Secur-Data Betriebsberatungs-Ges.m.b.H.
1010 Wien, Fischerstiege 9
Tel. +43 (1) 533 42 07-0
Internet: www.secur-data.at E-Mail: office@secur-data.at
Offenlegung gem. MedienG: www.secur-data.at/impressum

DSG-Info-Service

Jänner 2026 Ausgabe Nr. 120

Liebe Leserinnen und Leser,

herzlich willkommen im neuen Jahr und zu einer neuen Ausgabe unseres DSG-Info-Service!

Das Jahr 2026 begann sehr positiv mit dem Neujahrempfang der Datenschutzbehörde am 13. Jänner 2026 sowie mit dem Neujahrempfang der Privacy Officers, dem Verein betrieblicher und behördlicher Datenschutzbeauftragter, am 15. Jänner 2026. Beide Veranstaltungen waren sehr gut besucht.

Auch das neue Jahr stellt uns alle wieder vor neue Herausforderungen. Das NIS-2-Gesetz (NISG 2026) wurde zu Jahresende 2025 endlich verabschiedet und tritt 2026 in Kraft, der „Digitale Omnibus" mit geplanten Änderungen von DSGVO, Data Act und AI Act nimmt Fahrt auf. Beides möchten wir Ihnen in dieser Ausgabe kurz näherbringen.

Außerdem präsentieren wir Neuigkeiten zur diesjährigen Schwerpunktprüfung der Österreichischen Datenschutzbehörde sowie zu aktuellen Angemessenheitsbeschlüssen der Europäischen Kommission. Schließlich berichten wir über Aktuelles aus der datenschutzrechtlichen Rechtsprechung und Sie erhalten wie gewohnt einen Überblick über verhängte Verwaltungsstrafen der vergangenen Monate sowie relevante Ankündigungen!

Abschließend zur Erinnerung – am 28. Jänner 2026 ist europäischer Datenschutztag!

Viel Spaß bei der Lektüre wünscht

Mag. Judith Leschanz
Geschäftsführung

1. NISG 2026

Grundsätzliches zum neuen NISG 2026

Mit über einem Jahr nach Ablauf der Umsetzungsfrist wurde vom Nationalrat am 18. Dezember 2025 das NISG 2026[1] (Netz- und Informationssystemsicherheitsgesetz 2026 – BGBl. I Nr. 94/2025) mit der notwendigen Verfassungsmehrheit beschlossen und tritt 9 Monate nach Kundmachung im Bundesgesetzblatt, also mit 1. Oktober 2026, in Kraft. Wir haben Sie dazu bereits in DSG-Info Nr. 108[2] sowie Nr. 112[3] informiert.

Die NIS-2-Richtlinie[4] (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in

[1] https://kurzlinks.de/jmsq
[2] https://kurzlinks.de/h9x8
[3] https://kurzlinks.de/tvn5
[4] https://kurzlinks.de/exds

der Union folgt der NIS-1-Richtlinie[5] (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz -und Informationssystemen in der Union. Das NISG 2018[6] zur Umsetzung der NIS1-Richtlinie gilt noch bis Herbst 2026.

Durch die neuen Bestimmungen des NISG 2026 sollen bei Unternehmen das **Sicherheitsniveau angehoben**, Risiken durch Datenverluste oder Betriebsausfälle verringert, die Reaktionsfähigkeit auf Angriffe wie zB Hacking verbessert und dadurch das Vertrauen der Kunden generell gestärkt werden. Von allen betroffenen Unternehmen sind daher ab Oktober 2026 verpflichtend angemessene Maßnahmen zur Sicherung und Stärkung ihrer Cyberresilienz zu ergreifen.

Inhalt

Das **NISG 2026** erweitert den bisherigen Anwendungsbereich auf eine **Vielzahl von Unternehmen und Sektoren**.

Vom Anwendungsbereich erfasst sind einerseits Unternehmen aus **Sektoren mit hoher Kritikalität** nach Anlage 1 (zB Energie, Verkehr, Gesundheitswesen, öffentliche Verwaltung, digitale Infrastruktur).

Andererseits sind Unternehmen **aus sonstigen kritischen Sektoren** gemäß Anlage 2 (zB Post, Lebensmittel, Anbieter digitaler Dienste) umfasst. Banken fallen nicht unter das NISG 2026, sondern unterliegen der DORA (Digital Operational Resilience Act) Verordnung (EU) 2022/2554[7] als Lex specialis.

Generell unterscheidet das NISG 2026 **zwischen wesentlichen und wichtigen Einrichtungen** sowie zwischen großen und mittleren Unternehmen, jeweils anhand der Anzahl der Mitarbeiter, dem Jahresumsatz und der Jahresbilanzsumme. Zusätzlich kann die neue Cybersicherheitsbehörde Unternehmen als wesentliche oder wichtige Einrichtung einstufen.

Aus der Einstufung als wesentliche oder wichtige Einrichtung ergeben sich unterschiedliche Folgen. Insbesondere gilt für wesentliche Einrichtungen eine **Ex-ante-Aufsicht**, für wichtige Einrichtungen nur eine **Ex-post-Aufsicht** im Anlassfall.

Alle betroffenen Unternehmen trifft die **Registrierungspflicht** bis zum 1. Jänner 2027. Außerdem trifft die Unternehmen eine **Pflicht zur Selbstdeklaration** über umgesetzte Maßnahmen inkl. Sicherheit in der Lieferkette bis spätestens 1. Oktober 2027.

Das NISG 2026 normiert im Vergleich zum bisherigen NISG 2018 darüber hinaus **erweiterte Anforderungen an das Risikomanagement.** Insbesondere sind Maßnahmen zur Sicherheit der Netz- und Informationssysteme sowie der Lieferkette und zur Verhinderung bzw. Verringerung von Auswirkungen bei Sicherheitsvorfällen zu treffen.

Das NISG 2026 enthält außerdem für die betroffenen Unternehmen Meldepflichten bei erheblichen Cybersicherheitsvorfällen binnen 24 Stunden, 72 Stunden bzw. eines Monats an das jeweils zuständige **Notfallteam (Cybersecurity Incident Response Team)**. Daneben gelten weiterhin die Vorschriften zur Meldung von Datenschutzvorfällen nach der DSGVO.

Sanktionen

Neben **Verwaltungsstrafen**, die auch gegen **juristische Personen** bzw. eingetragene Personengesellschaften bei mangelnder Überwachung oder Kontrolle verhängt werden können, sieht das NISG 2026 **Sanktionen** in Höhe von bis zu **EUR 10 Mio.** oder 2 % des Gesamtjahresumsatzes (für wesentliche Einrichtungen) bzw. bis zu **EUR 7 Mio.** oder 1,4 % des Gesamtjahresumsatzes (für wichtige Einrichtungen) vor.

