KÜNSTLICH
MENSCHLICH
INTELLIGENT
KOMPETENZZENTRUM

WHITEPAPER

KI und KI-Verordnung im Unternehmen

Ergebnisse der Online-Veranstaltung: „Den EU AI Act navigieren – Was müssen KMUs wissen?“ vom 12.02.2025

Das Forschungs- und Entwicklungsprojekt KMI wird im Rahmen der Fördermaßnahme „Zukunft der Arbeit: Regionale Kompetenzzentren der Arbeitsforschung – Künstliche Intelligenz" im Programm „Innovationen für die Produktion, Dienstleistung und Arbeit von morgen" des Bundesministeriums für Forschung, Technologie und Raumfahrt (BMFTR) für die Laufzeit vom 01.12.2021 – 30.11.2026 gefördert und vom Projektträger Karlsruhe (PTKA) betreut.

Gefördert durch:

Bundesministerium
für Forschung, Technologie
und Raumfahrt

Kompetenzzentren
Arbeitsforschung

Autorinnen und Autoren:
Stefan Schreiber[1]
Prof. Dr. Heralt Hug[1]
Maria Heider[2]
Christina Mamtoumidou[2]
Sabine Hartig[2]
Dr. Sebastian Schuhmann[2]

[1]CMS Hasche Sigle Partnerschaft von Rechtsanwälten und Steuerberatern mbB
[2]Institut für Angewandte Informatik e.V.

In Zusammenarbeit mit:
ACOD Automotive Cluster Ostdeutschland GmbH

August 2025

Die Inhalte dieser Veröffentlichung und der ihr zugrunde liegende Umsetzungsleitfaden dienen ausschließlich der allgemeinen Information und stellen keine Rechtsberatung dar. Das Kompetenzzentrum KMI übernimmt für die Richtigkeit und Vollständigkeit der Angaben keine Haftung. Die Veröffentlichung basiert auf der am 12. Juli 2024 im Amtsblatt der Europäischen Union publizierten Fassung der Verordnung (EU) 2024/1689.

CMS law·tax·future

KÜNSTLICH MENSCHLICH INTELLIGENT KOMPETENZZENTRUM

ACOD AUTOMOTIVE CLUSTER OSTDEUTSCHLAND

Inhaltsverzeichnis

1 Einleitung

Der EU AI Act, die europäische Verordnung über künstliche Intelligenz (KI), hat eine wichtige Bedeutung für nahezu alle Unternehmen, die Künstliche Intelligenz entwickeln, nutzen oder anpassen. Daher betrifft sie sowohl die Zielgruppe der Entwickler:innen als auch die der Nutzer:innen. Die neue KI-Verordnung hat das Ziel, die verantwortungsvolle Entwicklung und Verwendung von Künstlicher Intelligenz in der EU zu fördern. Dafür wurden gesetzlich Regelungen festgelegt, die von KI-Entwickler:innen und KI-Betreiber:innen zu beachten sind.

Dieses Paper soll die Veranstaltung „Den EU AI Act navigieren: Was müssen KMUs wissen?“ von Prof. Dr. Heralt Hug und Stefan Schreiber (CMS Deutschland) vom 12.02.2025 zusammenfassen und zudem einen Handlungsleitfaden für insb. kleine und mittelständische Unternehmen im Umgang mit Künstlicher Intelligenz bieten.

Im Vortrag wurden relevante Aspekte für Unternehmen im Umgang mit Künstlicher Intelligenz thematisiert. Die Grundlage dafür war die neue KI-Verordnung, die am 1. August 2024 in Kraft getreten ist. Im Zentrum der Betrachtung stand die Risikobewertung der KI-Systeme, die zugleich den Schwerpunkt der neuen KI-Verordnung bildet. Um eine genauere Risikoeinschätzung zu ermöglichen, werden KI-Anwendungen in verschiedene KI-Risikoklassen eingeteilt. Anhand dieser Einordnung wird für Unternehmen deutlich, welche Anforderungen auf sie zutreffen. Auch KI-Entwickler:innen und KI-Betreiber:innen können ihre Verantwortung leichter erkennen und wahrnehmen. Abschließend wurden einzelne Fallbeispiele diskutiert.

