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 2025 Ausgabe Nr. 116

Liebe Leserinnen und Leser,

Ein frohes neues Jahr und herzlich willkommen zur ersten Ausgabe der DSG-Info im Jahr 2025! Wir freuen uns, Sie auch in diesem Jahr mit den wichtigsten Neuigkeiten und Analysen rund um den Datenschutz zu begleiten.

2025 wird ein entscheidendes Jahr für den regulatorischen Rahmen in der EU: In dieser Ausgabe beleuchten wir zentrale neue Rechtsakte, die ab diesem Jahr wirksam werden. Darunter der Digital Operational Resilience Act (DORA), die NIS-2-Richtlinie, die in Österreich noch der nationalen Umsetzung bedarf, und der AI Act, dessen erste inhaltliche Bestimmungen heuer in Kraft treten. Diese Regelwerke werden Unternehmen und Behörden gleichermaßen fordern – wir erklären, was Sie jetzt wissen und beachten müssen.

Im April informieren wir Sie im Rahmen unseres diesjährigen Datenschutz-Praxisseminars über aktuelle Entwicklungen und Best Practices. Nähere Infos finden Sie hier und in unserer DSG-Info.

Außerdem freuen wir uns, Ihnen unsere neue Website vorzustellen! Dort finden Sie künftig alle Artikel, weiterführende Ressourcen und eine Übersicht unseres Beratungsangebots. Schauen Sie vorbei und entdecken Sie unser neues Design.

Wir wünschen Ihnen eine spannende Lektüre und einen erfolgreichen Start ins Jahr 2025!

Mag. Judith Leschanz
Geschäftsführung

1. Neues Jahr – neues Gesetz: Digital Operational Resilience Act (DORA)

Am 16. Jänner 2023 ist die VO (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Betriebsstabilität digitaler Systeme des Finanzsektors **(„Digital Operational Resilience Act“**; DORA) in Kraft getreten[1]. Sie ist von den betroffenen Unternehmen ab **17. Jänner 2025** verpflichtend anzuwenden. Mit DORA sollen bestehende regulatorische Lücken für den gesamten europäischen Finanzsektor geschlossen und die Betriebsstabilität im Finanzsektor gestärkt werden.

[1] https://kurzlinks.de/67uk

Aufgrund der in DORA enthaltenen Ermächtigung für die Europäische Kommission wurden noch folgende Rechtsakte erlassen:

- DELEGIERTE VERORDNUNG (EU) 2024/1502 DER KOMMISSION vom 22. Februar 2024[2] zur Ergänzung der VO (EU) 2022/2554 des Europäischen Parlaments und des Rates durch Festlegung der Kriterien für die Einstufung von IKT-Drittdienstleistern als für Finanzunternehmen kritisch
- DELEGIERTE VERORDNUNG (EU) 2024/1505 DER KOMMISSION vom 22. Februar 2024[3] zur Ergänzung der VO (EU) 2022/2554 des Europäischen Parlaments und des Rates durch Festlegung der Höhe der von der federführenden Überwachungsbehörde bei kritischen IKT-Drittdienstleistern zu erhebenden Überwachungsgebühren und der Art und Weise der Entrichtung dieser Gebühren

Zum Wirksamwerden der DORA-VO wurde vom österreichischen Gesetzgeber am 18. April 2024 ein Vollzugsgesetz (DORA-Vollzugsgesetz, DORA-VG) veröffentlicht, das im Finanzausschuss am 27. Juni 2024 die Stimmenmehrheit von ÖVP, SPÖ, Grünen und Neos erhielt und am 3. Juli 2024 im NR beschlossen wurde.[4] Das Gesetz soll insb. den Anwendungsbereich der DORA-VO in Bezug auf die nationalen Institute klarstellen. In Österreich ist die **Finanzmarktaufsicht (FMA)** für den Vollzug von DORA zuständig.

