Newsletter August 2026
Knyrim Trieb Rechtsanwälte OG

Sehr geehrte Damen und Herren!
Liebe Datenschutzinteressierte!

Unser aktueller Newsletter bietet Ihnen Wissenswertes zu Cybersecurity, KI-Transparenzpflichten, Missbräuchlichkeit von Auskunftsbegehren und zur höchsten DSGVO-Strafe Österreichs. Darüber hinaus informieren wir Sie über unsere Publikationen, geben einen Ausblick auf einen spannenden Seminar- und Tagungs-Herbst 2026 und freuen uns über Ranking-Erfolge!

NISG 2026 – Cybersecurity neu

Beitrag verfasst von Mag. Gregor Brandstetter, BA – KTR-Newsletter August 2026

Bald ist es soweit: Das **Zeitfenster zur Registrierung „wichtiger" und „wesentlicher" Einrichtungen iSd NISG 2026**, der Umsetzung der NIS-2-Richtlinie in österreichisches Recht, **öffnet sich am 1.10.2026**. Zahlreiche andere Pflichten sind innerhalb bestimmter Fristen ab der Registrierung zu erfüllen. Wir wollen Ihnen im Folgenden einen Überblick geben.

Die wichtigste Frage für Unternehmen und Organisationen in Bezug auf das neue „Sicherheitspaket" (neben dem Netz- und Informationssystemsicherheitsgesetz 2026 (NISG 2026) sind vor allem noch das Resilienz kritischer Einrichtungen-Gesetz (RKEG) und die Verordnung (EU) 2022/2554 über die digitale operationale Resilienz im Finanzsektor (DORA) für Unternehmen beachtlich) ist, ob der (jeweilige) **Anwendungsbereich** eröffnet ist. Dazu sind für das NISG 2026 zwei voneinander getrennte Fragen zu klären:

- Werden bestimmte Schwellenwerte in Bezug auf die Unternehmensgröße überschritten?
- Erbringt das Unternehmen Dienste in einem relevanten Sektor?

Beide Fragen sind bei näherer Betrachtung komplexer, als es auf den ersten Blick scheint. Unsere Beratungspraxis hat gezeigt, dass insbesondere Konzernstrukturen Probleme bei der Beurteilung der Schwellenwerte schaffen und die Grenzen der erfassten Sektoren durch zahlreiche Verweise auf Spezialgesetze schwer zu bestimmen sind. Hinzu kommt, dass bestimmte Aspekte iZm dem Anwendungsbereich des NISG 2026 auch unionsrechtskonform auszulegen sind.

Beachten Sie bei Ermittlung der **Unternehmensgröße** jedenfalls die Zurechnungsregeln der „KMU-Empfehlung" (2003/361/EG). Kennzahlen verbundener Unternehmen sind voll zuzurechnen, jene von

Partnerunternehmen anteilig. Ziehen Sie zur Beurteilung der **Sektoren** Experten hinzu. Beachten Sie, dass die Richtlinie selbst Verweise auf anderes Unionsrecht enthält. Besonders schwierig sind dabei Verweise auf nationales Recht, das bestimmte EU-Richtlinien umsetzt. So verweist die NIS-2-Richtlinie etwa auf die Elektrizitätsbinnenmarktrichtlinie (2019/944), die in Österreich mit dem ElWG umgesetzt wurde. Im NISG 2026 wird aber leider auf das außer Kraft getretene Vorgängergesetz, das ElWOG, verwiesen.

Kommen Sie zu dem Ergebnis, dass Ihr Unternehmen dem NISG 2026 unterliegt, sind folgende Pflichten einzuhalten:

Registrieren Sie Ihr Unternehmen: Die Registrierung hat **bis zum 1.1.2027 im Unternehmensserviceportal (USP)** zu erfolgen. Dabei sind u.a. Angaben zum Sektor zu machen, innerhalb dessen Ihr Unternehmen Dienste erbringt. Auch Änderungen der Registrierungsdaten sind zu melden.

Klären Sie die Verantwortlichkeit des **Leitungsorgans**: Die explizite Verpflichtung der Leitung, zumeist Geschäftsführung oder Vorstand, Schulungen zu besuchen und die Einhaltung der Risikomanagementmaßnahmen sicherzustellen, ist ein Paradigmenwechsel. Zwar hat sich der österreichische Gesetzgeber gegen eigene Verwaltungsstrafen für Leitungsorgane entschieden, insbesondere sind aber Regressansprüche der Gesellschaft gegen Leitungsorgane nicht ausgeschlossen.

Treffen Sie **Risikomanagementmaßnahmen**: Der „harte Kern" an Pflichten in Bezug auf die Netz- und Informationssicherheit bleibt bestehen. Analysieren Sie die Risiken für Ihr Unternehmen und treffen Sie geeignete und angemessene Abhilfemaßnahmen. Beachten Sie dabei die Durchführungsverordnung 2024/2690 und eine allenfalls künftige NIS-Verordnung. Hinsichtlich der umgesetzten Maßnahmen bestehen auch Nachweispflichten.