2 Handlungsleitfaden für Unternehmen auf Grundlage der KI-Verordnung

Der Handlungsleitfaden in diesem Paper orientiert sich am risikobasierten Ansatz der KI-Verordnung. Die darin definierten Risikoklassen werden unmittelbar mit den konkreten Auswirkungen auf Unternehmen sowie den daraus resultierenden Rechten und Pflichten verknüpft.

2.1 Anwendungsbereiche und Rollen der KI-Nutzung

Die KI-Verordnung regelt verschiedene Einsatzmöglichkeiten und Anwendungsbereiche, die Art und Weise der Nutzung sowie den Nutzungszweck von KI-Systemen. Dabei unterscheidet sie zwischen dem sachlichen Anwendungsbereich (was gilt als KI-System?) und dem persönlichen Anwendungsbereich (wer ist von den Gesetzen betroffen?). Wichtig für Unternehmen ist, dass sie in einem ersten Schritt feststellen, ob und inwieweit sie und ihre Anwendungsbereiche dort verordnet sind.

2.1.1 Sachlicher Anwendungsbereich

Der **sachliche Anwendungsbereich** definiert die KI als Gegenstand. Er wird nach Art. 3 Nr. 1 KI-VO folgendermaßen beschrieben:

- „Ein maschinengeschütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die physische oder virtuelle Umgebungen beeinflussen."
- Das bedeutet, dass die KI ein maschinenbasiertes System ist, das autonom arbeitet und bei Bedarf auch die Fähigkeit zur Anpassung besitzt.

Indem die KI-Eingaben (Input) verarbeitet, entstehen Ausgaben (Output).

2.1.2 Persönlicher Anwendungsbereich

Der **persönliche Anwendungsbereich** definiert dagegen die Adressat:innen der Regelungen und ist in Art. 3 Nr. 3 KI-VO und Art. 3 Nr. 4 KI-VO geregelt. Danach fallen unter den Geltungsbereich des Gesetzes alle natürlichen oder juristischen Personen, Unternehmen, Behörden und Einrichtungen.

Rollen bzgl. der Nutzung

Eng verknüpft mit dem persönlichen Anwendungsbereich ist die Art und Weise des Umgangs mit KI-Systemen. Unternehmen oder Personen können nach der KI-Verordnung entweder Anbieter:innen oder Betreiber:innen sein:

„Anbieter:in", Art. 3 Nr. 3 KI-VO

Anbieter:innen sind laut KI-VO Personen, die ein KI-System **entwickeln** oder **angepasst** haben und es im Unternehmen nutzen.

- „Natürliche oder juristische Personen, Behörden, Einrichtungen oder sonstige Stellen, die eine KI selbst entwickeln oder entwickeln lassen und diese unter ihrem eigenen Namen oder ihrer eigenen Marke in Verkehr bringen oder in Betrieb nehmen, egal ob entgeltlich oder unentgeltlich."
- Anbieter:in kann auch sein, wer ein KI-System erwirbt und wesentlich modifiziert (Art. 28 I lit. b) und c)).

„Betreiber:in", Art. 3 Nr. 4 KI-VO

Betreiber:innen sind laut KI-VO Mitarbeitende eines Unternehmens bzw. die Unternehmen selbst, die ein KI-System **verwenden**. In diesem Fall haftet das Unternehmen auch als Betreiber.

- „Jede natürliche oder juristische Person, Behörde, Einrichtung oder sonstige Stelle, die ein KI-System in eigener Verantwortung verwendet, es sei denn, das KI-System wird im Rahmen einer persönlichen und nicht beruflichen Tätigkeit verwendet“.

2.2 Die Risikoklassen des EU AI Acts - Einordnung und Auswirkungen für Unternehmen

Die Einordnung in Risikoklassen soll Unternehmen dabei helfen, ihre Rechte und Pflichten als Arbeitgeber:innen besser einzuschätzen, da diese von der potenziellen Gefahr durch die KI abhängen. Deshalb müssen Unternehmen die Risikoklasse ihrer KI-Systeme und sich daraus ergebende Pflichten frühzeitig feststellen.

Folgende vier Risikoklassen werden unterschieden:

- Inakzeptables Risiko (KI-Verbote)
- Hohes Risiko (Risikomanagement)
- Begrenztes Risiko (Hinweispflichten)
- Minimales Risiko (nicht geregelt in KI-VO)

Im Folgenden werden die vier Risikoklassen unter Nennung von Beispielen erläutert sowie Handlungsanweisungen vorgestellt, die sich daraus für Unternehmen ergeben (Abb. 1).