[5] https://kurzlinks.de/c3f2
[6] https://kurzlinks.de/d0zq
[7] https://kurzlinks.de/bfcy

Sollte es gleichzeitig zu einem **Datenschutzverstoß** kommen, sind **keine Doppelsanktionen** vorgesehen. Für öffentliche Stellen wird ein alternatives Sanktionsregime eingeführt. Zusätzlich sieht das NISG 2026 weitere Strafen von EUR 50.000 bis EUR 100.000 vor, zB bei Nichterfüllung der Pflicht zur Registrierung oder Selbstdeklaration.

Cybersicherheitsbehörde

Als Cybersicherheitsbehörde wird das **Bundesamt für Cybersicherheit** als neue, dem Innenministerium nachgeordnete Stelle eingeführt, welche an die zuständigen Ausschüsse des Nationalrates zu berichten hat. Dieses ist u.a. die zentrale Anlaufstelle für die Gewährleistung der Sicherheit von Netz- und Informationssystemen und der grenzüberschreitenden Zusammenarbeit und hat auch die Funktion als **nationales Koordinierungszentrum für Cybersicherheit**. Außerdem wurde beim Innenministerium eigens eine NIS-Stelle[8] für Fragen und Informationen zu diesem Thema eingerichtet und werden dort auch Plattformen für Vorfallsmeldungen bestimmter Sektoren geführt.

Verantwortlichkeit der Leitungsorgane

Die **Leitungsorgane** aller vom NISG 2026 umfassten Unternehmen sind für die Einhaltung der Vorschriften und Kontrolle, insbesondere die Risikomaßnahmen betreffend**, verantwortlich**. Sie haben **verpflichtend an Schulungen teilzunehmen**, wobei das NISG 2026 nur Geschäftsführung und Vorstände, nicht aber Prokuristen oder Aufsichtsräte, betrifft.

Auswirkungen auf betroffene Unternehmen

Alle Unternehmen sind angehalten, rasch zu prüfen, ob sie aufgrund des erweiterten Anwendungsbereichs nunmehr unter das NISG 2026 fallen. Die **Wirtschafskammer Österreich** hat zu diesem Zweck einen **Online-Ratgeber** (https://ratgeber.wko.at/nis2/) erstellt, damit jedes Unternehmen die Anwendbarkeit des NISG 2026 überprüfen kann.

Betroffene Unternehmen haben unverzüglich alle notwendigen Schritte zur Erfüllung der Pflichten aus dem NISG 2026 umsetzen. Insbesondere sollten notwendige Anpassungen für die **Registrierung**, welche **bis Ende 2026** durchzuführen ist, rasch in die Wege geleitet werden.

In weiterer Folge müssen **Vorbereitungen für die Selbstdeklaration** getroffen werden. Außerdem sind die internen Strukturen bzgl. Risikomanagement, Sicherheit der Lieferketten, Umsetzung der Meldeverpflichtungen sowie Verantwortlichkeiten der Leitungsorgane zu adaptieren. Wichtig ist in diesem Zusammenhang, dass auf Aufforderung der Cybersicherheitsbehörde binnen 2 Jahren (bei wesentlichen Einrichtungen binnen 2 Monaten) die Umsetzung der Risikomaßnahmen nachzuweisen ist, wobei der organisatorische und operative Teil der Prüfung durch eine entsprechende Zertifizierung (zB ISO 27001) ersetzt werden kann.

Wenn Sie Unterstützung beim Thema NIS-2 bzw. NISG 2026 benötigen, beraten wir Sie gerne dazu!

Auf unser Website finden Sie außerdem eine Checkliste zum Thema NIS-2[9].

[8] www.nis.gv.at/

[9] https://kurzlinks.de/wgn1

Erfüllung der Pflichten der NIS-2-Richtlinie und des NISG 2026

Mit Oktober 2026 tritt in Österreich das neues Netz- und Informationssystemsicherheitsgesetz (NISG 2026) in Kraft, das deutlich mehr Unternehmen betrifft als sein Vorgänger.

Unternehmen müssen sich auf umfassende neue Anforderungen einstellen, um die Sicherheit ihrer Netz- und Informationssysteme zu gewährleisten. Unsere Beratung steht Ihnen zur Seite, um diese Herausforderungen erfolgreich zu meistern.

Wichtige Pflichten des neuen Gesetzes:

- **Risikomanagement**: Unternehmen müssen Risiken für ihre IT-Systeme analysieren und geeignete Maßnahmen zur Risikominimierung ergreifen.
- **Vorfallmeldung**: Sicherheitsvorfälle, die den Betrieb beeinträchtigen könnten, müssen unverzüglich gemeldet und zügig behoben werden.
- **Krisenmanagement**: Pläne zur Wiederherstellung und Minimierung von Ausfällen müssen entwickelt und regelmäßig getestet werden.
- **Informationsaustausch**: Unternehmen sind verpflichtet, mit Behörden und Partnern zusammenzuarbeiten und Informationen über Bedrohungen und Vorfälle auszutauschen.
- **Lieferkettensicherheit**: Auch die Sicherheit von Lieferanten und Drittanbietern muss überwacht und sichergestellt werden.
- **Compliance**: Alle Maßnahmen müssen dokumentiert werden und nachweislich den gesetzlichen Vorgaben entsprechen.

Unsere Beratung unterstützt Sie in allen Bereichen:

- **Individuelle Risikobewertungen**: Wir analysieren Ihre spezifischen Risiken und entwickeln maßgeschneiderte Sicherheitskonzepte, die den Anforderungen des NIS-2-Gesetzes gerecht werden.
- **Effektives Vorfallmanagement**: Wir helfen Ihnen, ein effizientes Vorfallmanagement aufzubauen und unterstützen Sie bei der Einhaltung der strengen Meldepflichten.
- **Krisen- und Wiederherstellungsplanung**: Wir entwickeln robuste Krisenpläne und Wiederherstellungsstrategien, die sicherstellen, dass Ihr Betrieb im Ernstfall schnell lauffähig gemacht wird.
- **Umfassende Schulungen**: Wir bieten Schulungen und Sensibilisierungsprogramme an, um Ihr Team auf die neuen Anforderungen vorzubereiten und die Cybersicherheitskultur in Ihrem Unternehmen zu stärken.
- **Dokumentation und Compliance**: Wir unterstützen Sie bei der Erstellung und Pflege der erforderlichen Dokumentation, um sicherzustellen, dass Sie jederzeit nachweisen können, dass Sie alle gesetzlichen Vorgaben erfüllen.

