asteyo

WHITE PAPER · EU-DIGITALSOUVERÄNITÄT BY DESIGN

EU-Digitalsouveränität by Design

Warum regulierte Mittelstandsunternehmen überdenken, wer ihre Software entwickelt und betreibt.

Dr. Thomas Wolenski, CSO · Alexandru Bereczki, CEO

Juni 2026 · v0.4

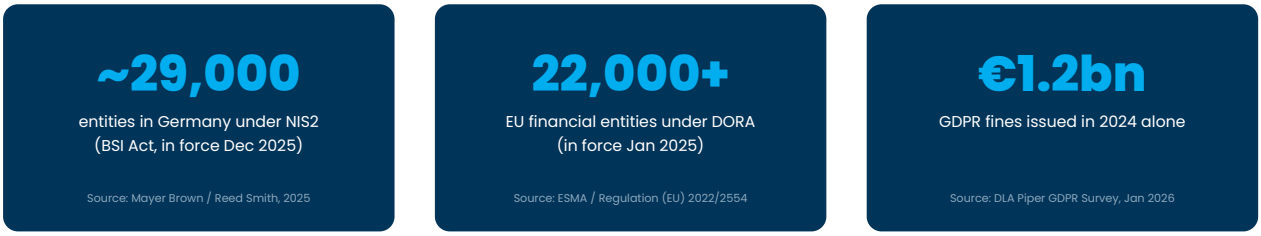
Asteyo SRL, Cluj-Napoca · office@asteyo.com · asteyo.com

EXECUTIVE SUMMARY

Eine Governance-Frage, keine reine Kostenfrage

Das deutsche NIS2-Umsetzungsgesetz (in Kraft seit 6. Dezember 2025) hat die Zahl der regulierten Organisationen von rund 4.500 auf ca. 29.000 ausgeweitet. Zusammen mit der DSGVO, DORA und dem EU Data Act machen diese Regelwerke eine Frage zum Thema für das Board: Wer entwickelt und betreibt Ihre Software – und unter welcher Rechtsordnung?

Dieses Papier richtet sich an das ambitionierte Mittelstandsunternehmen — typischerweise 200 bis 1.000 Mitarbeitende —, das nun unter NIS2 als „wichtige“ oder „wesentliche“ Einrichtung eingestuft ist oder als kleinere Finanzinstitution in den DORA-Anwendungsbereich fällt. Es stellt die regulatorische Lage dar, quantifiziert die versteckten Compliance-Kosten des falschen Sourcing-Modells und unterscheidet präzise zwischen *wo Daten gehostet werden* (Ihrer Cloud-Entscheidung) und *wer Ihre Systeme entwickelt und betreibt* (Ihrer Delivery-Partner-Entscheidung). Asteyo adressiert das Zweite.



Von links nach rechts: NIS2 Deutschland (BSI-Gesetz, Dez. 2025); DORA (ESMA, Jan. 2025); DSGVO-Bußgelder 2024 (DLA Piper, Jan. 2026).

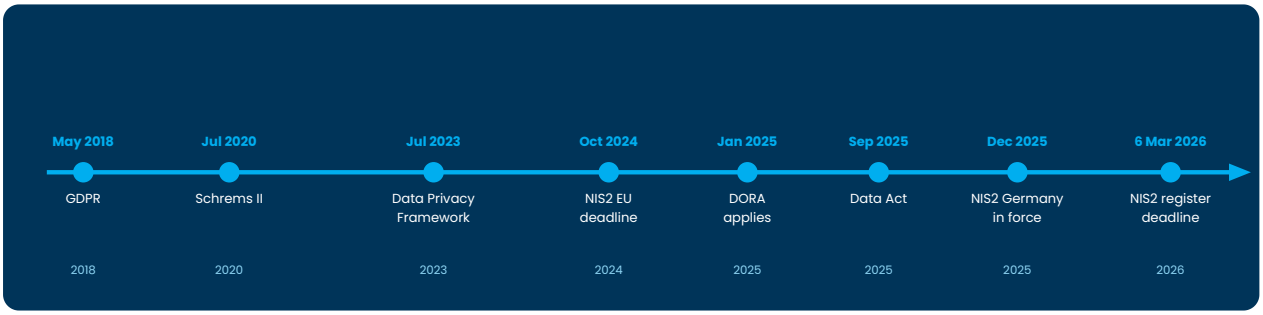
Drei Thesen dieses Papiers

- Die regulatorische Welle ist real, und das Fenster für weitere Verzögerungen hat sich geschlossen.
- Der Compliance-Mehraufwand durch Nicht-EU-Delivery-Modelle ist erheblich und steckt weitgehend im Tagessatz versteckt.
- EU-souveränes Nearshore ist eine Entscheidung über Menschen und Jurisdiktion, keine Hosting-Entscheidung – und Asteyo ist in genau diesem Bereich präzise.