Melden Sie **Vorfälle**: Kommt es zu Cybersicherheitsvorfällen, muss Ihr Unternehmen ausreichend vorbereitet sein, um **innerhalb der kurzen Frist von bloß 24 Stunden eine Meldung an die Cybersicherheitsbehörde zu erstatten**. Zur Vorbereitung gehört es auch, ein entsprechendes Monitoring relevanter Bereiche eingerichtet zu haben. Wieder sind sektorspezifische Regelungen in der Durchführungsverordnung 2024/2690 zu finden.

Dokumentieren Sie ihre Compliance und überprüfen Sie diese regelmäßig.

Beachten Sie zuletzt, dass die Pflichten des NISG 2026 auf vielfältigste Weise mit anderen Rechtsakten in Verbindung stehen. Prüfen Sie, ob auch die Anwendbarkeit des **RKEG** oder von **DORA** möglich ist. Vergleichen Sie bisher erlangte Zertifizierungen, v.a. nach ISO 27001, mit den nun umzusetzenden Maßnahmen.

Unsere Erfahrung zeigt: Die „Anlaufkosten" sind nicht unerheblich, aber jeder abgewehrte Angriff spart ein Vielfaches an Geld und Ressourcen. Bedenken Sie, dass Angreifer zunehmend auf den Einsatz von KI setzen. Schwachstellen und Angriffsziele können dadurch automatisiert aufgespürt werden. Cybersecurity ist damit lange nicht mehr nur „teures Papier", sondern die **Sicherung der Betriebsfähigkeit des Unternehmens!**

Transparenzpflichten der KI-Verordnung und zugehöriger Verhaltenskodex

Beitrag verfasst von Dr. Rainer Knyrim und Jakob Brunbauer – KTR-Newsletter August 2026

Seit dem 2.8.2026 sind die **Transparenzpflichten der KI-Verordnung** (AI Act), insbesondere jene des **Artikel 50 AI Act, anzuwenden**, die wir nachstehend erklären. Des Weiteren geben wir Ihnen einen Überblick zum **Code of Practice on Transparency of AI-Generated Content** (Verhaltenskodex), den die Europäische Kommission (EK) am 10.6.2026 als freiwilligen Verhaltenskodex veröffentlicht hat.

Für **Nutzer:innen** wird es zunehmend schwieriger, zwischen menschlichen und KI-generierten **Inhalten** zu unterscheiden. Besonders sogenannte **Deepfakes** – nach Art 3 Z 60 AI Act durch KI erzeugte oder manipulierte Bild-, Ton- oder Videoinhalte, die wirklichen Personen, Gegenständen oder Ereignissen ähneln – erschweren die Differenzierung, wobei hier bereits die Gefahr der **Annahme**, das Dargestellte würde real existieren, genügt, um als Deepfake zu gelten.

Die EU hat bereits im Jahr 2023 die **Transparenzpflichten** des Art 50 AI Act beschlossen, die aufgrund des stufenweisen Inkrafttretens der Verordnung nun im August **verbindlich** wurden.

Art 50 AI Act normiert in Abs 2 **Pflichten**, welche spezifisch die **Anbieter** – nach Art 3 Z 3 AI Act also jede natürliche bzw. juristische Person, die ein KI-System zu allgemeinem Verwendungszweck entwickelt oder entwickeln lässt, und dieses unter eigenem Namen in Verkehr bringt bzw. in Betrieb nimmt – treffen. In Art 50 Abs 4 sind die Pflichten geregelt, die die **Betreiber** – nach Art 3 Z 4 AI Act also jede natürliche bzw. juristische Person, die ein KI-System in eigener Verantwortung verwendet (es sei denn, die Verwendung erfolgt im Rahmen einer privaten, nicht beruflichen Tätigkeit) – zu erfüllen haben. Abs 5 normiert weiters Pflichten, die **allgemein** – also sowohl von Betreibern als auch Anbietern – zu erfüllen sind.

Der **Verhaltenskodex** folgt dieser zweigliedrigen Struktur und konkretisiert die Vorgaben für die Praxis: In Abschnitt 1 werden die Regeln für die Kennzeichnung und Erkennung von KI-generierten und manipulierten Inhalten für Anbieter generativer KI behandelt und in Abschnitt 2 die Kennzeichnungspflichten für die Betreiber, speziell im Hinblick auf Deepfakes sowie bestimmte KI-generierte oder manipulierte Texte.

Seit 2.8.2026 müssen Anbieter ihre **KI-generierten Audio-, Bild-, Text- oder Videoinhalte mit maschinenlesbaren Kennzeichen** versehen, wobei diese Zeichen nur dann verwendet werden müssen, wenn ein KI-System die Hauptfunktion der Aufgabe erfüllt, z.B. wenn jemand einen Arbeitsleitfaden mit KI generiert. Erfüllt das KI-System nur eine Nebenaufgabe, z.B. die Rechtschreibkorrektur des Arbeitsleitfadens, ist grundsätzlich keine Kennzeichnung nötig. Hier nennt der Code of Practice allerdings keine konkreten Ansätze, wie diese Differenzierung durch Anbieter umzusetzen ist.