Durch die von den Unternehmen aufgrund der in DORA normierten Bestimmungen umzusetzenden Maßnahmen sollen folgende Ziele erreicht werden:

- IKT-Risikomanagement (Kapitel II, Art. 5 bis 16)
- Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle (Kapitel III, Art. 17 bis 23)
- Testen der digitalen operationellen Resilienz einschließlich Threat-led Penetration Testing (TLPT) (Kapitel IV, Art. 24 bis 27)
- Management des IKT-Drittparteienrisikos (Kapitel V, Abschnitt I, Art. 28 bis 30)
- Überwachungsrahmen für kritische IKT-Drittdienstleister (Kapitel V, Abschnitt II, Art. 31 bis 44)
- Vereinbarungen über den Austausch von Informationen und Erkenntnissen zu Cyberbedrohungen (Kapitel VI, Art. 45)

Grundsätzlich stellt sich die Frage, warum die EU zwei Rechtsvorschriften für Cybersicherheit, nämlich die **NIS-2-RL** und die **DORA-VO** erlassen hat, die auf den ersten Blick ähnlich anmuten. Bei näherer Betrachtung dieser beiden Rechtsvorschriften zeigen sich jedoch einige wesentliche Unterschiede. Während NIS-2 als RL in nationales Recht umgesetzt werden muss,[5] handelt es sich bei DORA um eine VO, die zeitgleich in allen Mitgliedstaaten in Kraft tritt und unverändert in ihrer Gesamtheit durchgesetzt werden muss. Während die NIS-2-RL veröffentlicht wurde, um das allgemeine Niveau der Cybersicherheit in der EU zu vereinheitlichen (was durch NIS-1 nicht gelungen ist), soll die Umsetzung der Anforderungen der DORA-VO den europäischen Finanzsektor in die Lage versetzen, Cyberangriffen standzuhalten und betriebsfähig zu bleiben. Der Fokus von DORA liegt daher auf der **Verfügbarkeit** und **Integrität** von Finanzdienstleistungen.

Auch in Bezug auf den Umsetzungszeitpunkt sowie in der Behördenzuständigkeit ergeben sich Unterschiede. Während die Bußgelder in der NIS-2-RL festgelegt sind, wird die Festle-

[2] https://kurzlinks.de/7v3d
[3] https://kurzlinks.de/hk4p
[4] https://kurzlinks.de/xvd8
[5] *Pollirer*, Checkliste NIS-2, Dako 2024/43

gung und Bewertung der Sanktionen in DORA den Mitgliedstaaten überlassen.

DORA legt besonderen Wert auf die **Sicherheit der Lieferkette** und geht über die Anforderungen der NIS-2-RL weit hinaus. So müssen Finanzunternehmen die Risiken über die **gesamte** Lieferkette identifizieren und in entsprechenden Verzeichnissen dokumentieren. Verträge mit IKT-Dienstleistungsunternehmen dürfen nur mit Anbietern abgeschlossen werden, die über hohe und aktuelle Informationssicherheitsstandards verfügen.

DORA gilt – mit wenigen Ausnahmen – grundsätzlich für alle regulierten Finanzunternehmen in der EU und insbesondere auch für IKT-Dienstleister, die von diesen Unternehmen eingesetzt werden. Als **lex specialis** geht DORA der NIS-2-RL vor. Nichtsdestotrotz kann es zu Mehrfachregulierungen kommen, und zwar für Unternehmen im IT- und TK-Sektor, die sowohl als NIS-2-Einrichtungen als auch als kritische IKT-Dienstleister nach DORA gelten. Im Einzelnen sind gem. § 2 DORA-VG insbesondere folgende Unternehmen des Finanzsektors betroffen: Kreditinstitute, Zahlungsinstitute, E-Geld-Institute, Wertpapierfirmen, Anbieter von Kryptowerte-Dienstleistungen und Emittenten von vermögenswertreferenzierten Token, Handelsplätze, Datenbereitstellungsdienste, Verwaltungsgesellschaften, Unternehmen gem § 1 Z 1 VAG sowie Pensionskassen. Somit fallen so gut wie alle beaufsichtigten Unternehmen des europäischen Finanzsektors unter die Bestimmungen von DORA. Darüber hinaus sind auch **kritische IKT-Dienstleister**, die für Finanzunternehmen tätig sind, von DORA betroffen, wobei die Einstufung als „kritisch“ vom Finanzunternehmen erfolgt.

Die Anforderungen, die DORA an Finanzunternehmen mit Geschäftstätigkeit in der EU festlegt, werden in technischen **Regulierungsstandards** (Regulatory Technical Standards, „RTS“) und **Durchführungsstandards** (Implementing Technical Standards, „ITS“) konkretisiert. Die drei europäischen Aufsichtsbehörden European Banking Authority (**EBA**), European Insurance and Occupational Pensions Authority (**EIOPA**) und die European Securities and Markets Authority (**ESMA**) haben im März und Juli 2024 die zwei finalen Pakete von RTS und ITS der Europäischen Kommission vorgelegt. Bisher wurden aber noch nicht alle dieser Standards von der Kommission angenommen.