Unser umfassendes wissenschaftliches Know-how und unser praxisorientierter Ansatz machen uns zum idealen Partner für die Umsetzung der Anforderungen des NISG 2026. Mit unserer Unterstützung sind Sie bestens vorbereitet, um die neuen gesetzlichen Pflichten effizient und nachhaltig zu erfüllen.

Kontaktieren Sie uns für eine individuelle Beratung und lassen Sie uns gemeinsam Ihre IT-Sicherheitsziele erreichen!

2. Aktuelles von der Datenschutzbehörde

Schwerpunktprüfung Neu in 2026

Wie wir Sie bereits im letzten DSG-Info-Service Nr. 119[10] informiert haben, wird die Österreichische Datenschutzbehörde (DSB) auch 2026 Schwerpunktprüfungen durchführen. Diese amtswegigen Prüfverfahren werden in leicht abgeänderter Form durchgeführt werden.

Die **Prüfverfahren** werden im Sinne einer J**ahresstrategie** und erstmals **ohne Auswahl eines bestimmten Sektors** durchgeführt. Die DSB hat sich wie in den Vorjahren zur Teilnahme an der **Maßnahme des Europäischen Datenschutzausschuss** (EDSA) zum koordinierten Durchsetzungsrahmen (Coordinated Enforcement Framework, CEF) verpflichtet. Für 2026 wurde vom EDSA[11] als Thema die **Einhaltung der Transparenz- und Informationspflichten** gemäß Art. 12, 13 und 14 Datenschutz-Grundverordnung (DSGVO) mitgeteilt. Im Zuge eines Fragebogens sollen dabei einerseits die Erfüllung der Rechenschaftsverpflichtungen durch Verantwortliche, andererseits die Transparenz der Datenverarbeitung sowie die Ausübung der Betroffenenrechte nach DSGVO kontrolliert werden.

Wie die DSB vor kurzem auf ihrer Website[12] verlautbarte, sollen die **diesjährigen Schwerpunktprüfungen in zwei Teilen** erfolgen: Im Zentrum des **ersten Teils der Prüfung** stehen die Vorgaben zur **Sicherheit der Verarbeitung** gemäß Art. 32 DSGVO und somit die Einhaltung geeigneter technischer und organisatorischer Maßnahmen. Dies schließt sowohl die Dokumentationspflichten im Rahmen der Verarbeitungsverzeichnisse nach Art. 30 als auch die Risikobewertung nach Art. 35 DSGVO ein. Als Zeitpunkt des Beginns der Verfahren nannte die Behörde März 2026.

Details für die Inhalte des zweiten Teils der diesjährigen Schwerpunktprüfungen kündigte die Behörde für Juni 2026 an. Darin soll jedenfalls der **Fragebogen des ESDA** an Verantwortliche und Auftragsverarbeiter zur Beantwortung übermittelt werden.

Da die Schwerpunktprüfungen für 2026 wie erwähnt sektorunabhängig erfolgen, können diese jedes Unternehmen treffen.

Um optimal auf beide Teile einer möglichen Prüfung durch die DSB vorbereitet zu sein, sollten einerseits die Sicherheit der Verarbeitung, insbesondere die Verarbeitungsverzeichnisse, andererseits die Datenschutzerklärungen und die darin enthaltenen Informationen jeweils auf ihre Aktualität sowie die Berücksichtigung aktueller Judikatur und der Unternehmenssituation geprüft und gegebenenfalls angepasst werden.

Nach erfolgter Prüfung werden die Ergebnisse wiederum durch den EDSA sowie durch die DSB in gewohnter Weise veröffentlicht.

3. Neue Angemessenheitsbeschlüsse der Kommission

Ende 2025 hat die Europäische Kommission (EK) neue Angemessenheitsbeschlüsse gemäß Art. 45 DSGVO (bzw. gemäß Art. 36 der RL (EU) 2016/680[13]) beschlossen. In diesen Angemessenheitsbeschlüssen legt die EK fest, dass ein Drittland oder eine internationale Organisation ein angemessenes Schutzniveau für die Verarbeitung personenbezogener Daten bietet und

[10] https://kurzlinks.de/kqj6
[11] https://kurzlinks.de/wk6w
[12] https://kurzlinks.de/v09b
[13] https://kurzlinks.de/l2qu

daher personenbezogene Daten ohne zusätzliche Schutzmaßnahmen übermittelt werden dürfen.

Neue Angemessenheitsbeschlüsse mit dem Vereinigten Königreich

Die mit 27. Dezember 2025 ausgelaufenen **Angemessenheitsbeschlüsse mit dem Vereinigten Königreich** (UK) aus 2021 wurden mit 19. Dezember 2025 bis zum **27. Dezember 2031 verlängert**. Relevant ist für Unternehmen insb. der Angemessenheitsbeschluss[14] bzgl. der DSGVO. Der zweite Angemessenheitsbeschluss[15] betrifft die EU-Richtlinie 2016/680 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung.

Die Verlängerung beider Beschlüsse bedeutet, dass bei Übermittlung von personenbezogenen Daten an das Vereinigte Königreich (UK) weiterhin von einem angemessenen Datenschutzniveau ausgegangen werden kann.

Allerdings hat die EK angekündigt, die praktische Umsetzung des englischen Datenschutzrechts weiterhin zu überwachen, sodass es noch zu notwendigen Korrekturen kommen kann.

Neuer Angemessenheitsbeschluss mit der Europäischen Patentorganisation

Erstmals hat die Europäische Kommission am 15. Juli 2025 einen **Angemessenheitsbeschluss**[16] **mit** einer internationalen Organisation, der **Europäischen Patentorganisation** (EPO), abgeschlossen. Das Datenschutzniveau in der EPO gilt ab dem 15. Juli 2025 als „angemessen" iSd. Art. 45 DSGVO.

Weitere Angemessenheitsbeschlüsse in Verhandlung

Aktuell in Prüfung durch die EK und daher noch nicht beschlossen ist der **Angemessenheitsbeschluss mit Brasilien**, zu dem bereits 2023 die Verhandlungen begonnen haben. Im November 2025 hat der EDSA eine diesbezügliche Stellungnahme[17] veröffentlicht, in der er von einem mit der EU vergleichbaren Datenschutzniveau in Brasilien spricht, aber gleichzeitig Verbesserungsvorschläge im Bereich der Durchsetzung der Betroffenenrechte und der aktuell nicht vorhandenen Unabhängigkeit der brasilianischen Datenschutzbehörde macht.