Die Regulierungswelle, 2018–2026

Vier ineinandergreifende Regelwerke definieren heute, was „compliant IT-Sourcing" für ein reguliertes Mittelstandsunternehmen in der DACH-Region bedeutet.

- **DSGVO (2018).** Die Basis, die nicht verschwunden ist. Die kumulierten Bußgelder übersteigen mittlerweile 7 Milliarden €; allein 2024 verhängten Behörden rund **1,2 Milliarden €**,[2] darunter 310 Mio. € (LinkedIn), 251 Mio. € (Meta) und 290 Mio. € (Uber für die Übermittlung von Fahrerdaten in die USA).[3]
- **NIS2 – Deutschland (Dezember 2025).** Die Zahl der national überwachten Einrichtungen stieg von ca. 4.500 auf ca. 29.000,[1] darunter Fertigung, Energie, Gesundheit, Logistik und digitale Infrastruktur. Lieferkettensicherheit und Registrierung (Frist: 6. März 2026[7]) sind explizite Pflichten. Die Geschäftsleitung trägt nun direkte persönliche Verantwortung für Cybersicherheit.
- **DORA (Januar 2025).** Betrifft über 22.000 EU-Finanzinstitute.[9] Kapitel V verändert jede IT-Beschaffung: Register of Information, Prüfungs- und Ausstiegsrechte (Artikel 30), Transparenz bei Sub-Prozessoren und Bewertung des Konzentrationsrisikos. Im November 2025 veröffentlichten die ESAs die erste Liste von 19 kritischen IKT-Drittanbieter-Dienstleistern (CTPPs), darunter AWS, Microsoft, Google Cloud, Oracle, SAP und Deutsche Telekom.[11]
- **EU Data Act (September 2025).** Räumt Kunden das gesetzliche Recht auf Anbieterwechsel ein: vertragliche, technische und kommerzielle Hindernisse müssen beseitigt werden; Wechselgebühren werden bis Januar 2027 abgeschafft.[12]



Regulatorische Meilensteine 2018–2026. Quellen: EUR-Lex, BSI, ESMA, Europäische Kommission.

Einmalige Implementierungskosten (Schätzung): Die Bundesregierung schätzt rund €2,2 Milliarden an einmaligen NIS2-Umsetzungskosten für die Gesamtwirtschaft.[8] Cybersicherheit ist nun eine explizite Pflicht der Unternehmensleitung – nicht nur der IT-Abteilung.

02 · DIE US-TRANSFERFRAGE

Eine rechtmäßige, aber fragile Brücke

Das EU-US-Datenschutzrahmenabkommen (DPF, Juli 2023) ist derzeit die operative Rechtsgrundlage für Übermittlungen an DPF-zertifizierte US-Unternehmen. Es überstand seine erste Anfechtung vor Gericht im September 2025 – doch die Brücke steht unter Druck.

- **Das Berufungsverfahren läuft.** Latombe hat am 31. Oktober 2025 Rechtssache C-703/25 P beim EuGH eingereicht; ein Verhandlungstermin wurde noch nicht festgesetzt.[4]
- **Die politischen Grundlagen haben sich geschwächt.** Im Januar 2025 wurden drei von fünf Mitgliedern des PCLOB – dem Gremium, das die DPF-Schutzmaßnahmen trägt – abgesetzt.[5]
- **FISA §702 und der CLOUD Act bleiben in Kraft.** US-Anbieter können weiterhin nach US-Recht verpflichtet werden, weltweit gespeicherte Daten offenzulegen.