- **Sicherheitstests:** Mindestens jährliche Prüfungen kritischer Systeme
- **Drittparteienmanagement:** Effiziente Überwachung Ihrer IKT-Partner

Ihr Vorteil:

- ✓ Mit unserer **praxisorientierten Beratung** vermeiden Sie Unsicherheit und schaffen eine nachhaltige Grundlage für Ihre digitale Resilienz. Profitieren Sie von unserer Expertise, um Bußgelder zu vermeiden und einen rechtssicheren Status zu erreichen – maßgeschneidert auf Ihre Bedürfnisse, **effizient** und **praxisnah**.

Bereiten Sie sich frühzeitig vor – wir begleiten Sie auf dem Weg zur DORA-Konformität!

2. Neue NIS-RL erweitert Anwendungsbereich

Die **NIS-2-RL** (RL (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union)[6] ist die Nachfolgerin der ursprünglichen RL für die Netz- und Informationssicherheit aus dem Jahr 2016,[7] die am 28. Dezember 2018 mit dem NISG[8] umgesetzt wurde. Die aufgrund der Bestimmungen des § 4 Abs. 2 NISG erforderliche Netz- und Informationssystemsicherheitsverordnung (NISV)[9] wurde am 17. Juli 2019 verlautbart.

Die Definition der neuen NIS-2-RL wurde notwendig, weil die ursprüngliche NIS-RL nicht einheitlich in den Mitgliedstaaten umgesetzt wurde und dadurch ein fragmentiertes Regelwerk entstand. Mit der NIS-2-RL sollen nun diese Unzulänglichkeiten durch folgende wesentliche Ansätze beseitigt werden:

- Harmonisierung und Verbesserung des Sicherheitsniveaus in den Mitgliedstaaten
- Definition und Umsetzung von Cybersicherheitsstrategien und Risikomanagement-Abläufen
- Verschärfte Sanktionen bei Verstößen
- Zuverlässige Meldung von Sicherheitsvorfällen bei den zuständigen Stellen
- Gewährleistung der durchgängigen Bereitstellung kritischer Dienste
- Definition und Umsetzung von Sicherheitsmaßnahmen für die Lieferkette, um die Sicherheit externer Anbieter zu überprüfen und zu gewährleisten
- Implementierung eines Asset-Managements, um kritische Informationssysteme zu identifizieren und zu schützen

Darüber hinaus wurde der Anwendungsbereich wesentlich erweitert, wie die Tabelle unten zeigt. Im Unterschied zur ursprünglichen NIS-RL wurden die von der NIS-2-RL betroffenen Einrichtungen in „**wesentliche Einrichtungen**“, die einer strengen ex-ante- und ex-post-Aufsicht (Art. 32 NIS-2-RL) sowie in „**wichtige Einrichtungen**“, die nur einer ex-post-Aufsicht (Art. 33 NIS-2-RL) unterliegen, unterteilt. Des Weiteren wächst auch die Forderung nach mehr Cyber-Sicherheit stetig und erfordert neue Maßnahmen, um der **Entwicklung der**

[6] https://kurzlinks.de/75c5
[7] Richtlinie (EU) 2016/1148, https://kurzlinks.de/2hur
[8] https://kurzlinks.de/5vrd
[9] https://kurzlinks.de/8xgo

Bedrohungslandschaft und der **steigenden Cyberkriminalität** entgegenzuwirken. Waren von der NIS-RL noch rund 100 Organisationen und Unternehmen in Österreich betroffen,[10] so gilt NIS-2 für mehr als 5.000 Organisationen und Unternehmen sowie für schätzungsweise 50.000 Unternehmen, die diese Gruppe als Lieferanten versorgen.[11]

Betroffene Sektoren

Anhang I (= Sektoren mit hoher Kritikalität)	Anhang II (= sonstige kritische Sektoren)
Energie (Elektrizität, Fernwärme/Kälte, Öl, Gas und Wasserstoff)	Post- und Kurierdienste
Verkehr (Luft, Schiene, Schifffahrt, Straße)	Abfallbewirtschaftung
Bankwesen	Chemie (Herstellung und Handel)
Finanzmarktinfrastrukturen	Lebensmittel (Produktion, Verarbeitung, Vertrieb)
Gesundheitswesen (Gesundheitsdienstleister, EU-Referenzlaboratorien, Forschung und Herstellung von pharmazeutischen und medizinischen Produkten und Geräte)	Verarbeitendes / Herstellendes Gewerbe (Medizinprodukten; Datenverarbeitungs-, elektronische und optische Geräte und elektronische Ausrüstungen; Maschinenbau; Kraftwagen und Kraftwagenteile und sonstiger Fahrzeugbau)
Trinkwasser	Anbieter digitaler Dienste (Suchmaschinen, Online-Marktplätze und soziale Netzwerke)
Abwasser	Forschung
Digitale Infrastruktur (IXP, DNS, TLD, Cloud-Computing, Rechenzentren, CDN, TSP und Anbieter öffentlicher elektronischer Kommunikationsnetze- und dienste)	
Verwaltung von IKT-Diensten (B2B)	
Öffentliche Verwaltung	
Weltraum	