4. Digitaler Omnibus

Im November 2025 stellte die Europäische Kommission (EK) ihre Pläne für den sog. „Digitalen Omnibus" vor, worin im ersten Teil[18] Änderungen der DSGVO sowie des Data Act, und in einem zweiten Teil[19] Änderungen des sog. AI Act[20] vorgeschlagen werden.

Der Digitale Omnibus ist Teil einer **Serie an „Omnibus"-Paketen**[21], welche die EK in 2025 veröffentlicht hat. Ziel dieser neuen Vereinfachung von Vorschriften soll eine Reduzierung des Aufwands für Unternehmen durch Entbürokratisierung und bessere Kosteneffizienz sein, um generell die Wettbewerbsfähigkeit von Unternehmen sowie das Wachstum in der EU zu steigern. Dass diese Neuregulierungen nicht unumstritten sind, zeigten kritische Worte aus Teilen der Zivilgesellschaft[22], als im

[14] https://kurzlinks.de/2wvm
[15] https://kurzlinks.de/54dl
[16] https://kurzlinks.de/7ykc
[17] https://kurzlinks.de/qmh3
[18] https://kurzlinks.de/y1xu
[19] https://kurzlinks.de/ict0
[20] https://kurzlinks.de/oflw
[21] https://kurzlinks.de/s25m
[22] https://kurzlinks.de/s2ud

Vorfeld erste Entwürfe zum Digitalen Omnibus bekannt wurden.

Wesentliche Inhalte

Neben umfangreichen Änderungen des AI Act und der DSGVO enthalten die vorliegenden Entwürfe zum Digitalen Omnibus zusätzlich Vereinfachungen der Vorschriften des Data Act[23], des Data Governance Act[24] und auch der Open Data Directive[25].

Der **Data Governance Act** und **die Open Data Directive** sollen künftig **im Data Act integriert** werden.

Im Data Act werden u.a. Erleichterungen für KMUs auf sog. **Small-Mid-Caps-Unternehmen** erweitert. Auch sollen Dateninhaber künftig die Herausgabe von Geschäftsgeheimnissen verweigern dürfen, wenn dadurch ein hohes Risiko der Datenübermittlung an Drittländer ohne ausreichendes Schutzniveau entsteht.

Meldungen von Sicherheitsvorfällen bzgl. NIS-2, DORA und DSGVO sollen bei der **European Union Agency for Cybersecurity** (ENISA) mittels Schnittstelle zentralisiert werden.

Der Digitale Omnibus legt auch eine verbindliche Regelung und damit **Modernisierung von Cookie-Vorschriften** fest, wodurch die Bestimmungen zu Cookies der **e-Privacy-Richtlinie**[26] **obsolet** werden. Die Pläne für eine e-Privacy-Verordnung hatte die EK bereits im Rahmen ihres Arbeitsprogramms 2025[27] als beendet erklärt.

Vereinfachung der Regelungen des AI Act

Der **Geltungsbeginn** der Vorschriften für Hochrisiko-KI wird auf 2. Dezember 2027 sowie für alle Produkte im Rahmen eines Hochrisiko KI-Systems auf 2. August 2028 **verschoben**.

Dies ist sinnvoll, da vor allem die durch die EK zu erlassenden technischen Standards zur harmonisierten Konformität für Unternehmen mit dem AI Act noch nicht existieren.

Zur generellen **Vereinfachung** wurden die Vorschriften für **Anbieter von Hochrisikosystemen** speziell bzgl. des Registrierungsaufwands reduziert.

Erleichterungen für kleinere Unternehmen soll die **Ergänzung** vereinfachter Anforderungen bzgl. KMUs, auch hier auf **Small-Mid-Caps-Unternehmen** einschließlich Start-ups ausgeweitet, vor allem hinsichtlich der technischen Dokumentation bringen.

Erleichterungen für Anbieter gibt es durch den **Entfall** der Vorschrift zur Erstellung eines harmonisierten **Plans** zur **Überwachung** nach dem Inverkehrbringen **von Hochrisiko-KI Systemen**.

Weiters wird die Nutzung von KI-Regulatory Sandboxes erweitert und um sog. „Real-world"-Bedingungen ergänzt.

Schließlich sollen die **Befugnisse des KI-Büros** insgesamt gestärkt und die Aufsicht über KI-Systeme zentralisiert werden.

Änderungen der DSGVO

Die Definition „personenbezogener Daten" in **Art. 4 Z 1 DSGVO** wird angepasst, sodass eine natürliche Person für eine Stelle, zB ein Unternehmen, dann nicht als identifizierbar gilt, wenn diese die betroffene Person nicht identifizieren kann.

Art. 9 Abs. 1 DSGVO wird um die Klarstellung ergänzt, dass sensible Daten, inkl. Gesundheitsdaten und Daten zur sexuellen Orientierung, **unmittelbar aus der Verarbeitung** hervorzugehen haben. Außerdem soll neu geregelt werden, dass sensible Daten für die **Entwicklung und den Betrieb von KI-Systemen** ebenso wie biometrische Daten, wenn zur Identitätsfeststellung notwendig, verarbeitet werden können.

[23] https://kurzlinks.de/i4a4
[24] https://kurzlinks.de/hdmo
[25] https://kurzlinks.de/h9f3
[26] https://kurzlinks.de/tulk
[27] https://kurzlinks.de/s25m

Weiters wird – in Verbindung mit dem neuen **Art. 88c DSGVO** – auch die Verarbeitung biometrischer Daten im Zusammenhang mit KI-Systemen unter bestimmten Voraussetzungen als rechtmäßig anerkannt.

In **Art. 12 Abs. 5 DSGVO** soll klargestellt werden, dass einem **Auskunftsbegehren** dann nicht entsprochen werden muss oder eine Gebühr verlangt werden kann, wenn damit **datenschutzfremde Zwecke** verfolgt werden.

Durch eine Ergänzung **in Art. 13 Abs. 4 DSGVO** ist die Information dann nicht zu erteilen, wenn aufgrund der Datenerhebung klar ist, welche personenbezogenen Daten vom Verantwortlichen verarbeitet werden.

Die **Meldung von Datenschutzvorfällen** nach **Art. 33 DSGVO** soll künftig auf ein **hohes Risiko** abgestellt binnen **96 Stunden** anstatt aktuell binnen 72 Stunden erfolgen. Weiteres sollen alle **Meldungen an Behörden** künftig über ein **einheitliches Portal** mittels einheitlichem, durch den Europäischen Datenschutzausschuss zu erstellenden Formular erfolgen. Diese Änderungen würden definitiv Erleichterungen im administrativen Aufwand von Data Breach Meldungen bedeuten.