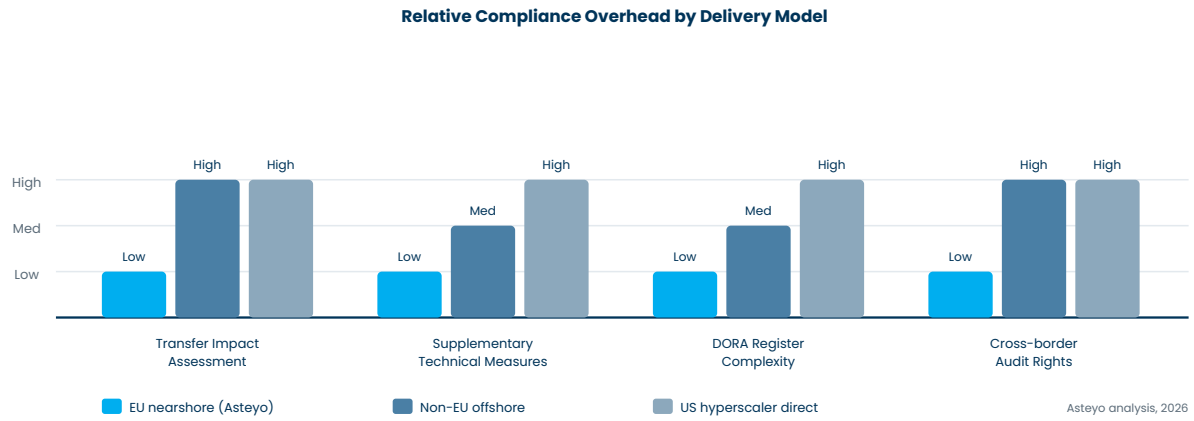
Für regulierte Käufer bleiben US-Übermittlungen rechtmäßig, stützen sich aber auf einen wiederholt angegriffenen und politisch exponierten Mechanismus. Ein in der EU ansässiger Anbieter, der nach EU-Recht operiert, EU-basiertes Personal beschäftigt und keine US-Muttergesellschaft hat, beseitigt diese Unsicherheit – er managt sie nicht.

EU-basierter Betrieb: Asteyos Service-Delivery verbleibt innerhalb des EU-Rechtsrahmens.

Was das falsche Sourcing-Modell wirklich kostet

Ein Offshore-Engagement auf einem US-Hyperscaler mit einer Sub-Prozessor-Kette über drei Jurisdiktionen kann erhebliche Compliance-Investitionen erfordern, bevor es für kritische NIS2- oder DORA-Aufgaben geeignet ist. Der ausgewiesene Tagessatz verschleiert diese Last.

- **Transfer Impact Assessment** – eine formale rechtliche Analyse, bevor personenbezogene Daten die EU verlassen; in komplexen Ketten fallen TIAs auf Auftragnehmer, Cloud-Anbieter und jeden Sub-Prozessor an.
- **Ergänzende technische Maßnahmen** – fällt ein TIA ungünstig aus, entstehen durch Verschlüsselung oder Pseudonymisierung mit EU-kontrollierten Schlüsseln zusätzliche Kosten und operationale Reibung.
- **Grenzüberschreitende Prüfungsrechte** – die Ausübung von DORA-Artikel-30-Prüfungsrechten in einem Drittland ist logistisch und rechtlich aufwendiger und kann mit lokalen Gesetzen kollidieren, die Inspektionen einschränken.
- **DORA-Register-Komplexität** – eine Multi-Jurisdiktion-Kette erschwert das Register of Information; Aufseher prüfen Einreichungen aktiv.
- **Incident- und Konzentrationsrisiko** – ENISA Threat Landscape 2025 zählt Lieferketten-Kompromittierung zu den bedeutendsten Zukunftsrisiken.[13] Die Kosten eines Vorfalls, der bei einem Drittanbieter entsteht, können die Tagessatz-Ersparnisse vieler Jahre übersteigen.



Relativer Compliance-Aufwand nach Delivery-Modell (qualitativ; Asteyo-Analyse, 2026). Niedrigere Balken = geringere Regulierungslast.

04 · WAS „EU-SOUVERÄNES NEARSHORE“ WIRKLICH BEDEUTET

Eine Jurisdiktionsentscheidung, keine Hosting-Entscheidung

„Digitale Souveränität“ vermischt zwei unterschiedliche Fragen. Wer sie verwechselt, trifft schlechte Beschaffungsentscheidungen.