Rot = Neuerungen gegenüber NIS1

(Quelle: bundeskanzleramt.gv.at)

Betroffen sind mittlere und große Unternehmen bestimmter Sektoren, sowie die digitale Infrastruktur. Die Klassifizierung der Unternehmensgröße basiert auf Empfehlungen und Definitionen der EK für KMU.

[10] https://www.wko.at/it-sichherheit/nis2

[11] https://www.cxber-trust.at/nis/

Größenklasse	Mitarbeiter (VZÄ)	Jahresumsatz	Jahresbilanzsumme
Klein (KU)	< 50 und	≤ 10 Mio. EUR oder	≤ 10 Mio. EUR
Mittel (MU)	< 250 und	≤ 50 Mio. EUR oder	≤ 43 Mio. EUR
Groß (GU)	≥ 250 oder	> 50 Mio. EUR und	> 43 Mio. EUR

Kleinunternehmen fallen nicht unter die NIS-2-RL, **außer** es handelt sich um

- Vertrauensdiensteanbieter,
- Anbieter öffentlicher Kommunikationsnetze oder Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste,
- TLD-Namensregister und DNS-Diensteanbieter, ausgenommen Betreiber von Root-Namensservern,
- Unternehmen, die alleiniger Anbieter eines Service in einem Mitgliedstaat sind, das essentiell für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Aktivitäten ist.

Darüber hinaus sind auch **Zulieferer und Dienstleister** von NIS-2-Unternehmen durch die Verpflichtung zur Gewährleistung der Sicherheit der **Lieferkette** ihrer Kunden verpflichtet, Cybersecurity-Maßnahmen umzusetzen (Art. 22 NIS-2-RL).

Art. 21 Abs. 5 NIS-2-RL sieht vor, dass die Europäische Kommission Durchführungsrechtsakte[12] zu den in Art. 21 Abs. 2 NIS-2-RL angeführten zehn Maßnahmen zum Schutz der Netz- und Informationssysteme vor Sicherheitsvorfällen erlässt. Sie betreffen DNS-Diensteanbieter, TLD-Namenregister, Cloud-Computing-Dienstleister, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter.

Gem Art. 21 NIS-2-RL haben die Mitgliedstaaten sicherzustellen, dass die wesentlichen und wichtigen Einrichtungen geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, und zwar unter Berücksichtigung des Stands der Technik, europäischer und internationaler Normen, sowie des bestehenden Risikos.

Diese Maßnahmen müssen gem Art. 21 Abs. 2 NIS-2-RL zumindest Folgendes umfassen:

1. Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme
2. Bewältigung von Sicherheitsvorfällen
3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement
4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen

[12] https://kurzlinks.de/5qe0

6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit
7. grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit
8. Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung
9. Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen
10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung

Verstöße gegen die Bestimmungen der NIS-2-RL können bei wesentlichen Einrichtungen mit einer maximalen **Geldbuße in Höhe von 10 Mio. EUR oder 2 % des weltweiten Umsatzes** sanktioniert werden, je nachdem, welcher Betrag höher ist. Für wichtige Einrichtungen beträgt die maximale Höhe der **Geldbuße 7 Mio. EUR oder 1,4 % des weltweiten Umsatzes**, je nachdem, welcher Betrag höher ist.

Die NIS-2-RL ist am 16. Jänner 2023 in Kraft getreten und war von den **EU-MS bis 17. Oktober 2024** in nationales Recht umzusetzen. Der österreichische Gesetzgeber legte am 3. April 2024 den Entwurf des Netz- und Informationssystemsicherheitsgesetz 2024 (**NISG 2024**) vor, der am 19. Juni 2024 mit den Stimmen der ÖVP und der Grünen mehrheitlich den Innenausschuss passierte. Bei der Abstimmung im Parlament am 3. Juli 2024 fand sich allerdings keine Zweidrittelmehrheit für das NISG 2024, das daher vorerst **nicht beschlossen** wurde. Bedingt durch die Wahlen zum NR am 29. September 2024 und die aktuellen Regierungsverhandlungen wird es daher zu einer erheblichen Verzögerung bei der Umsetzung der NIS-2-RL in nationales Recht kommen.