Art 50 Abs 2 AI Act legt fest, dass die Kennzeichen für KI-generierte und KI-modifizierte Inhalte **wirksam, interoperabel, belastbar und zuverlässig** sein müssen. Nachdem dies von einer einzelnen Art der Kennzeichnung – z.B. einem Wasserzeichen – im Moment noch nicht vollumfänglich erfüllt werden kann, muss unter Umständen auf einen **mehrschichtigen Kennzeichnungsprozess**, also eine Kombination aus mehreren Kennzeichen, zurückgegriffen werden. Technisch bewerkstelligt man die Lesbarkeit durch den Menschen beispielsweise durch Wasserzeichen und die Maschinenlesbarkeit durch Metadaten, die hinter die Datei gelegt werden. Diese Metadaten können dann von, ebenfalls vom Anbieter bereitgestellten, Anwendungen ausgelesen werden und so die KI-Generierung bestätigen. Allerdings gibt es hier im Moment kein „All-in-One-Modell“, mit dem man alle Outputs von allen KI-Modellen am Markt nachprüfen könnte. Vielmehr kann im Moment z.B. ein von Google Gemini kreiertes Bild nur mit dem Google-Nachweismodell SynthID als KI-generiert erkannt werden.

Dies führt zu erheblichen Problemen in der **Nachweisbarkeit**, sollen doch die Anbieter gemäß Verhaltenskodex **jedermann in die Lage versetzen**, Inhalte prüfen zu können.

Die Anbieterpflichten des Art 50 Abs 2 AI Act gehen aber noch weiter, sodass in den **Nutzungsbedingungen** der Anbieter das Entfernen der technischen Wasserzeichen und Metadaten, etwa in der weiteren Wertschöpfungskette, ausgeschlossen werden muss. Dadurch impliziert die Konkretisierung des Verhaltenskodex plötzlich **Betreiberpflichten** und unter Umständen sogar Pflichten für den Endnutzer, welche im AI Act nicht explizit enthalten sind.

Im Hinblick auf die Betreiberpflichten nach Art 50 Abs 4 AI Act sind **Deepfakes vom Betreiber in menschenlesbarer, wahrnehmbarer Form zu kennzeichnen**. Es wird vom Betreiber somit im Gegensatz zur Anbieterpflicht nach Art 50 Abs 2 AI Act **keine maschinenlesbare Kennzeichnung** verlangt. Der Code of Practice schlägt hierfür eigens vom AI Office der EK entworfene **Icons**, die in mehreren Varianten zum Download zur Verfügung stehen, als Kennzeichnung vor (https://digital-strategy.ec.europa.eu/en/policies/eu-icons-labelling-ai-generated-content). Die Kennzeichnungspflicht ist weiters so beschränkt, dass sie, sollte es sich um ein künstlerisches Werk handeln, den Genuss desselben nicht stört. Daneben gibt es eine weitere Ausnahme für **Texte zur Information der Öffentlichkeit**. Diese müssen zwar grundsätzlich auch gekennzeichnet werden, wenn sie mit KI generiert werden. Dies gilt aber nicht, wenn diese von einem Menschen redaktionell Korrektur gelesen werden, dann sind sie zur Gänze nicht kennzeichnungspflichtig.

Fazit: Die nun in Kraft getretenen Transparenzpflichten des Art 50 AI Act und der kurz davor veröffentlichte Verhaltenskodex stellen einen wichtigen Schritt in Richtung transparenter Nutzung und Datenverarbeitung von KI-generierten Inhalten dar. **Für Betreiber ist es aktuell wichtig, beim Einsatz von KI-Systemen zu prüfen, inwieweit der jeweilige Anbieter die Transparenzpflichten bereits umgesetzt hat.**

Wann kann ein Auskunftsbegehren nach aktueller Judikatur wegen Missbräuchlichkeit abgelehnt werden?

Beitrag verfasst von Jennifer Salomon, LL.M. – KTR-Newsletter August 2026

Das Recht auf Auskunft nach Art 15 DSGVO ist der „Klassiker" unter den Betroffenenrechten- und zugleich häufiger Anlass für Streitigkeiten in der Praxis. Es soll betroffenen Personen die Überprüfung der Rechtmäßigkeit der Verarbeitung ihrer personenbezogenen Daten sowie ggf. die Geltendmachung weiterer Rechte ermöglichen. Das Recht auf Auskunft ist jedoch kein uneingeschränktes Recht.

Bei **offenkundig unbegründeten** oder – insbesondere im Fall häufiger Wiederholung – **exzessiven Anträgen** einer betroffenen Person kann der Verantwortliche gemäß Art 12 Abs 5 DSGVO entweder ein **angemessenes Entgelt** verlangen oder **sich weigern**, aufgrund des Antrags **tätig zu werden**, wobei der Verantwortliche für diese Missbrauchsabsicht der betroffenen Person beweispflichtig ist. Diese Bestimmung unterstreicht die generelle Judikatur des EuGH, wonach sich der Einzelne nicht in betrügerischer oder missbräuchlicher Weise auf unionsrechtliche Normen berufen darf. Grenze des Auskunftsbegehren ist daher die „**Missbräuchlichkeit**" des Auskunftsbegehrens.