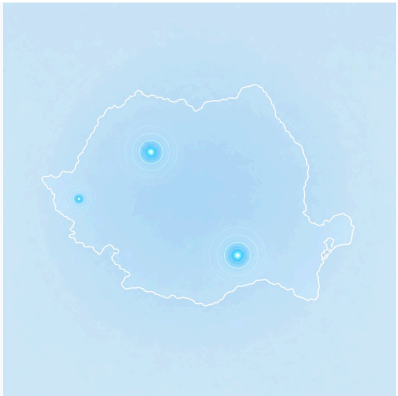
Wo werden Daten gehostet?
Das ist Ihre Cloud-Entscheidung. AWS European Sovereign Cloud, Microsoft EU Data Boundary und Google Sovereign Controls sind ernsthafte Antworten auf diese Frage, und ein reifer Käufer sollte sie nach ihren Vorzügen bewerten.

Wer entwickelt, betreibt und kann auf das System zugreifen?
Das ist Ihre Delivery-Partner-Entscheidung: Welche Menschen schreiben den Code, halten die Zugangsdaten, sehen die Daten und reagieren auf Vorfälle – und welcher Rechtsordnung unterstehen sie.

Asteyo adressiert die zweite Frage, und ist dabei präzise. Wir beanspruchen nicht, Ihre Cloud-Souveränität zu lösen. Was wir bieten, ist Delivery unter EU-Jurisdiktion: die Ingenieure, ihre Zugänge, ihr Arbeitgeber und ihre Sub-Prozessoren befinden sich sämtlich innerhalb des EU-Rechtsrahmens. Für die meisten regulierten Mittelstandskäufer ist die Personen-und-Zugriff-Schicht genau dort, wo Offshore-Modelle die schwierigsten Compliance-Lücken hinterlassen.

Verifizierbare Merkmale EU-souveräner Delivery

- **EU-Jurisdiktion über den Anbieter** – in einem EU-Mitgliedstaat gegründet, nicht durch Drittstaaten-Behörden zur Auskunft verpflichtbar.
- **EU-basierte Verarbeitung und Zugriffe** – alle Zugriffe auf Kundendaten durch das Personal des Anbieters erfolgen aus EU-Territorium.
- **Transparente Unterauftragsvergabe** – die gesamte Sub-Prozessor-Kette ist EU-ansässig oder durch einen gültigen, dokumentierten Übermittlungsmechanismus abgedeckt.
- **Prüfungs- und Ausstiegsrechte als Standard** – als Baseline-Konditionen angeboten, nicht als Premium-Zugeständnisse.
- **Unabhängige Sicherheitszertifizierung** – ISO/IEC 27001 oder gleichwertig.



Rumänien – EU-Mitgliedstaat seit 2007, gleiche Zeitzone wie DACH-Kunden (max. 1 Stunde Versatz).

05 · WIE ASTEYO PASST

Compliance by Design, ehrlich über den Geltungsbereich

Asteyo SRL ist in Cluj-Napoca, Rumänien gegründet – einem EU-Mitgliedstaat seit 1. Januar 2007. Das ist die Architektur, kein nachträglicher Anstrich auf ein bestehendes Modell.

Rumäniens IT-Sektor beschäftigt schätzungsweise 200.000 bis 250.000 Software-Fachleute. Cluj-Napoca beherbergt rund 20.000 bis 23.000 IT-Fachkräfte in ca. 450 Unternehmen, verankert durch zwei der größten technischen Universitäten in Mittel- und Osteuropa.[15] Die Ingenieure arbeiten in derselben Zeitzone wie DACH-Kunden (maximal eine Stunde Versatz), was Echtzeit-Zusammenarbeit ohne Nacht-Handoff ermöglicht.