- **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 NISG 2024 gerecht werden.
- ✓ **Effizientes 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 NIS-2-Anforderungen. Mit unserer Unterstützung sind Sie bestens vorbereitet, um die neuen gesetzlichen Pflichten effizient und nachhaltig zu erfüllen.

Kontaktieren Sie uns für eine individuelle Beratung .

3. KI-Gesetz: Europäische Initiative tritt schrittweise in Kraft

Der **AI Act**[13] ist der erste Rechtsrahmen der EU für Künstliche Intelligenz und soll nach Ansicht der Europäischen Kommission Europa in die Lage versetzen, weltweit eine führende Rolle bei der Festlegung von globalen Standards zu spielen. Er ist Teil eines umfassenden Pakets politischer Maßnahmen zur Unterstützung und Entwicklung vertrauenswürdiger KI, zu dem auch das KI-Innovationspaket[14] und der koordinierte KI-Plan[15] sowie die **AI Liability Directive**[16] gehören, die Vorschriften zu außervertraglichen Haftungsfragen iZm KI-Systemen regeln soll. Des Weiteren ist auch eine Überarbeitung der sektoralen Sicherheitsvorschriften (zB Produktsicherheit) geplant.

Der AI Act ist sehr umfangreich, er enthält 180 Erwägungsgründe, 113 Artikel und 13 Anhänge. Er fordert, dass KI-Anwendungen nicht nur effizient, sondern auch sicher, transparent, ethisch korrekt und grundrechtskonform gestaltet sein müssen.

Art. 3 Z 1 **definiert** ein KI-System wie folgt:

ein maschinengestütztes 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 können;“

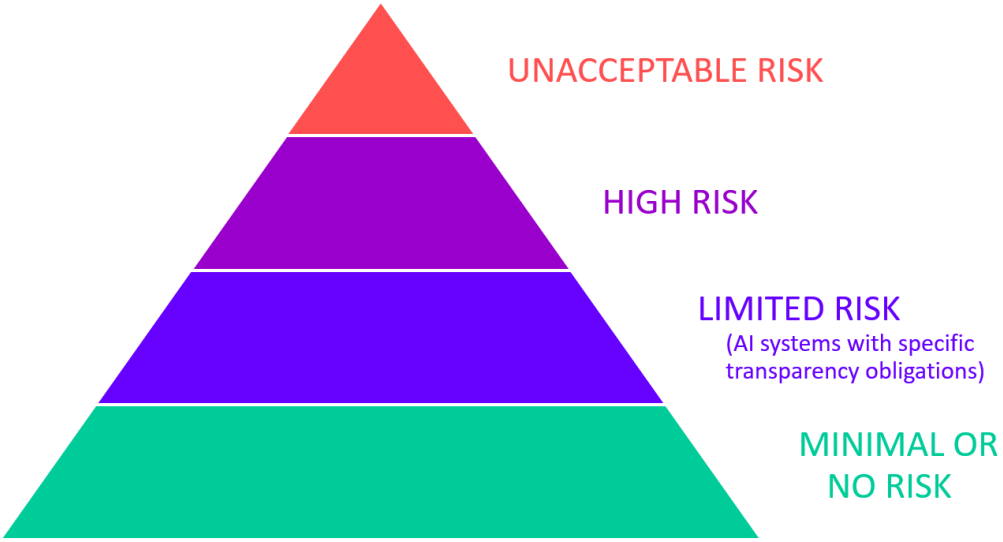
Die Nichtbeachtung der Bestimmungen des AI Act ist mit **hohen Bußgeldern** verbunden und zwar:

- bis zu **35 Mio. EUR bzw. 7 % des weltweiten Jahresumsatzes** (abhängig davon, welcher Wert höher ist) bei Missachtung der in Art. 5 genannten KI-Praktiken in Bezug auf verbotene KI-Systeme oder die Nichteinhaltung der Anforderungen an Daten.
- bis zu **15 Mio. EUR bzw. 3 % des weltweiten Jahresumsatzes** (abhängig davon, welcher Wert höher ist) bei Verstößen gegen geltende Bestimmungen für Anbieter (Art. 16), Bevollmächtigte (Art. 22) sowie Einführer (Art. 23), Händler (Art. 24), Betreiber (Art. 26), notifizierte Stellen (Art. 31, 33 Abs. 1, 3 und 4, Art. 34), Transparenzpflichten für Anbieter und Nutzer (Art. 50).
- Bis zu **7,5 Mio. EUR bzw. 1 % des weltweiten Jahresumsatzes** (abhängig davon, welcher Wert höher ist) bei Falschaussagen bzw. unvollständigen oder irreführenden Informationen an notifizierte Stellen oder zuständige Behörden.