Der EuGH hat 2023 klargestellt: Ein Auskunftsbegehren **muss nicht begründet** werden. Der Verantwortliche darf es daher nicht allein deshalb zurückweisen, weil die betroffene Person einen *„fremden"* Zweck verfolgt - etwa die Vorbereitung einer Schadenersatzklage ohne datenschutzrechtlichen Bezug. ErwGr 63 DSGVO, wonach das Recht auf Auskunft besteht, damit sich die betroffene Person der Verarbeitung bewusst werden und die Rechtmäßigkeit überprüfen kann, ändere daran nichts (EuGH 26.10.2023, C-307/22 - *FT [Kopie der Patientenakte*], Rz 38 und 43).

Jedoch hat der EuGH kürzlich nachjustiert und festgestellt, dass eine missbräuchliche Antragstellung vorliegt, wenn sich aus einer Gesamtheit **objektiver Umstände** ergibt, dass trotz formaler Einhaltung der in der Unionsregelung vorgesehenen Bedingungen das Ziel dieser Regelung nicht erreicht wird (EuGH 19.3.2026, C-526/24 - *Brillen Rottler)*. Hinsichtlich der Erreichung des Ziels von Art 15 DSGVO sind laut diesem jüngsten Judikat sehr wohl die Ziele nach ErwGr 63 DSGVO heranzuziehen. Selbst wenn diese Ziele mit dem Auskunftsbegehren erreicht werden können, kann der Verantwortliche anhand aller Umstände des Einzelfalls das Bestehen eines **subjektiven Elements** nachweisen, das in der **Absicht** der betroffenen Person besteht, sich einen aus der Unionsregelung resultierenden **Vorteil zu verschaffen**, indem die **Voraussetzungen** für seine Erlangung **künstlich geschaffen** werden. Dies kann vorliegen, wenn die betroffene Person das Auskunftsbegehren zu einem anderen Zweck stellt als dem, sich der Datenverarbeitung bewusst zu werden und deren Rechtmäßigkeit zu überprüfen, um anschließend ihre Rechte aus der DSGVO schützen zu können, z.B., wenn die betroffene Person ein Auskunftsbegehren stellt, um künstlich die Voraussetzungen für die Erlangung von Schadenersatz vom Verantwortlichen zu schaffen, weil sie davon ausgeht, dass das Auskunftsbegehren gar nicht oder nicht entsprechend der DSGVO beantwortet wird.

Datenschutzfremde Beweggründe können laut OLG Wien zudem für den **Umfang des Auskunftsrechts** relevant sein. Die Beweggründe sind selbst dann zu beachten, wenn sie erst im Laufe des Gerichts- (oder Behörden)verfahrens hervorkommen (OLG Wien 28.7.2025, 13 R 15/25h).

Hinweise zur **Missbräuchlichkeit** bietet zudem die Judikatur des VwGH zu Art 57 Abs 4 DSGVO (Beschwerden bei der Aufsichtsbehörde), die wegen des nahezu identischen Wortlauts auf Art 12 Abs 5 DSGVO übertragbar ist. Auch danach sind die Motive für die Antragstellung relevant, um Missbräuchlichkeit feststellen zu können und liegt eine solche etwa dann vor, wenn ein **Antrag gar keinen Bezug** zu **datenschutzrechtlichen Fragestellungen** bzw. **Verstößen** aufweist (VwGH, Ra 2022/04/0049) oder wenn das Auskunftsbegehren **objektiv nicht erforderlich ist**, um die aus der DSGVO zukommenden **Rechte zu schützen**, **sondern** der Antrag einem **anderen Zweck dient** und **ohne diese sachfremden Gründe nicht gestellt** worden wäre (Ra 2020/04/0084). Auch wenn keine geradezu schikanöse Absicht mit einer Antragstellung verbunden ist, kann es nämlich als missbräuchlich angesehen werden, wenn eine Person Ressourcen in Anspruch nimmt, obwohl sich bereits aus dem Antrag ergibt, dass offenkundig andere Ziele verfolgt werden als die Durchsetzung des Schutzes, den die Bestimmungen der DSGVO gewähren (Ra 2022/04/0049). Ein weiterer Hinweis für Missbräuchlichkeit kann durch „**Feindseligkeit**“ gegenüber einer bestimmten Person argumentiert werden (Ra 2025/04/0143).

Zur **Exzessivität** von Auskunftsbegehren liegt ebenfalls bereits Judikatur vor: Die Beurteilung, ob Exzessivität gegeben ist, muss aus qualitativer Sicht erfolgen und hängt nicht allein von der Zahl der Auskunftsanträge der betroffenen Person ab. Somit kann auch ein erstes Auskunftsbegehren als „*exzessiv*“ im Sinne von Art 12 Abs 5 DSGVO angesehen werden (EuGH, C-526/24 - *Brillen Rottler).* Im Gegenzug reicht eine hohe Anzahl von Anträgen alleine nicht aus, um Exzessivität zu begründen. Diese kann aber ein Indiz dafür darstellen, dass vorwiegend datenschutzfremde Zwecke verfolgt werden (EuGH, C-416/23 - *ÖDSB, Exzessive Anfragen*; Ra 2023/04/0002).