- **DSGVO-nativ by Design.** Asteyo hat seit Gründung unter der DSGVO operiert. Es gibt keine Compliance-Altlasten aus der Zeit vor 2018 und keine Legacy-Datenweitergabevereinbarungen.
- **ISO 27001 und ISO 9001.** Asteyo hält die Zertifizierungen ISO/IEC 27001:2022 und ISO 9001:2015, ausgestellt von SYSTEMA (IAS/IAF-akkreditiert), gültig Dezember 2025 bis Dezember 2028 (SoA datiert 10. August 2025). Zertifizierter Geltungsbereich: kundenorientierte Software-Entwicklung.
- **DORA- und NIS2-Vertragsunterstützung.** In Zusammenarbeit mit unseren EU-Rechtsberatern strukturieren wir Engagements entsprechend der einschlägigen Anforderungen: Prüfungs- und Inspektionsrechte; Austritts- und Kündigungsrechte nach DORA Artikel 30; Unterstützung beim Register of Information; im SLA verankerte Kooperation bei der Incident-Meldepflicht.
- **Anbieterwiderstandsfähigkeit, direkt adressiert.** Jedes Engagement ist so strukturiert, dass der Kunde die Arbeit zurücknehmen oder verlagern kann, mit Wissenstransfer als vertraglicher Leistung. Der Build-Operate-Transfer-Weg (Stage 3) ist die stärkste mögliche Antwort auf Lock-in: die Kompetenz kann zu Ihrer werden.

200k+
IT-Fachkräfte in Rumänien
4.-größte Tech-Workforce in der EU[14]

~22k
IT-Fachkräfte in Cluj
Ca. 450 Unternehmen, 2 große Technische Universitäten[15]

Max 1h
Zeitzonenversatz zur DACH-Region
Voller Arbeitstag-Overlap, kein Nacht-Handoff

ISO 27001 SYSTEMA · ISO 9001 SYSTEMA · EU · GDPR

SYSTEMA (IAS/IAF-akkreditiert) · Gültig Dez. 2025–Dez. 2028 · Geltungsbereich: kundenorientierte Software-Entwicklung

06 · ENGAGEMENT-MODELL

Ein Weg für risikobewusste Käufer

Der typische CIO/CISO-Einwand gegenüber jedem neuen Anbieter: Wie weiß ich, dass das funktioniert, bevor ich mich für etwas Kritisches darauf verlasse? Asteyos dreistufiges Modell beantwortet das konstruktiv, nicht durch Versprechungen.

STAGE 1

Spezialist-Engagement

Ein einzelner Spezialist oder kleines Pod-Team tritt einem bestehenden Team für einen definierten Scope bei – ein natürlicher Compliance-Perimeter, leicht zu dokumentieren im DORA-Register oder einer NIS2-Lieferanten-Bewertung. EU-Jurisdiktion vom ersten Tag. Ausstieg jederzeit möglich.