2.2.1 Inakzeptables Risiko

KI-Modelle mit einem inakzeptablen Risiko werden durch den AI Act in der EU verboten. Ein solches Risiko besteht, wenn KI-Systeme eine Bedrohung für Menschen darstellen, zum Beispiel in folgenden Fällen:

- Social Scoring.
- Unterschwellige Beeinflussung.

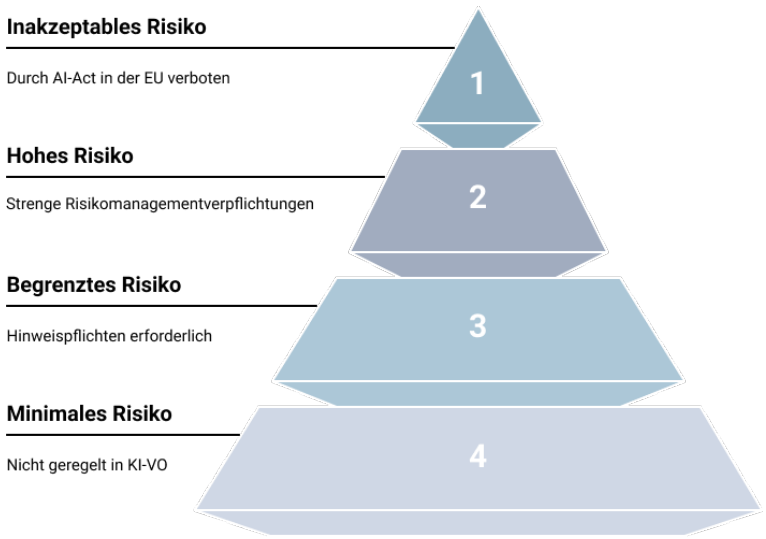

Abbildung 1: Die vier Risikoklassen des EU AI Acts

- Ausnutzung menschlicher Schwächen und Schutzbedürftigkeit.
- Biometrische Echtzeit-Identifizierung in öffentlichen Räumen.
- Emotionserkennung an Arbeitsplätzen und Bildungseinrichtungen.

2.2.2 Hohes Risiko

Bei KI-Systemen, die mit einem hohen Risiko eingestuft werden, können erhebliche Gefahren für Gesundheit, Sicherheit oder für die Grundrechte bestehen, weshalb sie strengen Verpflichtungen unterliegen.

Solche KI-Systeme können in folgenden Bereichen eingesetzt werden:

- Kritische Infrastruktur
- Allgemeine und berufliche Bildung oder Beschäftigung.
- Gesundheits- oder Bankwesen.
- Private und öffentliche Dienstleistungen und Sozialleistungen.
- Strafverfolgung, Justizverwaltung, Grenzverwaltung.

Konkrete Beispiele für Hochrisikosysteme sind folgende:

- KI-Systeme, die als Sicherheitskomponenten eingesetzt werden, z.B. in medizinischen Geräten, Fahrzeugen, Aufzügen.
- KI-Systeme, die zur biometrischen Identifizierung von Personen und Emotionserkennung weder in der Öffentlichkeit noch am Arbeitsplatz oder in Bildungseinrichtungen eingesetzt werden.
- KI-Sicherheitskomponenten in kritischen Infrastrukturen (z.B. Straßenverkehr oder Grundversorgung), deren Ausfall das Leben und die Gesundheit der Bürger:innen gefährden könnte.
- KI-Tools für die Beschäftigung, das Management von Arbeitnehmern und den Zugang zur Selbstständigkeit (z.B. CV-Sortierungssoftware für die Einstellung).

Auswirkungen für Unternehmen:

Laut Art. 8 bis Art. 15 KI-VO müssen folgende Anforderungen an Hochrisikosysteme eingehalten werden:

- Einrichtung eines Systems zur Einschätzung und Verhütung von Risiken (Art. 9 KI-VO).
- Erfüllung von Qualitätsstandards in Bezug auf Trainings-Verteidigungs- und Testdatensätzen (Art. 10 KI-VO).
- Technische Dokumentation (Art. 11 KI-VO) und Aufzeichnungspflichten (Art. 12 KI-VO).
- Transparenz und Informationspflichten (Art. 13 KI-VO).
- Sicherstellung menschlicher Aufsicht (Art. 14 KI-VO).
- Erfüllung von Genauigkeit, Robustheit und Cybersicherheit (Art. 15 KI-VO).