Was bedeutet das für die Praxis?

- Die Beantwortung von Auskunftsbegehren kann abgelehnt werden (oder nur gegen Kostenersatz erteilt werden), wenn das Begehren missbräuchlich gestellt wurde.
- Auskunftsbegehren müssen nicht begründet werden, jedoch können die vorgebrachten und ersichtlichen Gründe für das Vorliegen von Missbräuchlichkeit herangezogen werden.

- Missbräuchlichkeit liegt jedenfalls vor, wenn die betroffene Person ein Auskunftsbegehren stellt, nur um künstlich die Voraussetzungen für die Erlangung von Schadenersatz vom Verantwortlichen zu schaffen.
- Auffallende Feindseligkeit kann einen weiteren Anhaltspunkt für Missbräuchlichkeit darstellen.
- Die Häufigkeit von Auskunftsbegehren alleine stellt noch keine Missbräuchlichkeit dar, kann aber ein Indiz dafür sein.
- Bereits das erste Auskunftsbegehren kann exzessiv sein.

Ob Missbräuchlichkeit vorliegt, ist daher stets **im Einzelfall** zu prüfen und muss vom Verantwortlichen **nachgewiesen** werden. Wir unterstützen Sie gerne bei dieser Beurteilung!

Compliancesystem macht sich bezahlt: Höchste DSGVO-Geldstrafe Österreichs vom VwGH auf EUR 13 Mio. herabgesetzt

Beitrag verfasst von Dr. Rainer Knyrim und Jakob Brunbauer – KTR-Newsletter August 2026

Vorgeschichte:
Bereits im Jahr 2019 erging ein Straferkenntnis der österreichischen **Datenschutzbehörde** (DSB) an die Österreichische Post, da diese in den Jahren zuvor u.a. „Parteiaffinitäten" ohne Zustimmung der Betroffenen erhoben und als Marketingdaten weiterverkauft hatte.

Über Umwege gelangte eine dagegen eingebrachte Beschwerde zum **Bundesverwaltungsgericht** (BVwG), welches das Verfahren 2020 zunächst gemäß § 45 Abs 1 Z 3 VStG einstellte; die DSB hatte im Straferkenntnis keine namentlich genannten natürlichen Personen adressiert, sondern lediglich die Österreichische Post als juristische Person. Zum damaligen Zeitpunkt wäre dies im Rahmen der Auslegung von Art 83 DSGVO nicht ausreichend gewesen. Durch Revision der DSB landete das Urteil 2022 vor dem **Verwaltungsgerichtshof** (VwGH), welcher das Revisionsverfahren zur Klärung einer Vorfrage durch den **EuGH** zunächst pausierte. Anfang des Jahres 2024 stellte der EuGH durch das Urteil Deutsche Wohnen SE (C-807/21) klar, dass eine Geldbuße wegen eines in Art 83 Abs 4 bis 6 DSGVO genannten Verstoßes gegen eine juristische Person als Verantwortliche verhängt werden kann, ohne dass der Verstoß zuvor einer natürlichen Person zugerechnet wurde, woraufhin der VwGH das Erkenntnis des BVwG aus 2022 aufhob. Das BVwG entschied daraufhin Ende 2024, das **Strafmaß von ursprünglich fast EUR 19 Mio**. auf EUR 16 Mio. zu senken. Gegen dieses Urteil erhob die Österreichische Post Revision und veranlasste sohin den VwGH, sich erneut (ein drittes Mal!) mit dem Sachverhalt zu beschäftigen und in der Sache final zu entscheiden (Ro 2025/04/0007-7).

Die Gründe für die Herabsetzung:
Der VwGH bestätigte das Vorbringen der Revisionswerberin, dass die im BVwG-Erkenntnis genannte Mangelhaftigkeit der Dokumentationspflicht – Datenschutz-Folgenabschätzung (DSFA) bzw. Verarbeitungsverzeichnis (VVZ) – erst durch die (vom VwGH bestätigte) falsche rechtliche Einschätzung, dass der Verkauf von Marketingdaten inkl. politischer Affinitäten zulässig sei, entstanden sei und somit im grundsätzlichen Vergehen des Verkaufes dieser Daten konsumiert werde. Zur „Konsumtion" führte der VwGH aus, dass Delikte, die in einem anderen ebenfalls verwirklichten Delikt bereits vollumfänglich erfasst sind, **nicht doppelt zugerechnet** werden.

Über die Festsetzung der Strafhöhe entschied der VwGH „in der Sache selbst" und nahm eine Strafbemessung vor, die er als verhältnismäßig, aber zugleich abschreckend für zukünftige Fälle erachtete. Das bestehende interne **Compliancesystem wurde vom VwGH ausdrücklich als Milderungsgrund berücksichtigt**. Des Weiteren wirkten sich sowohl die **unangemessen lange**

Verfahrensdauer vor dem VwGH als auch die vorgenannte **Konsumtion** strafmildernd aus, sodass die Strafe von EUR 16 Mio. auf EUR 13 Mio. herabgesetzt wurde.