STAGE 2

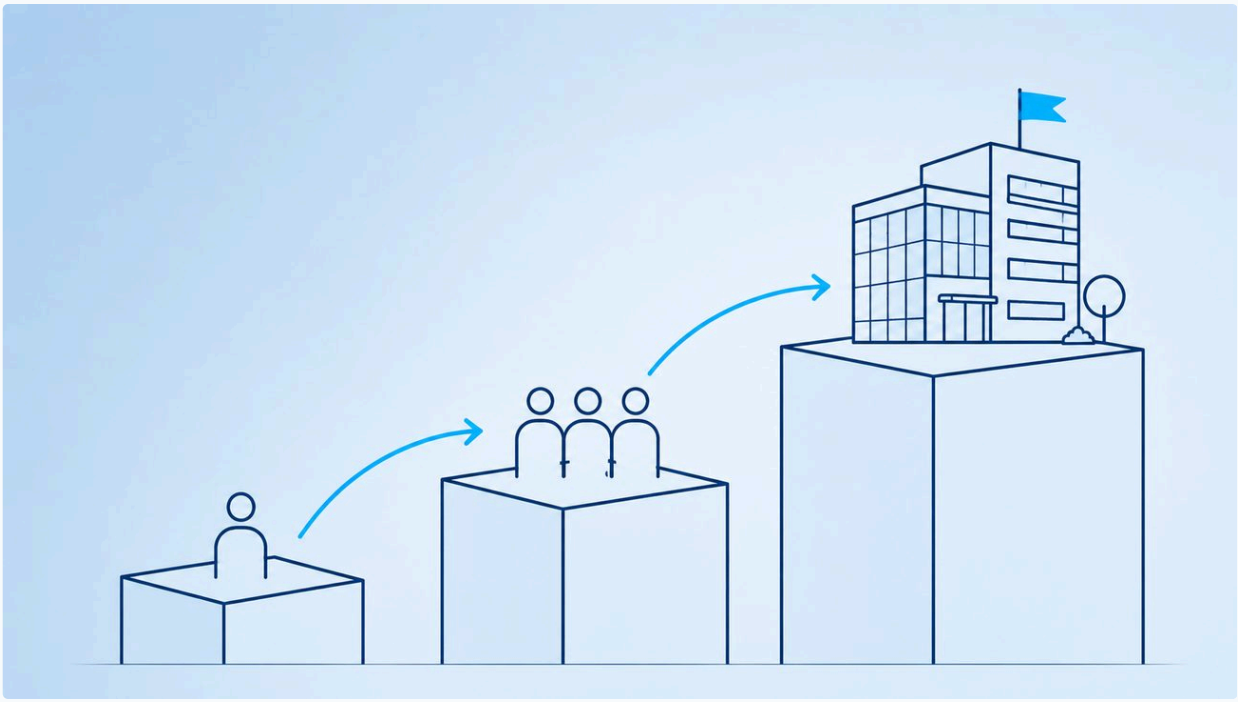
Dediziertes Team

Vier bis zwölf Ingenieure, die als benannte, stabile Einheit unter den Sicherheits- und Qualitätsrahmen des Kunden agieren. Eine stabile, dokumentierbare Anbieterbeziehung, wie sie das DORA-Register vorsieht.

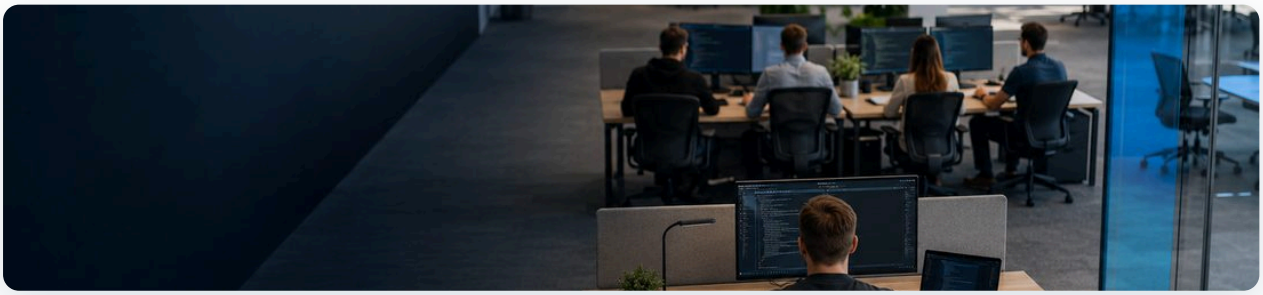
STAGE 3

Build-Operate-Transfer (BOT)

Asteyo baut und betreibt eine dedizierte Nearshore-Kapazität, überträgt dann schrittweise operative Kontrolle und Eigentum an den Kunden. Ein vollständig eigenes, EU-ansässiges Delivery-Center.



Vom Spezialist-Engagement bis zum kundeneigenen Delivery-Center. Jede Stufe ist prüfbar und reversibel.



Asteyo-Delivery-Teams wachsen mit dem Kunden – vom Spezialist-Pod zur skalierbaren, stabilen Einheit.

asteyo

"

Für ein reguliertes Mittelstandsunternehmen sind die Compliance-Frage und die Delivery-Frage heute dieselbe Frage: Wer hat Zugriff auf Ihre Systeme, nach welchem Recht, und wie weisen Sie das einem Aufseher nach?

ASTEYO EU-DIGITALSOUVERÄNITÄT THESE, 2026

07 · NÄCHSTER SCHRITT

Beginnen Sie mit einem Gespräch

Das Fenster für weitere Aufschübe hat sich geschlossen. Deutschlands NIS2-Pflichten sind in Kraft; die Registrierungsfrist lief am 6. März 2026 ab. DOARs Drittanbieter-Anforderungen sind aktiv. Die Wechselrechte des Data Act gelten.

Ein Lieferketten-Lücken-Audit deckt typischerweise einen oder mehrere der folgenden Punkte auf:

- Einen außerhalb der EU ansässigen Anbieter, der eine kritische oder wichtige Funktion unterstützt.
- Eine US-Hyperscaler-Abhängigkeit ohne EU-souveränen Fallback-Plan.
- Eine Sub-Prozessor-Kette mit Drittland-Sub-Prozessoren, die nicht durch ein aktuelles TIA abgedeckt sind.
- Vertragsbedingungen ohne Prüfungs- und Ausstiegsrechte, die DORA Artikel 30 oder einer NIS2-Lieferanten-Bewertung genügen.