Weiters soll mittels Ergänzung des **Art. 35 DSGVO** der Europäische Datenschutzausschuss eine für alle EU-Länder **harmonisierte Black bzw. White List** bzgl. der **Datenschutzfolgenabschätzung** (DSFA) erstellen. In Österreich wurden Listen für Verarbeitungstätigkeiten, für die eine verpflichtende (sog. Black-List[28]) oder keine (sog. White List[29]) DSFA durchzuführen ist, bereits erstellt und mittels Durchführungsrechtsakt erlassen. EU-weit würde dies aber zu administrativen Erleichterungen führen, da derartige Listen in anderen Ländern der EU häufig nicht existieren. Zusätzlich würde es durch diese Vereinheitlichung mehr Rechtssicherheit im Bereich der DSFA geben.

Die neuen Bestimmungen in Art. 88a, 88b und 88c DSGVO betreffen Ergänzungen im Zusammenhang mit der (zusätzlichen) rechtmäßigen Verarbeitung personenbezogener Daten. **Art. 88a DSGVO** behandelt die **Verarbeitung im Zuge von Datenendgeräten,** welche bisher unter die e-Privacy-Richtlinie fallen. Die rechtliche Beurteilung und Prüfung von Cookies fiele damit künftig unter die DSGVO. Die Zustimmung oder Ablehnung eines Users soll nunmehr für 6 Monate gültig sein und ist erst danach wieder einzuholen.

Durch den neuen **Art. 88b DSGVO** kommt es zu einem neuen Management von Cookies. Die **Cookie-Thematik**, speziell Cookie Banner, soll **einheitlich geregelt** werden, wobei explizit Medienunternehmen von dieser Regelung ausgenommen werden.

Schließlich normiert **Art. 88c DSGVO**, dass die **Verarbeitung** personenbezogener Daten für die **Entwicklung oder den Betrieb eines KI-Systems aufgrund des berechtigten Interesses** nach Art. 6 Abs. 1 lit. f DSGVO erfolgen kann und somit rechtmäßig ist.

Weiteres Vorgehen

Alle **Legislativvorschläge** wurden dem **EU-Parlament** und dem **Rat zur Prüfung und Annahme vorgelegt**. In einer aktuellen Aussendung[30] wurde **Michael McNamara als Berichterstatter** für den **Omnibus zum AI Act** ernannt, während der Berichterstatter für den Omnibus bzgl. Änderungen der DSGVO und des Data Act zu Redaktionsschluss noch nicht feststand. Die aktuelle Ratspräsidentschaft Zypern plant bis Ende Juni 2026 zumindest die Ratsinternen Verhandlungen anzuschließen.

Offen bleibt, inwieweit die vorgeschlagenen Änderungen eine Mehrheit finden und in welcher Form.

Aufgrund der vielen Änderungen wird es einige Monate, vielleicht sogar Jahre dauern, bis alle

[28] https://kurzlinks.de/aeuc
[29] https://kurzlinks.de/w126
[30] https://kurzlinks.de/q6qg

Regelungen beschlossen und in Geltung gesetzt werden. Auch sind einige Punkte – zB Art. 41a DSGVO mit Regelungen zur Pseudonymisierung oder Art. 57 DSGVO zum Aufsetzen digitaler Sandboxen – noch nicht final ausgearbeitet. Im vorliegenden Vorschlag sind auch falsche Referenzen (zB die in Art. 4 DSGVO neuen Definitionen Z 32 bis 38, wenn aktuell erst Z 1 bis Z 26 existieren) noch zu korrigieren.

5. Neues aus der Rechtsprechung

Entscheidung des Europäischen Gerichtshofs (EuGH) zu „Russmedia“

Im Fall des rumänischen Plattformbetreibers „Russmedia Digital[31]“ (C C-492/23) befasste sich der Europäische Gerichtshof (EuGH) im Rahmen eines **Vorabentscheidungsverfahrens** u.a. mit der Frage der Verantwortlichkeit von Betreibern und Anbietern von Websites und deren Inhalten.

Auf der betreffenden, als Verkaufsplattform für Produkte und Dienstleistungen angelegten Website waren ohne deren Zustimmung und Information sexuelle Dienstleistungen inklusive persönlicher Daten einer Person angeboten worden. Trotz eines an den Plattformbetreiber gerichteten Löschbegehrens wurden die Daten auf weitere Seiten verbreitet und somit weiterverarbeitet.

Der EuGH befasste sich mit der Frage der **Unterscheidung von Hosting-Provider und Content-Anbieter**. Hosting-Provider stellen die technische Plattform zur Verfügung, während Anbieter (zB Onlineshops) in weiterer Folge auf dieser Plattform eigene Inhalte bereitstellen und somit den „Content“ als Anbieter verwalten.

Der **Betreiber des Online-Platzes** trägt jedenfalls die inhaltliche Verantwortung und ist **Verantwortlicher** nach Art. 4 Z 7 DSGVO.

Den **Anbieter** trifft nach Art. 5 Abs. 2 DSGVO die **Rechenschaftspflicht**, also die Pflicht zur Prüfung der Daten und des Inhalts sowie der Identität der inserierenden Person insb. bei Daten nach Art. 9 DSGVO, und auch die Pflicht, das Vorliegen einer ausdrücklichen Einwilligung oder einer Ausnahme nach Art. 9 DSGVO zu prüfen, bevor er die Daten veröffentlicht oder bei Nichtvorliegen die Veröffentlichung verweigert. **Betreiber** eines Online-Platzes haben als Verantwortliche die Pflicht, neben der Compliance (Art. 24 DSGVO) auch die **geeigneten technischen und organisatorischen Maßnahmen** bzw. die Sicherheit der Verarbeitung nach dem Stand der Technik gemäß Art. 32 DSGVO zu garantieren. Weiters haben sie die **Veröffentlichung von sensiblen Daten** nach **Art. 9 DSGVO** zu kontrollieren, die rechtswidrige missbräuchliche Verarbeitung zu verhindern und die ausdrückliche Einwilligung einzuholen. Auch können sich **Betreiber** laut dieser Entscheidung nicht mehr auf das Haftungsprivileg berufen, welches bis dato nur von der technischen Bereitstellung und nicht der inhaltlichen Befassung ausging.

