GP, 1 f). Gerade das hatte die DSB bezweifelt und eine neuerliche Prüfung angeregt (*DSB*, Stellungnahme vom 21.4.2026, 2/SN-93/ME, 2 f). Wie die Verarbeitung solcher Daten angesichts der übermittelbaren Dokumente und behördlichen Informationen praktisch ausgeschlossen werden soll, erläutern die Materialien nicht.

Dass zentrale Register zum Ziel von Angriffen werden, ist keine theoretische Gefahr. In der Nacht auf den 30.7.2026 verschaffte sich eine unbekannte Täterschaft Zugriff auf das liechtensteinische Verzeichnis der wirtschaftlich berechtigten Personen (VwbP) und griff Datenkopien zu rund 31.000 Rechtsträgern ab, darunter Personalien, Staatsangehörigkeit und Wohnsitzland der wirtschaftlich Berechtigten (*SRF* vom 2.8.2026). Als mögliches Einfallstor wurde in der Folge das Portal für die Erfassung von Einträgen in das Verzeichnis genannt; die Regierung sprach von einem Angriff *„auf hohem technischen Niveau auf eine hochkomplexe Sicherheitsstruktur"* (*SRF* vom 4.8.2026, Wirtschaftsdaten geklaut: Liechtenstein identifiziert mögliches Einfallstor für Hack). Abgeflossen ist damit nicht bloß eine Liste von Personalien, sondern die Information, wer hinter welcher Gesellschaft, Stiftung oder Treuhänderschaft steht.

Der jüngste Vorfall in Dänemark zeigt eine zweite Schwachstelle. Betroffen war dort nicht ein Register wirtschaftlicher Eigentümer, sondern das zentrale Personenregister CPR. Unter Missbrauch des rechtmäßigen Abfragezugangs eines dänischen Unternehmens verschafften sich Unbefugte Zugang zu Namen, Adressen und Personennummern von rund 8,8 Mio registrierten Personen; ausgenommen waren nur Personen mit Namens- und Adressschutz (Mitteilung der CPR-Verwaltung vom 5.10.2026). Ein Register ist demnach nur so sicher wie der am schwächsten gesicherte berechtigte Zugang. Das WiEReG vermittelt solche Zugänge einer großen Zahl von Verpflichteten, Behörden und Antragstellern. Die Pflicht der Verpflichteten, Zugangsdaten geheim zu halten (§ 12 Abs 7 WiEReG 2027), beantwortet aber noch nicht die Frage, ob Zugriffe technisch ausreichend begrenzt, überwacht und gegen Missbrauch abgesichert sind.

Je umfangreicher und aussagekräftiger die zentral gespeicherten personenbezogenen Daten sind, je länger sie aufbewahrt werden und je mehr Stellen auf sie zugreifen dürfen, desto größer ist das mögliche Schadensausmaß eines erfolgreichen Angriffs und desto höher der Schutzbedarf. Der EuGH hat bereits im Urteil *Luxembourg Business Registers* (EuGH 22.11.2022, verbundene Rs C-37/20 und C-601/20, *Luxembourg Business Registers*, Rn 43) hervorgehoben, dass die Folgen einer missbräuchlichen Verwendung dadurch verschärft werden, dass einmal zugänglich gemachte Daten gespeichert und weiterverbreitet werden können. Für ein Datenleck gilt dies in noch höherem Maß, denn es lässt sich nicht rückgängig machen. Der Gesetzgeber sollte daher die Grundsätze der Datenminimierung, der Speicherbegrenzung und der Vertraulichkeit berücksichtigen und Datenschutz-Folgenabschätzungen auch dann vornehmen, wenn er dazu nach eigener Ansicht (siehe allerdings die berechtigten Zweifel in der Stellungnahme der DSB) nicht zwingend verpflichtet sein mag. Transparenz ist ein legitimes Ziel der Geldwäscheprävention. Mit steigenden Offenlegungspflichten trifft den Staat aber auch eine besondere Verantwortung dafür, dass diese Daten nicht missbräuchlich verwendet werden können.

Wien, im Oktober 2026 *Nikolaus Arnold*