Im Falle von KMUs gilt aber der jeweils niedrigere Betrag.

Kern des AI Act ist ein **risikobasierter Ansatz**, wobei das Risikopotential anhand der nachstehenden vier Risikofelder qualifiziert wird:[17]

[13] https://kurzlinks.de/zmk1
[14] https://kurzelinks.de/0yjn
[15] https://kurzelinks.de/wbqa
[16] https://kurzelinks.de/faii
[17] Quelle: https://kurzelinks.de/2dxo



- **Inakzeptables Risiko**: Betrifft KI-Systeme, die eine eindeutige Bedrohung für die Sicherheit, die Lebensgrundlage und die Menschenrechte darstellen. Darunter fallen zB KI-Systeme wie Social Scoring, die Menschen sozial bewerten und Systeme zur biometrischen Klassifizierung in Bezug auf die in den Art. 9 und 10 DSGVO als besonders schützenswert angeführten Daten (Art. 5).
- **Hohes Risiko**: Diese Gruppe stellt den bedeutendsten Anwendungsbereich des AI Act dar und ist aufgrund ihrer Risikoneigung besonders stark reglementiert. Sie behandelt den Einsatz von KI-Systemen in sensiblen Lebensbereichen. In diese Gruppe fallen KI-Systeme in kritischen Infrastrukturen (Verkehr, Wasser, Gas-, Wärme- und Stromversorgung), im Bildungs- und Berufswesen (zB Bewerberauswahl), Strafverfolgung, private und öffentliche Dienstleister (zB Bonitätsprüfung) uä (Art. 6 bis 49, Anhang III).
- **Begrenztes Risiko**: Umfasst KI-Systeme, von denen nur ein begrenztes Risiko ausgeht wie zB Chatbots. Für diese Gruppe gelten spezifische Transparenzpflichten (Art. 50, Anhang XII).
- **Minimales Risiko**: Der AI Act erlaubt die freie Nutzung von KI-Systemen mit minimalem Risiko. Diese Gruppe enthält die überwiegende Mehrheit der derzeit in der EU eingesetzten KI-Systeme wie zB Spamfilter oder KI-fähige Videospiele.

In der politischen Diskussion war insb. die Einbeziehung von „General Purpose AI Models“ (GPAI) besonders umstritten. Als „KI-Systeme mit allgemeinem Verwendungszweck“ bezeichnet man KI, die allgemeine Funktionen wie Bild- und Spracherkennung, Videogenerierung, Mustererkennung, Beantwortung von Fragen sowie Übersetzungen usw. ausführt. Darunter fallen Large Language Models (LLM) und andere generative AI-Tools wie ChatGPT, Google Gemini, Bing AI ua. Entsprechend der im AI Act festgelegten Logik werden diese GPAI-Modelle in die dritte Risikostufe eingeordnet. Dabei werden zwei Gruppen unterschieden, und zwar GPAI „mit **allgemeinem Verwendungszweck**“ und GPAI „mit **allgemeinem Verwendungszweck mit systemischem Risiko**“. Diese Differenzierung bezieht sich nicht auf die Anwendung selbst, sondern auf die Rechenleistung und Reichweite des zugrundeliegenden Basismodells. Die Rechenleistung wird in Gleitkomma-

operationen pro Sekunde (Floating Point Operations Per Second, FLOP) gemessen. Art. 51 Abs. 2 legt den **Schwellenwert** für GPAI mit allgemeinem Verwendungszweck mit systemischem Risiko mit 10^{25} FLOP fest.

Der AI Act sieht eine **Verwaltungsstruktur** mit mehreren zentralen Regulierungsbehörden vor, die jeweils unterschiedliche Aufgaben in Bezug auf die Umsetzung und Durchsetzung des AI Act wahrnehmen sollen. Im Einzelnen sind dies:

Auf EU-Ebene:

- Einrichtung eines **Büros für Künstliche Intelligenz**, das die Umsetzung und Durchsetzung des AI Act gewährleisten soll (Art. 64). Es wurde bereits am 24. Jänner 2024 gegründet.
- Des Weiteren wird ein „**Europäisches Gremium für Künstliche Intelligenz**" eingerichtet, das sowohl die Kommission wie auch die Mitgliedstaaten unterstützen soll, um eine einheitliche und wirksame Anwendung des AI Act zu erleichtern (Art. 65).
- Ein **Beratungsforum** aus unabhängigen Experten soll den Ausschuss und die Kommission beraten (Art. 67).
- Schlussendlich soll ein **wissenschaftliches Gremium unabhängiger Sachverständiger** eingerichtet werden, das die Durchsetzungstätigkeiten im Rahmen des AI Act unterstützen soll (Art. 68).