Deutlich herabgesetzt wurden auch die ursprünglichen **Verfahrenskosten von EUR 1,6 Mio. auf EUR 100.000,00**, da nach Art 83 Abs 4 bis 6 DSGVO, so der VwGH, bereits ein außergewöhnlich hohes Strafmaß verhängt wurde und somit außergewöhnliche Umstände vorlagen. Daher war davon abzusehen, die üblichen 10 % des Strafmaßes als Verfahrenskosten festzusetzten.

Die Entscheidung des VwGH veranschaulicht, dass

- die Einrichtung bzw. das **Bestehen eines internen Compliancesystems strafmildernd** wirkt;
- es sich insgesamt lohnt, den **Instanzenzug** einzuschlagen, um eine mildere Strafe zu erhalten.

Die ursprüngliche **Strafe** von über EUR 19 Mio. wurde **um mehr als 30 % auf EUR 13 Mio. reduziert**, die **Verfahrenskosten um über 90 %**. Die Strafe ist damit – soweit uns ersichtlich ist – zwar nach wie vor die höchste in Österreich jemals im Datenschutzrecht verhängte Strafe, die Reduktion um mehrere Millionen Euro dürfte aber ebenso ein Rekord sein.

Lehrgänge – Seminare – Tagungen

KTR-Newsletter August 2026

Dies sind unsere kommenden Veranstaltungen im Überblick. Beachten Sie die Rabattmöglichkeiten, die wir als Vortragende und Leitende für Teilnehmer:innen anbieten können, die sich über unsere Empfehlung anmelden!

Der Seminarherbst bietet auch diesmal viele Termine in **Wien**, darüber hinaus tragen wir in **Graz** und in **Liechtenstein** bei spannenden Veranstaltungen vor.

Die **Privacy & Security** wird es übrigens nicht nur im November 2026 zum bereits elften Mal in Andau im Burgenland geben, **2027** folgt nach dem gelungenen Auftakt im Mai 2026 auch wieder eine eigene **PriSec GERMANY**.

LEHRGÄNGE

16. bis 18. November 2026
NIS-2 Lehrgang
Mit oder ohne Zertifizierung (Prüfung) buchbar.
Fachliche Leitung: Dr. Rainer Knyrim
Details und Anmeldung HIER.
Kanzlei-Rabatt: Business Circle gewährt einen Rabatt in Höhe von EUR 300,00 auf den Nettopreis bei Angabe des Codes „**35OXV**“ im Feld „Rabattcode“ in Teil 2 des Anmeldeformulars.

23. bis 25. November 2026
Lehrgang zum/zur zertifizierten Datenschutzbeauftragten
Mit oder ohne Zertifizierung (Prüfung) buchbar.
Fachliche Leitung: Dr. Rainer Knyrim
Details und Anmeldung HIER.
Kanzlei-Rabatt: Business Circle gewährt einen Rabatt in Höhe von EUR 300,00 auf den Nettopreis bei Angabe des Codes „**3VY0L**“ im Feld „Rabattcode“ in Teil 2 des Anmeldeformulars.

SEMINARE

16. September 2026
KI-Kompetenz: Technische Grundlagen, ethische Aspekte und rechtliche Rahmenbedingungen
Vortrag: Dr. Stephan Varga, BSc
Details und Anmeldung (AWAK) HIER

13. Oktober 2026
Datenschutz für Fortgeschrittene und Rezertifizierung als Datenschutzbeauftragter Fachliche Leitung: Dr. Rainer Knyrim
Details und Anmeldung HIER.
Kanzlei-Rabatt: Business Circle gewährt einen Rabatt in Höhe von EUR 100,00 auf den Nettopreis bei Angabe des Codes „**3E7UL**“ im Feld „Rabattcode“ in Teil 2 des Anmeldeformulars.

25. November 2026
Fortbildungsseminar zur Datenschutz-Grundverordnung TRIESEN
Vortrag: Dr. Gerald Trieb, LL.M.
Details und Anmeldung (Private Universität im Fürstentum Liechtenstein) HIER.

1. Dezember 2026
Update EU Datenschutzrecht
Fachliche Leitung: Dr. Rainer Knyrim
Details und Anmeldung HIER.
Kanzlei-Rabatt: Business Circle gewährt einen Rabatt in Höhe von EUR 100,00 auf den Nettopreis bei Angabe des Codes „**13MBC**“ im Feld „Rabattcode“ in Teil 2 des Anmeldeformulars.

2. Dezember 2026
Die Digitalisierungsrechtsakte der EU – Datenstrategie und KI-Zukunft
Fachliche Leitung: Dr. Rainer Knyrim
Details und Anmeldung HIER
Kanzlei-Rabatt: Business Circle gewährt einen Rabatt in Höhe von EUR 100,00 auf den Nettopreis bei Angabe des Codes „**3UIYA**“ im Feld „Rabattcode“ in Teil 2 des Anmeldeformulars.