Das bedeutet künftig für Betreiber von Online-Marktplätzen, dass diese die inserierenden Nutzer zu identifizieren bzw. verifizieren haben. Jedoch trifft auch Anbieter die Verpflichtung, **technische Vorkehrungen** vor der Veröffentlichung, also **proaktiv**, zu treffen, um die missbräuchliche rechtswidrige Verbreitung (u.a. auch das Kopieren von Inhalten) zu vermeiden bzw. verhindern. Der EuGH spricht von „allen nach dem **Stand der Technik** verfügbaren“ Maßnahmen, die iSd Art. 32 DSGVO zu treffen sind und betont in der Entscheidung die Wichtigkeit zur Vornahme datenschutzfreundlicher Voreinstellungen iSd „privacy by design“ sowie „privacy by default“ von Art. 25 DSGVO.

[31] https://kurzlinks.de/lm88

Diese Entscheidung des EuGH bedeutet künftig mehr **Schutz der Persönlichkeitsrechte** und vor Missbrauch. Dadurch wird dem Zweck der DSGVO bzgl. **Schutz der Grundrechte** und Freiheiten Rechnung getragen, es könnte jedoch auch zu einem Wegfall der Anonymität im Internet führen.

Entscheidung des Europäischen Gerichtshofs (EuGH) zum Thema Bodycams

Am 18. Dezember 2025 hat der EuGH eine Entscheidung (C-422/24[32]) zur **Hinweispflicht** bei Aufnahmen durch **Bodycams** getroffen. Auslöser war deren Verwendung durch die Kontrollore des **öffentlichen Verkehrsunternehmens in Stockholm**, welches zur Dokumentation und Verhinderung von Straftaten bei Kontrollen der Fahrgäste Aufnahmen mittels Bodycams durchführte. Der EuGH befasste sich mit der Frage, ob die Informationspflichten nach Art. 13, 14 DSGVO hierauf Anwendung finden. Die schwedische Datenschutzbehörde verhängte wegen des **Verstoßes gegen die Informationsverpflichtung** eine Geldstrafe in Höhe von EUR 355.000. Die Verkehrsbetriebe wandten die Anwendung des Ausnahmetatbestand nach Art. 14 Abs. 5 lit. b DSGVO ein, wonach die Information nicht erfolgen muss, wenn diese unmöglich ist oder einen unverhältnismäßigen Aufwand erfordert.

Der EUGH entschied schließlich im Rahmen eines Vorabentscheidungsverfahrens, dass auf die **Verarbeitung personenbezogener Daten durch Bodycams die Informationsverpflichtungen** nach Art. 13 DSGVO **anzuwenden** sind und den Betroffenen **Datenschutzinformationen (unmittelbar) zu erteilen** sind. Bei der Abgrenzungsprüfung von Art. 13 zu Art. 14 DSGVO stellte der EuGH mit Verweis auf Erw-G 61 fest, dass es dabei auf die Quelle der Daten ankommt. Im Falle der Aufnahme durch eine Bodycam erfolgt die (unwissentliche) Aufnahme und Datenerfassung beim Betroffenen selbst. Die Verarbeitung erfolgt unmittelbar, daher hat auch die Information darüber unmittelbar zu erfolgen und nicht erst zu einem späteren Zeitpunkt.

Bei der Frage, wie diese **Informationspflicht in der Praxis** erfüllt werden kann, gibt der EuGH keine konkreten Empfehlungen, verweist aber auf die **Leitlinien des EDSA**[33], wonach auf erster Ebene die wichtigsten Informationen (Verantwortlicher, Zweck der Verarbeitung, Empfänger, Rechtsgrundlage, Speicherdauer und Recht auf Auskunft) anzugeben sind. Auf zweiter Ebene sind dann die weiteren Angaben zur Verfügung zu stellen.

Zu diesem Zweck könnten etwa Hinweisschilder für die Videoüberwachung in den zu kontrollierenden Fahrzeugen in Türnähe angebracht werden oder Hinweise zB mittels Aufnähern mit den bekannten **Piktogrammen** auf der Kleidung der Kontrolleure erfolgen.

Entscheidung der Österreichischen Datenschutzbehörde (DSB) zur Wächter-Funktion „Watchdog" bei Tesla-Fahrzeugen

Eine Entscheidung[34] inklusive Verhängung einer Geldstrafe in Höhe von EUR 600 traf die DSB Ende 2025 im Zusammenhang mit der Wächterfunktion bei Tesla-Fahrzeugen.

Ausgangspunkt war eine Beschwerde aufgrund der **Videoüberwachungsanlage „Watchdog"** in einem Tesla-Fahrzeug, welche u.a. zum Zweck der Dokumentation von Unfällen bzw. beim Einparken eingesetzt wird. Durch diese Anlage wurden Videos erstellt und dabei sowohl andere Fahrzeuge als auch vorbeigehende Fußgänger aufgenommen.

Die DSB stellte eine **Verletzung von Art. 12** und **Art. 13 DSGVO** aufgrund der Nicht-Erfüllung der Informationsverpflichtung und der nicht vorhandenen Kennzeichnung der Videoüber-

[32] https://kurzlinks.de/ahko
[33] https://kurzlinks.de/bm8m
[34] DSB 29.9.2025, GZ: D550.929 (2025-0.682.666)

wachung fest und verhängte eine Strafzahlung in geringer Höhe.

Diese Entscheidung ist nicht rechtkräftig und es bleibt abzuwarten, wie das Bundesverwaltungsgericht (BVwG) dazu entscheiden wird.

In einem ähnlichen Fall bzgl. der Videoüberwachung „Watchdog" bei Tesla-Fahrzeugen aus 2024 kam das **Bundesverwaltungsgericht**[35] (BVwG) zu ähnlichen Erkenntnissen bzgl. des Verstoßes gegen die Informationspflicht nach Art. 13 DSGVO. Es wurde damals jedoch keine Strafe verhängt, da es zu keiner Aufzeichnung kam.

In der Entscheidung führte das BVwG die Begriffe **„Verantwortlicher"** und **„Verarbeitung"** sowie insb. **„Erfassen" und Erheben" von Daten** näher aus. In diesem Zusammenhang genügt, dass es zu einer **Bilderfassung ohne Aufnahme und Speicherung** kommt, damit der Begriff „Verarbeitung" nach Art. 4 Z 2 DSGVO erfüllt ist. Daher hat eine Information der Betroffenen nach Art. 12, 13 DSGVO zu erfolgen.

Entscheidung des Obersten Gerichtshofs zur Zustimmung zu personalisierter Werbung

In einem seit 11 Jahren anhängigen Verfahren erließ nunmehr der **Oberste Gerichtshof** (OGH) eine Entscheidung[36] zum Thema der **rechtmäßigen Datenverarbeitung** durch den Betreiber META, speziell zu sog. **„Social Plugins"**. Dabei handelt es sich um Verbindungen von Websites oder Apps zu sozialen Netzwerken, erkennbar an den angezeigten Icons, durch die es zu einer Personalisierung der Inhalte für den Nutzer sowie zu Verarbeitungen für Werbezwecke durch diese Dienste kommt.