Auf nationaler Ebene:

- Jeder MS muss mindestens eine notifizierende Behörde einrichten, die insb. KMU einschließlich Start-up-Unternehmen bei der Durchführung des AI Act zur Seite stehen und die ordnungsgemäße und rechtzeitige Durchführung von Konformitätsbewertungen sicherstellen soll (Art. 70). Vorerst wurde mit Beschluss des Nationalrates vom 21. Jänner 2024 eine KI-Servicestelle in der Rundfunk und Telekom Regulierungs-GmbH (RTR) eingerichtet, die in einem weiteren Ausbauschritt in eine KI-Behörde übergeht.
- Jeder MS muss darüber hinaus auch mindestens eine Marktüberwachungsbehörde einrichten, die zur Durchführung externer Konformitätsbewertungen berechtigt ist (Art. 70).

Vom AI Act sind unterschiedliche Akteure betroffen (Art. 2):

- Anbieter
- Betreiber
- Einführer und Händler
- Produkthersteller
- Bevollmächtigte von Anbietern
- betroffene Personen

Der Sitz in einem Drittstaat entbindet Anbieter, Betreiber und Bevollmächtigte nicht von den im AI Act normierten Pflichten, wenn das KI-System für die EU bestimmt ist oder das vom KI-System hervorgebrachte Ergebnis in der EU verwendet wird.

Beratung zu Künstlicher Intelligenz

Rechtskonformer Einsatz von Künstlicher Intelligenz (KI) – Ihre Lösung für sichere Innovation!

In der modernen Geschäftswelt wird der rechtskonforme Einsatz von Künstlicher Intelligenz (KI) zum entscheidenden Wettbewerbsfaktor. Nutzen Sie die Chancen der KI, ohne rechtliche Risiken einzugehen – mit unserer maßgeschneiderten Beratung.

Warum rechtskonforme KI unverzichtbar ist?

Der verantwortungsvolle Umgang mit Daten ist nicht nur gesetzlich vorgeschrieben, sondern stärkt auch das Vertrauen Ihrer Kunden und Partner. Unsere ExpertInnen helfen Ihnen, die gesetzlichen Anforderungen – wie die DSGVO, das DSG und das KI Gesetz (AI Act) – effizient und transparent zu erfüllen.

Unsere Leistungen im Überblick:

- **Rechtskonforme Umsetzung:** Beratung zu nationalen und europäischen Regelungen
- **Risikobewertung und -management:** Durchführung detaillierter Risikobewertungen und Entwicklung von Compliance-Strategien
- **Transparenz und Dokumentation:** Unterstützung bei der Erfüllung von Transparenzanforderungen und lückenloser Dokumentation
- **Schulung und Sensibilisierung:** Schulungen und Workshops für Ihre Führungskräfte und Mitarbeitende

Ihre Vorteile:

- ✓ **Praktische Lösungen, die funktionieren:** Wir kombinieren tiefgehende rechtliche Expertise mit einer Hands-on-Mentalität. Unser Ziel ist es, Sie nicht nur zu beraten, sondern aktiv bei der Umsetzung Ihrer KI-Projekte zu unterstützen. Wir begleiten Sie von der ersten Risikoanalyse bis hin zur finalen Implementierung.
- ✓ **Sicherheit, Effizienz, Wettbewerbsvorteil:** Unsere praxisorientierte Beratung ermöglicht es Ihnen, die Potenziale der KI voll auszuschöpfen – ohne dabei den rechtlichen Rahmen aus den Augen zu verlieren. So sichern Sie sich Effizienzgewinne, stärken Ihre Reputation und minimieren Haftungsrisiken.

Kontaktieren Sie uns jetzt für Ihr individuelles Angebot!