14. Dezember 2026
DSGVO und KI im Marketing
Fachliche Leitung: Dr. Rainer Knyrim
Details und Anmeldung HIER.
Kanzlei-Rabatt: Business Circle gewährt einen Rabatt in Höhe von EUR 100,00 auf den Nettopreis bei Angabe des Codes „**3RHUP**“ im Feld „Rabattcode“ in Teil 2 des Anmeldeformulars.

TAGUNGEN

12. Oktober 2026
Jahrestagung Datenschutzrecht WIEN
Fachliche Leitung: Dr. Gerald Trieb, LL.M.
Vortrag: Mag. Gregor Brandstetter, BA
Details und Anmeldung HIER.
Die MANZ Rechtsakademie gewährt einen Kanzlei-Rabatt in Höhe von -25 % auf den Normalpreis bei Angabe des Codes „**Kanzlei-Rabatt Knyrim-Trieb**“ unter „Anmerkung“.

1. Dezember 2026
Jahrestagung Datenschutzrecht GRAZ
Fachliche Leitung: Dr. Gerald Trieb, LL.M.
Vortrag: Mag. Gregor Brandstetter, BA
Details und Anmeldung HIER.
Die MANZ Rechtsakademie gewährt einen Kanzlei-Rabatt in Höhe von -25 % auf den Normalpreis bei Angabe des Codes „**Kanzlei-Rabatt Knyrim-Trieb**“ unter „Anmerkung“.

KONFERENZ

12. bis 13. November 2026
PriSec – Privacy & Security
Fachliche Leitung: Dr. Rainer Knyrim
Roundtable Session: Mag. Gregor Brandstetter, BA
Details und Anmeldung HIER.
Kanzlei-Rabatt: Business Circle gewährt einen Rabatt in Höhe von EUR 100,00 auf den Nettopreis bei Angabe des Codes „**6PS5U**“ im Feld „Rabattcode“ in Teil 2 des Anmeldeformulars.

11. bis 12. Mai 2027
PriSec – Privacy & Security GERMANY
Fachbeirat: Dr. Rainer Knyrim
Details und Anmeldung HIER.


Publikationen unserer Kanzlei

KTR-Newsletter August 2026

Gemäß unserem Motto **„Wir schreiben selbst“** sind auch in den letzten Monaten wieder Beiträge und Publikationen unserer Jurist:innen erschienen.

BEITRÄGE

Rainer Knyrim, Gregor Brandstetter
NISG 2026: Neues und Altbekanntes, Dako 2/2026, 2026/14.

Nachzulesen HIER.

Rainer Knyrim/Reinhard Ebner
Chronologie einer Cyberattacke, Interview mit **Manuel Löw-Beer**, Dako 1/2026, 2026/2.

Nachzulesen HIER.

Der DatKomm

Der von Dr. Rainer Knyrim herausgegebene „DatKomm" wurde zuletzt durch diese neuen Kommentierungen aktualisiert:

- Art 3: räumlicher Anwendungsbereich der DSGVO
- Art 9-11: Verarbeitung besonderer personenbezogener Daten
- Art 20-23: Datenübertragbarkeit, Widerspruchsrecht, Automatisierte Entscheidungen und Profiling, Ausnahmen von Betroffenenrechten
- Art 26-27: gemeinsame Verantwortliche, Benennung eines Vertreters in der EU
- Art 85-87: Novelle zum Medienprivileg nach VfGH-Entscheidung
- Art 90: Geheimhaltungspflichten, Neuerungen nach Inkrafttreten des IFG

Das nächste Paket an Ergänzungslieferungen ist bereits geschnürt und wird im Lauf des Herbstes 2026 erscheinen!

ZEITSCHRIFT

Dako 3/2026
Das jüngste Heft erschien im Juli 2026. Es ist dem Schwerpunkt „**Digitale Souveränität**" gewidmet und enthält, neben einer Einleitung von Herausgeber Rainer Knyrim, Beiträge von Mirjam Tercero, Christof Tschohl, Michael Mrak, Michael Staudacher, Rifat Büyükyorulmaz, Viktoria Haidinger und Michael Löffler. Das **Interview** führte Hans-Jürgen Pollirer mit Roland Ledinger vom Bundesrechenzentrum. Die **Checkliste** von Hans-Jürgen Pollirer unterstützt bei der **Auswahl von Auftragsverarbeitern und deren Sub-Auftragsverarbeitern**.

Inhaltsverzeichnis und Bestellmöglichkeit bei MANZ HIER.

PODCAST

Im RECHTaktuell-Podcast „**NISG: Pflichten, Fristen, Risiken**“ vom 29.5.2026 sprach **Dr. Rainer Knyrim** mit **Dr.in Elisabeth Maier** vom MANZ Verlag über die wichtigsten Eckpunkte der neuen gesetzlichen Regelungen für Netz- und Informationssicherheit.