Einerseits stellte der OGH – nach Entscheidung durch den EuGH – fest, dass die **Verarbeitung personenbezogener Daten zur Personalisierung von Werbung generell rechtswidrig** und unzulässig ist.

Auch kann sich ein Betreiber hierbei nicht auf die Verarbeitung zur Vertragserfüllung berufen, weil insb. auch sensible Daten dabei erhoben werden können.

Weiters entschied der OGH, dass die Verwendung von **Social Plugins** nur zulässig ist, wenn dies **zu technischen Zwecken** passiert **oder eine Einwilligung** des Nutzers **vorliegt**. Außerdem hielt der OGH fest, dass Online-Betreiber wie META verpflichtet sind, über alle verarbeiteten personenbezogenen Daten, insb. auch jenen, die nicht beim Betroffenen erhoben werden, über deren **Herkunft und Empfänger Auskunft** zu erteilen.

Vorherige Entscheidungen zu diesem Thema, wie insb. Schrems gegen Facebook (C-446/21[37]) konnten durch den OGH nicht herangezogen werden, da diese nach dem Zeitpunkt des Schlusses der mündlichen Verhandlung erster Instanz erfolgt sind.

Entscheidung des EFTA-Gerichtshofes zum Thema Kündigung des Arbeitsvertrages eines Datenschutzbeauftragten

Eine spannende Entscheidung zur **Abberufung eines Datenschutzbeauftragten** (DSBA) fasste der für die EFTA-Staaten Norwegen, Island und Liechtenstein als supranationaler Gerichtshof eingerichtete EFTA-Court[38] im Rahmen eines durch den Fürstlichen Obersten Gerichtshof in Liechtenstein vorgelegten **Vorabentscheidungsverfahrens zur Auslegung des Art. 38 DSGVO**. Darin stellte der EFTA-Court fest, dass es bei der **Abberufung eines Datenschutzbeauftragten** immer darauf ankommt, dass diese Abberufung bzw. Kündigung **nicht im Zusammenhang mit der Erfüllung seiner Aufgaben** stehen darf und auch bei einer nationalen Regelung zur Kündigung eines DSBA immer darauf zu achten ist, dass die nationale Regelung nicht

[35] BVwG 27.3.2024 GZ: W214 2259197-1/14E
[36] OGH 26.11.2025, 6 Ob 189/24y
[37] https://kurzlinks.de/tf5q
[38] Entscheidung vom 16.12.2025, E-5/25 https://kurzlinks.de/bhb9

die Verwirklichung der Ziele der DSGVO beeinträchtigt.

Bzgl. der Möglichkeit zur **„Abberufung“** stellte der EFTA-Court fest, dass eine arbeitsrechtliche **Kündigung** davon erfasst, aber nicht darauf beschränkt ist. Das wäre zB der Entzug der Funktion. **Innerstaatlich** ist daher genau zu regeln, welche **Rechtsfolgen eine rechtswidrige Kündigung eines DSBA** hat, zB die Unwirksamkeit der Kündigung oder Schadenersatz. Nationale Gerichte haben zu prüfen, ob die **Abberufung eines DSBA** aufgrund der **Erfüllung seiner Aufgaben** nach der DSGVO erfolgt und daher rechtswidrig ist.

6. Verwaltungsstrafen

Verstoß gegen Informationspflichten sowie Datenübermittlung in Drittland: Strafe gegen ein kroatisches Telekommunikationsunternehmen

Die kroatische Datenschutzbehörde verhängte eine hohe **Geldstrafe**[39] **gegen** ein **Telekommunikationsunternehmen** aufgrund einer Vielzahl von Datenschutzverstößen. Das kroatische Unternehmen hatte über Jahre Leistungen an ein **Unternehmen in Serbien** ausgelagert. Da Serbien als Drittland gilt und es **keinen Angemessenheitsbeschluss zwischen der EU und Serbien** gibt, wurden 2020 Standardvertragsklauseln abgeschlossen. Diese Klauseln wurden jedoch nach ihrem Ablauf am 27. Dezember 2022 nicht erneuert, weshalb es zu einer Datenverarbeitung ohne Rechtsgrundlage kam, da das Unternehmen in Serbien weiterhin uneingeschränkt personenbezogene Daten von über 800.000 Personen verarbeitete.

Außerdem unterblieb sowohl eine angemessene **Risikoabschätzung** als auch die **Information der Betroffenen** nach Art. 13 DSGVO über den Drittlandsdatentransfer, und schließlich existierte auch keine gültige Auftragsverarbeitervereinbarung. Im Zuge der Prüfung der Aufsichtsbehörde wurde außerdem festgestellt, dass durch das serbische Unternehmen Daten aus Personalausweiskopien und Führungszeugnisse von Mitarbeitern verarbeitet wurden, was einen Verstoß gegen den **Grundsatz der Datenminimierung** nach Art. 5 Abs. 1 lit. c DSGVO darstellt.

Darüber hinaus ist das kroatische Unternehmen als Verantwortlicher seiner Pflicht zur Prüfung des Schutzes personenbezogenen Daten beim serbischen Auftragsverarbeiter, insb. mittels Einhaltung der technischen und organisatorischen Maßnahmen, nicht nachgekommen. Aufgrund der Summe der Datenschutzverstöße wurde eine **Geldstrafe in Höhe von EUR 4,5 Mio.** verhängt.

Hierbei zeigt sich, wie wichtig es ist, bei der Datenverarbeitung im Drittland einerseits die rechtliche Situation bzgl. **Angemessenheitsbeschlüssen** zu kennen und aktuelle Standardvertragsklauseln zu vereinbaren, sowie andererseits auch Themen wie die **Auftragsverarbeitung** genau zu prüfen.

Verwaltungsstrafe der spanischen Datenschutzbehörde aufgrund Videoüberwachung und Verarbeitung biometrischer Daten – Fall 1

Die spanische Datenschutzbehörde verhängte Ende 2025 mehrere Strafen wegen rechtswidriger Datenverarbeitung im Zusammenhang mit Videoüberwachungen. Der erste Fall[40] betraf die **internationale Universität von Valencia**, gegen die eine **Geldstrafe in Höhe von EUR 650.000** verhängt wurde. Die Universität hatte zur Betrugserkennung bei Prüfungen ein **KI-Tool zur Gesichtserkennung** eingesetzt. Dabei wurden Daten zur Identifizierung der Studenten während der Prüfung er-

[39] https://kurzlinks.de/lrqj

[40] https://www.aepd.es/documento/ps-00067-2024.pdf

fasst und mittels **Videoüberwachung** ein Abgleich mit ihren **biometrischen Daten** gemacht. Die Studenten wurden zwar informiert, jedoch wurden Widersprüche gegen die Verarbeitung von der Universität zurückgewiesen und keine Alternative zur Verarbeitung biometrischer Daten angeboten.