Anbieter:innen von Hochrisikosystemen müssen nach Art. 16 KI-VO folgende Anforderungen einhalten:

- Anbringung von Namen und Kontaktanschrift.
- Qualitätsmanagementsystem (Art. 17 KI-VO).
- Aufbewahrung von Unterlagen und Protokollen (Art. 18, 19 KI-VO).
- Durchführung eines Konformitätsbewertungsverfahrens vor dem Inverkehrbringen (Art. 43 KI-VO).
- Ausstellung einer EU-Konformitätserklärung und Anbringung der CE-Kennzeichnung (Art. 47, 48 KI-VO).
- Registrierung in einer EU-Datenbank (Art. 49 KI-VO).
- Informations- und Korrekturpflichten bei Feststellung von Nichtkonformität des Systems (Art. 20 KI-VO).
- Kooperation mit Behörden, Erfüllung der Barrierefreiheitsanforderungen.
- „Pflichtenfalle“: Übergang der Anbieterpflichten auf andere Personen, wie Händler und Betreiber (Art. 25 KI-VO).

Betreiber:innen haben nach Art. 26 KI-VO folgende Verpflichtungen:

- Sicherstellung durch technische und organisatorische Maßnahmen (TOMs), dass das System entsprechend seiner Betriebsanleitung verwendet wird.
- Sicherstellung einer menschlichen Aufsicht durch eine geschulte Person.
- Sicherstellung, dass Eingabedaten der Zweckbestimmung des Systems entsprechen und repräsentativ sind.
- Überwachen des Betriebs des KI-Systems anhand dessen Betriebsanleitung und ggf. Unterrichtung der Anbieter:in.
- Aufbewahrung der Protokolle für mindestens sechs Monate.
- Arbeitgeber:innen müssen Arbeitnehmer:innen beim Einsatz eines solchen Systems im Unternehmen im Voraus informieren.
- Informieren von Betroffenen, wenn ihnen gegenüber der Einsatz eines

solchen Systems geplant ist, welches Entscheidungen über natürliche Personen trifft oder dabei zumindest unterstützt.

Zulieferungsunternehmen bzw. Dritte, die ein KI-System, Instrumente, Dienste, Komponenten von Verfahren bereitstellen, die für bzw. in ein Hochrisiko-KI-System verwendet oder integriert werden, haben die Pflicht, eine schriftliche Vereinbarung mit dem oder der Anbieter:in zu schließen.

2.2.3 Begrenztes Risiko

Unter KI-Systeme mit einem begrenzten Risiko fallen all jene Systeme, die kein inakzeptables oder hohes Risiko darstellen. Dazu zählen zum Beispiel:

- Chatbots
- Suchalgorithmen

Auswirkungen für Unternehmen:

- Entwicklung und Verwendung unter Einhaltung von Transparenz- und Informationspflichten möglich.

2.2.4 Minimales Risiko

KI-Systeme mit minimalem Risiko sind nicht im EU AI Act geregelt, da es für diese keine bzw. nur sehr geringe Anforderungen gibt. Beispiele hierfür sind:

- Anwendungen wie KI-fähige Videospiele oder Spamfilter.

Auswirkungen für Unternehmen:

- Optional: Schulungen und/oder Code of Conduct.

2.3 Fristen für die Umsetzung im Unternehmen

In der KI-Verordnung sind zeitlich gestaffelte Umsetzungsfristen für die unterschiedlichen Anforderungen vorgesehen, welche im Folgenden aufgelistet

werden:

2025:

- 2. Februar 2025: Verbote gelten nach sechs Monaten.
- 2. Februar 2025: Schulungspflicht für Unternehmen, die KI-Systeme nutzen (z.B. Microsoft Co-Pilot, ChatGPT).
- 2. August 2025: Governance-Regeln und die Verpflichtungen für KI-Modelle mit allgemeinem Verwendungszweck gelten nach zwölf Monaten.