4. EuGH: Abfrage der Geschlechtsidentität bei Bahntickets unzulässig

Der Europäische Gerichtshof (EuGH) hat entschieden (Urteil vom 9.1.2025 - C-394/23)[18], dass Eisenbahnunternehmen ihre Kunden nicht verpflichten dürfen, beim Ticketkauf über die Wahl einer Anrede ihr Geschlecht offenzulegen. Diese Praxis verstößt gegen die Datenschutzgrundverordnung (DSGVO), da eine **geeignete Rechtsgrundlage** für die Verarbeitung fehlt und sie zudem nicht mit dem **Grundsatz der Datenminimierung** vereinbar ist.

Hintergrund des Verfahrens

Anlass des Vorabentscheidungsverfahrens war eine Beschwerde des Verbands Mousse, der sich gegen sexuelle Diskriminierung einsetzt. Mousse beanstandete vor der französischen Datenschutzbehörde CNIL die Praxis des Unternehmens SNCF Connect. Dieses verlangte von seinen Kunden, beim Online-Kauf von Fahrscheinen zwischen den Anreden „Herr“ und „Frau“ zu wählen. Nach Ansicht von Mousse handelt es sich hierbei um eine unverhältnismäßige Datenerhebung, die gegen die Grundsätze der DSGVO verstößt, insbesondere die der Rechtmäßigkeit und der Datenminimierung. Die CNIL wies die Beschwerde jedoch 2021 zurück, woraufhin Mousse den französischen Staatsrat anrief. Dieser legte die Frage dem EuGH vor.

EuGH: Anrede ist nicht erforderlich

Der EuGH stellte klar, dass für die Verarbeitung der gegenständlichen Daten als Rechtsgrundlage nur die **Erfüllung des jeweiligen Vertrags** (Art. 6 Abs. 1 lit. b DSGVO) oder die **Wahrung berechtigter Interessen** (Art. 6 Abs. 1 lit. f DSGVO) in Frage kommen. Im vorliegenden Fall sei die Angabe der Anrede bzw. des Geschlechts für die Erfüllung eines Schienentransportvertrags aber nicht erforderlich. Die ordnungsgemäße Durchführung hänge nicht davon ab, wie ein Kunde angesprochen wird.

Kein berechtigtes Interesse der Unternehmen

Der EuGH verwarf auch die Anwendung der Rechtsgrundlage eines berechtigten Interesses des Unternehmens. Die Datenverarbeitung müsse dafür objektiv notwendig sein und dürfe die Rechte und Freiheiten der betroffenen Personen nicht überwiegen. Die Verpflichtung zur Angabe der Anrede könne jedoch zu einer Diskriminierung aufgrund der Geschlechtsidentität führen und sei daher **nicht verhältnismäßig**. Zudem sei den Kunden das berechtigte Interesse nicht kommuniziert worden, zu dessen Umsetzung diese Daten erhoben wurden.

Bedeutung des Urteils

Das Urteil unterstreicht, dass Unternehmen bei der Verarbeitung personenbezogener Daten strikte Maßstäbe anlegen müssen. Insbesondere der Grundsatz der **Datenminimierung** schränkt die Erhebung von Daten ein, die nicht zwingend notwendig sind. Dies gilt auch für Angaben wie die Anrede oder das Geschlecht.

Für Unternehmen bedeutet das Urteil, dass sie ihre Datenverarbeitungspraxis kritisch prüfen und gegebenenfalls anpassen müssen, um rechtskonform zu handeln. Gleichzeitig stärkt die Entscheidung den Schutz vor unnötigen Datenerhebungen und potenzieller Diskriminierung.

[18] https://kurzlinks.de/f15s

Datenschutz-Seminar 2025

Die Entwicklung des nationalen und internationalen Datenschutzes geht weiter, auch 2025 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.

7. April 2025, 9:15 – 17:00 Uhr:

„Rechtsentwicklung und Best Practices“

Referenten: Prof. KommR Hans-Jürgen Pollirer, Mag. Judith Leschanz, Menas Saweha, Rona Paca

Gastreferent: Vertreter der Österreichischen Datenschutzbehörde

8. April 2025, 9:15 – 17:00 Uhr:

„Updates zur praktischen Anwendbarkeit & Use-Cases“

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

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

Der Datenschutzverein Privacy Ring[19] lädt am **13. März 2025** zur inzwischen 13. Fachtagung in Rotkreuz, Schweiz ein. Diesmal steht das Thema **Datenschutz @AI – Technologisches Verständnis und datenschutzrechtliche Herausforderungen** im Fokus. Die Veranstaltung kann auch online mitverfolgt werden.

Im Anschluss werden mit verschiedenen Expertinnen und Experten aus der Wirtschaft und dem öffentlichen Bereich eine Podiumsdiskussion sowie ein Get-together abgehalten.

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