Die spanische Datenschutzbehörde befand, dass es **weniger invasive Möglichkeiten** wie Vor-Ort-Kontrollen gäbe, um Betrug durch Studenten bei Prüfungen zu verhindern. Bei der Verarbeitung von **biometrischen Daten** sind die Maßstäbe von **Art. 9 DSGVO** anzuwenden. Eine **Einwilligung** nach Art. 9 Abs. 2 lit. a DSGVO käme aufgrund des **Machtungleichgewichts** zwischen Studenten und Universität und vor dem Hintergrund, dass es keine Alternative gibt, nicht in Betracht. Außerdem verstoße die Universität gegen den **Grundsatz der Datenminimierung** nach Art. 5 Abs. 1 lit. c DSGVO, da eine dauerhafte Gesichtserkennung für die Kontrolle nicht notwendig ist.

Anhand dieser Entscheidung zeigt sich, dass vor dem Einsatz von KI immer zuallererst **datenschutzrechtliche Aspekte** zu prüfen sind, insbesondere wenn es um die **Verarbeitung** von sensiblen oder **biometrischen Daten** nach Art. 9 DSGVO geht.

Verwaltungsstrafe der spanischen Datenschutzbehörde aufgrund Videoüberwachung und Verarbeitung biometrischer Daten – Fall 2

Eine weitere spannende Entscheidung[41] der spanischen Datenschutzbehörde betrifft das **Unternehmen Aena**, welches zahlreiche Flughäfen in Spanien wie zB Madrid-Barajas und Barcelona El-Prat betreibt. Das Unternehmen hatte im Rahmen eines Pilotprojekts auf insgesamt acht Flughäfen eine Videoüberwachung bzw. **Gesichtserkennung mittels Verarbeitung biometrischer Daten** für das Passieren von Sicherheitskontrollen oder das Boarding von Flügen eingesetzt. Die spanische Datenschutzbehörde stellte bei ihrer Prüfung fest, dass im Vorfeld eine **mangelhafte Risikoanalyse** durchgeführt wurde. Darüber hinaus kam es durch die Gesichtserkennung zur Verarbeitung von mehr Daten, als für den Zweck notwendig, und damit zu einem **Verstoß gegen den Grundsatz der Datenminimierung** nach Art. 5 Abs. 1 lit. c DSGVO. Weiters wäre die Verarbeitung weder notwendig noch verhältnismäßig gewesen und es gäbe laut Aufsichtsbehörde **weniger invasive Alternativen** zur Erfüllung des Zwecks.

Schließlich wurde im Zuge der Einführung der Videoüberwachung eine **mangelhaft durchgeführte Datenschutzfolgenabschätzung** (DSFA) festgestellt und die Behörde sah ein hohes Maß an Gefahr für die Rechte der Personen als gegeben an. Die **Aufsichtsbehörde untersagte die Verarbeitung** aller biometrischen Daten durch Aena auf den jeweiligen Flughäfen bis zur ordnungsmäßigen Durchführung der DSFA und verhängte eine **Strafe in Höhe von über EUR 10 Mio.**

Die Betreiberfirma Aena legte Berufung gegen diese Entscheidung an und kündigte gleichzeitig rasche datenschutzkonforme Lösungen an.

Anhand dieser Entscheidung zeigt sich die Notwendigkeit einer **korrekt** durchgeführten und **vollständigen DSFA** vor der Einführung neuer Technologien wie insb. Gesichtserkennung, einschließlich der **Berücksichtigung aller Risikogesichtspunkte** und der möglichen **Gefahren** für Betroffene.

[41] https://www.aepd.es/documento/ps-00431-2024.pdf

7. In eigener Sache: Neu an Bord

Im Oktober wurde unser Secur-Data-Team um Frau **Mag. Gertraud Wisiak** verstärkt. Durch ihre jahrelange Tätigkeit als Juristin und Datenschutzbeauftragte in der Finanzbranche bringt sie wertvolle Expertise für die Betreuung unserer Kunden mit.

••••

Datenschutz-Seminar 2026

Die Entwicklung des nationalen und internationalen Datenschutzes geht weiter, auch 2026 sind neue rechtliche Entscheidungen und Aktualisierungen zu erwarten. Lassen Sie sich im bewährt kleinen Kreis von unseren Top-Expertinnen und -Experten über alle wesentlichen Neuerungen in Angelegenheiten der Informationssicherheit und der Datenschutzpraxis informieren!

Neben praxisnaher Wissensvermittlung steht Secur-Data für State-of-the-Art-Anwendungstipps sowie praxistaugliche Muster und Vorlagen. Auch heuer wird Ihnen wieder **ein Vertreter der österreichischen Datenschutzbehörde** aktuelle Judikatur der DSB präsentieren und auf Ihre Fragen eingehen.

24. März 2026, 9:15 – 17:00 Uhr:

„Rechtliche Themen und Entwicklungen (Modul 1)“

Referenten: Prof. KommR Hans-Jürgen Pollirer, Mag. Judith Leschanz, Mag. Gertraud Wisiak, Mag. Rona Paca

Gastreferent: Vertreter der Österreichischen Datenschutzbehörde

25. März 2026, 9:15 – 17:00 Uhr:

„Praktische Umsetzung (Modul 2)“

Referenten: Prof. KommR Hans-Jürgen Pollirer, Mag. Judith Leschanz, Mag. Gertraud Wisiak, Friedrich Tuma, Mag. Krzysztof Müller

Ort: Hilton Vienna Plaza, Schottenring 11, 1010 Wien

Selbstverständlich stehen wir auch für Inhouse-Schulungen oder Seminare zu Spezialthemen zur Verfügung.

Hier geht’s zur Anmeldung: www.secur-data.at oder telefonisch unter (01) 533 42 07-0.

Save the Date – Privacy Ring 2026 in Liechtenstein

Der Datenschutzverein Privacy Ring[42] lädt am **12. Februar 2026** zur inzwischen 15. Fachtagung in Vaduz, Liechtenstein ein. Diesmal steht das Thema **Datenschutz und neue Technologien - zwischen Regulierung und Praxis** im Fokus. Die Teilnahme ist kostenlos.

[42] https://www.privacy-ring.uni-hannover.de/de/