2026:

- 2. August 2026: Für die meisten Regelungen, einschließlich für Hochrisiko-KI: 24 Monate nach Inkrafttreten der KI-VO.

2027:

- 2. August 2027: Für Hochrisiko-KI-Systeme, die in regulierte Produkte eingebettet sind, gilt eine 36-monatige Umsetzungsfrist.

3 Hinweise und Empfehlungen zur Umsetzung in der Unternehmerischen Praxis

Auch wenn derzeit viele Details, etwa zur konkreten Auslegung der Vorschriften oder zur zuständigen Kontrollinstanz (z.B. Bundesnetzagentur in Deutschland), noch nicht abschließend geklärt sind, empfiehlt es sich, bereits jetzt aktiv zu werden. Frühzeitige und proaktiv eingeleitete Maßnahmen schaffen Rechts- und Handlungssicherheit, fördern organisatorischen Wandel und können perspektivisch sogar einen Wettbewerbsvorteil verschaffen. Um den

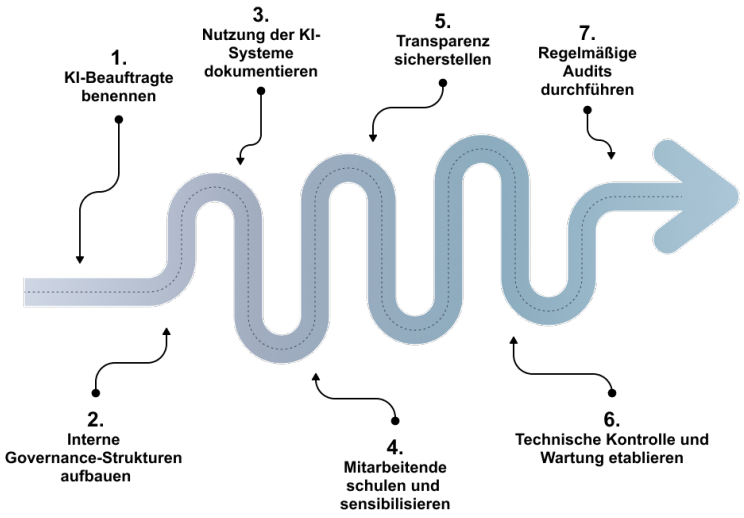

Abbildung 2: Orientierung für KI-Compliance

Unternehmen eine Orientierung für den Umgang mit KI-Systemen zu geben, werden im Folgenden zentrale Handlungsfelder benannt (Abb. 2).

Gerade für kleine und mittlere Unternehmen (KMUs) plant die Europäische Kommission vereinfachte Dokumentationsformulare, regulatorische Sandkästen für erprobende Anwendungen sowie reduzierte Anforderungen, um die Umsetzungskosten möglichst gering zu halten.

Dennoch bleibt für KMUs entscheidend, eine verantwortliche Instanz im Unternehmen zu benennen, z.B. einen KI-Beauftragten, der/die kontinuierlich den Überblick über regulatorische Neuerungen behält und regelmäßig interne Audits sowie Anpassungen der eingesetzten Systeme an neue Vorgaben anstößt.

Unterstützend wirkt der Aufbau einer internen KI-Governance-Struktur, die Zuständigkeiten und Prozesse definiert und verbindliche Regelungen verankert.

Alle Mitarbeitenden, die KI-Systeme nutzen, sollten dementsprechend ge-

schult werden und Einweisungen zu technischen Aspekten, rechtlichen Anforderungen und zur möglichen Risikoerkennung erhalten.

Wie auch bei anderen Arbeitsmitteln ist die Bereitstellung von verständlichen Bedienungsanleitungen sowie die regelmäßige Kontrolle und Wartung entscheidend, um KI-Systeme sicher in Unternehmen einzusetzen.