Jetzt sprechen

Asteyos Engagement beginnt mit einem Gespräch. Wir unterstützen Lücken-Analysen für spezifische Arbeitsstränge, erläutern, wie unsere Verträge auf Ihr DORA-Register oder Ihre NIS2-Lieferantenanforderungen einzahlen, und skizzieren, wie ein Stage-1-Spezialist-Engagement für ein laufendes Projekt aussieht.

office@asteyo.com · asteyo.com

ISO 27001 SYSTEMA · ISO 9001 SYSTEMA · EU · GDPR

ISO/IEC 27001:2022 & ISO 9001:2015 zertifiziert · SYSTEMA (IAS/IAF-akkreditiert) · Gültig Dez. 2025–Dez. 2028

Asteyo — Zuverlässigkeit · Menschen · Partnerschaften. Wir liefern.

QUELLEN

Quellen & Anmerkungen

Die Zahlen sind primären oder bestmöglich verfügbaren öffentlichen Quellen entnommen. Regulierungsreichweiten basieren auf Behörden- und Kanzlei-Analysen und stellen Schätzungen dar, die je nach Quelle und Methodik variieren können.

1 **Mayer Brown**, "Cyber Rules for Essential and Important Entities Take Effect in Germany (NIS2 Implementing Law)," Dec 2025. mayerbrown.com – Reed Smith, "Finally: Germany enacts its NIS2 law," 2025. reedsmith.com

2 **DLA Piper**, "GDPR Fines and Data Breach Survey: January 2026" (cumulative fines >€7bn; ~€1.2bn in 2024). CMS GDPR Enforcement Tracker. enforcementtracker.com

3 **Irish DPC**, decisions on LinkedIn (€310m) and Meta (€251m), 2024. Dutch Autoriteit Persoonsgegevens, Uber fine (€290m), 2024. autoriteitpersoonsgegevens.nl

4 **IAPP**, "European General Court dismisses Latombe challenge, upholds EU-US DPF," Sep 2025. iapp.org – Appeal: Case C-703/25 P (CJEU), filed 31 Oct 2025.

5 **WilmerHale**, "European Court of Justice to Review Challenge to EU-U.S. Data Privacy Framework," Dec 2025 (incl. PCLOB membership removals, Jan 2025). wilmerhale.com

6 **European Commission**, infringement proceedings / reasoned opinion on NIS2 non-transposition, May 2025. Morrison Foerster, "Flipping the NIS2 Switch," Dec 2025. mofo.com

7 **Privacy World (Squire Patton Boggs)**, "Germany Implements NIS2: Registration portal will open on January 6, 2026," Dec 2025 (registration due by 6 March 2026). privacyworld.blog

8 **Greenberg Traurig**, "NIS2 in Germany: The New BSI Act Makes Cybersecurity a Board-Level Issue," Dec 2025. gtlaw.com

9 **ESMA**, "Digital Operational Resilience Act (DORA)." esma.europa.eu – Regulation (EU) 2022/2554 (EUR-Lex). Audit/contract clauses: DORA Article 30.

10 **National competent authorities** collected first Registers of Information from financial entities in April 2025 (deadlines per member state).

11 **European Supervisory Authorities (EBA/EIOPA/ESMA)**, "ESAs designate critical ICT third-party providers under DORA," 18 Nov 2025 (19 CTPPs: AWS, Microsoft, Google Cloud, Oracle, SAP, Deutsche Telekom etc.). eiopa.europa.eu

12 **European Commission**, "Data Act," Regulation (EU) 2023/2854, applicable from 12 Sep 2025; switching fees phased out by 12 Jan 2027. digital-strategy.ec.europa.eu

13 **ENISA**, "ENISA Threat Landscape 2025," October 2025. enisa.europa.eu

14 **Index.dev**, "Software Development in Romania: Market Analysis & Hiring Guide for 2025." Romania Insider, "Over one in five Romanian university graduates are engineers, the highest share in EU." index.dev

15 **KiTalent**, "Cluj-Napoca's Tech Sector Is Booming," 2025. kitalent.com