- Was sind die Ziele des NISG 2026 bzw. der NIS-2-Richtlinie?
- Wen betrifft das NISG 2026?
- Wann kann eine Einrichtung unter das NISG 2026 fallen, obwohl man es nicht vermutet?
- Worauf müssen sich Einrichtungen einstellen bzw. vorbereiten?
- Was ist zu tun, wenn ein Cybersicherheitsvorfall passiert?
- Wer in der Organisation ist verantwortlich?
- Welche Strafen drohen bei Nichteinhaltung?

Zum Podcast von MANZ geht’s HIER.

ONLINE Q&A

Im Juli 2026 erschien die neue Ausgabe von Lexology Panoramic für den Bereich „Data Protection and Privacy“.

Dr. Rainer Knyrim und **Jennifer Salomon, LL.M.** haben den aktualisierten Beitrag zu **Österreich** verfasst.

Den Beitrag finden Sie als PDF-Datei HIER.

Wiedergabe mit Genehmigung von Law Business Research Ltd. Dieser Artikel wurde zuerst veröffentlicht in **Lexology Panoramic: Data Protection & Privacy 2027**. Für weitere Informationen besuchen Sie bitte: https://www.lexology.com/panoramic

Wir veröffentlichen unsere Publikationen bzw. Neuigkeiten dazu auch regelmäßig auf unserer **Website** unter und berichten oft auch auf **LinkedIn**:

- **https://www.kt.at/publikationen/**
- **Zur LinkedIn-Seite von Knyrim Trieb Rechtsanwälte OG**

Unsere Ranking-Erfolge – international und national

KTR-Newsletter August 2026

Gemeinsam mit unserem tollen **Team** konnten wir uns in den vergangenen Monaten wieder über große **Erfolge** in den internationalen Rankings von **Chambers, Legal 500** und **Lexology Index** sowie im hierzulande vielbeachteten **trend. Anwalts-Ranking** und die damit verbundene **Anerkennung unserer Arbeit** freuen!

Mit unserer besonderen Leidenschaft für alle **Datenschutz-, Digitalisierungs- und IT-Rechtsthemen** sind wir immer für unsere Klienten da und erarbeiten Lösungen!

🏆 **Chambers** ist wohl das traditionsreichste Ranking und basiert seine Ergebnisse auf umfassende Erhebungen: Im **Chambers Europe Legal Guide 2026** wurden Knyrim Trieb Rechtsanwälte erneut als führende Experten im Bereich **TMT: Data Protection** in **Österreich** ausgezeichnet:

- BAND 1 – Dr. Rainer Knyrim
- BAND 2 – Dr. Gerald Trieb, LL.M.
- BAND 1 – Knyrim Trieb Rechtsanwälte OG

🏆 Für das Ranking **Legal 500 EMEA 2026** erfolgt ebenfalls eine aufwändige Recherche, um die besten Rechtsanwält:innen in den EMEA-Ländern zu küren. Unsere Kanzlei hat neuerlich führende Positionen im Bereich **Data Privacy and Data Protection** erreicht!

- LEADING PARTNERS – Dr. Gerald Trieb, LL.M.
- HALL OF FAME – Dr. Rainer Knyrim
- TIER 1 – Knyrim Trieb Rechtsanwälte OG

🏆 Im neuen **Lexology Index – Data 2026** werden wir ebenfalls zum wiederholten Male als Experten für **Datenschutzrecht** in **Österreich** besonders empfohlen:

- THOUGHT LEADER – Dr. Gerald Trieb, LL.M.
- GLOBAL ELITE THOUGHT LEADER – Dr. Rainer Knyrim
- Dr. Gerald Trieb, LL.M. konnte heuer einen besonderen Erfolg verbuchen – er wurde als **Client Choice Winner** in der Kategorie **Data** in Österreich ausgezeichnet.

🏆 Zu guter Letzt – zurück nach **Österreich**:

Im **trend. Anwalts-Ranking** werden jeden April die besten Anwälte des Landes gekürt. Dr. Rainer Knyrim wurde 2026 zum **9. Mal auf Platz 1** im **Datenschutzrecht** gereiht! Bereits seit 2021 ist der Erfolg zudem stets ein doppelter für Knyrim Trieb Rechtsanwälte mit Dr. Gerald Trieb, LL.M. auf einer tollen **Top 5-Platzierung**.

Weitere Newsletter finden Sie auf unserer Website unter www.kt.at/newsletter.

Datenschutzinformation

Die Verarbeitung der Daten zu diesem Newsletter erfolgt durch Knyrim Trieb Rechtsanwälte OG. Für den Versand bedienen wir uns eines Newsletter-Versandpartners, derzeit Mailjet.de, für die Speicherung Ihrer Daten eines Internet-Service-Providers, derzeit A1 Telekom Austria. Die Einwilligung kann durch Klicken des untenstehenden Links „Vom Newsletter anmelden“ jederzeit widerrufen werden. Alle Informationen darüber, welche Daten wir für den Newsletter verarbeiten, finden Sie in unserer Datenschutzinformation: https://www.kt.at/datenschutzinformation/

Knyrim Trieb Rechtsanwälte OG
Mariahilfer Straße 89a, A-1060 Wien
T: +43 1 909 30 70, E: kt@kt.at, W: www.kt.at
FN 462250f, HG Wien