Außerdem soll die Transparenz und die Dokumentation bei der Nutzung von KI in Unternehmen bedacht werden. Entscheidungen und Prozesse von KI-Systemen sowie die Kommunikation mit einer KI für Mitarbeitende sollten stets nachvollziehbar sein. Unternehmen sollten dementsprechend die Nutzung jedes KI-Systems sorgfältig dokumentieren, insbesondere im Hinblick auf Zweck, Funktion, verwendete Datenquellen, Testergebnisse und getroffene Risikomanagementmaßnahmen. Dies ermöglicht sowohl die interne Nachvollziehbarkeit im Umgang mit KI-Systemen als auch eine rechtssichere Vorlage gegenüber Aufsichtsbehörden im Falle einer Kontrolle. Praxisnahe Hilfsmittel wie Checklisten und Musterprotokolle können den Mitarbeitenden hierfür bereitgestellt werden, um Orientierung zu bieten und so die Qualität und Vollständigkeit der Dokumentation zu sichern.

4 Schlusswort

Während bestimmte Einsatzbereiche, wie etwa die automatisierte Bilderkennung in der Qualitätskontrolle, als unstrittig gelten, bleibt der Umgang mit generativer KI rechtlich herausfordernd. Viele Detailfragen, mit zum Teil hoher Praxisrelevanz für Unternehmen, werden wohl erst perspektivisch in den nächsten Jahren durch gerichtliche Entscheidungen konkretisiert werden.

Genau deshalb ist es für Unternehmen ratsam, bereits jetzt erste strukturelle und organisatorische Maßnahmen zu ergreifen. Diese sollten als iterativer

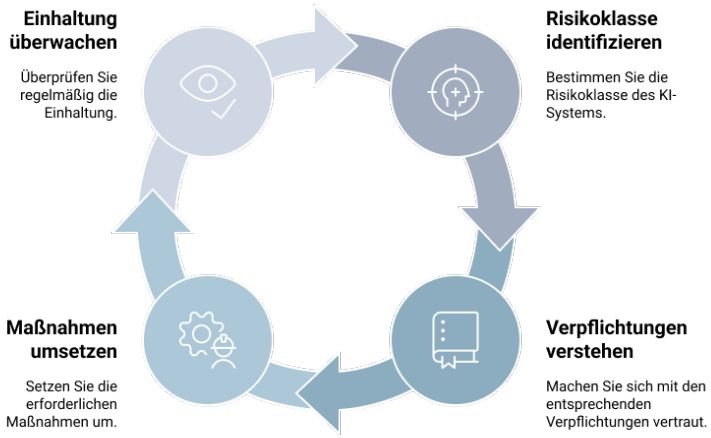

Abbildung 3: Zyklus der Risikobewertung und -einhaltung.

Prozess verstanden werden, der regelmäßig überprüft und angepasst wird (Abb. 3). Wer proaktiv und frühzeitig Verantwortung, Prozesse und Kompetenzen im Umgang mit KI-Systemen etabliert, schafft nicht nur die Grundlage für rechtskonformes Handeln, sondern befähigt auch Mitarbeitende, KI sicher und verantwortungsvoll einzusetzen. Ein menschzentrierter und vorausschauender Umgang mit den neuen Anforderungen stärkt das Vertrauen innerhalb der Organisation, die Resilienz gegenüber regulatorischen Veränderungen und kann langfristig als klarer Wettbewerbsvorteil wirken.

5 Weiterführende Links

European Union. (2024). Verordnung über künstliche Intelligenz. https://eur-lex.europa.eu/eli/reg/2024/1689/oj Zugriff: 15.05.2025

6 Impressum

Kompetenzzentrum KMI
Dr. Christian Zinke-Wehlmann (Leiter)

Institut für Angewandte Informatik (InfAI) e. V.
Goerdelerring 9
04109 Leipzig

Telefon: +49 341 229037 0
Telefax: +49 341 229037 99
E-Mail: info@infai.org

Vertretungsberechtigter Vorstand:
Prof. Dr. Bogdan Franczyk (1. Vorsitzender)
Prof. Dr. Erhard Rahm (2. Vorsitzender)
Prof. Dr. André Ludwig
Prof. Dr. Roland Fassauer

Vorstandsbeisitzer:
Prof. Dr. Sören Auer
Prof. Dr. Gerhard Heyer
Prof. Dr. Gerik Scheuermann

Geschäftsführung:
Ingolf Römer, Andreas Heinecke, Prof. Dr. Roland Fassauer

Registereintrag:
Registergericht: Amtsgericht Leipzig
Registernummer: VR 4342

Umsatzsteuer-ID:
Umsatzsteuer-Identifikationsnummer nach §27a
Umsatzsteuergesetz: DE274344504