HENRY OSWALD
LEXREG RESEARCH

Q2/2026: Warum AI Act, NIS2 und CRA für österreichische Kanzleien jetzt zum regulatorischen Wendepunkt werden

Q2/2026 ist für österreichische Kanzleien kein bloßer Beobachtungszeitraum mehr, sondern die Phase, in der drei große EU-Regime praktisch in die Umsetzungs- und Vorbereitungslogik der Mandanten hineinwirken: der AI Act, NIS2 und der Cyber Resilience Act. Der gemeinsame Nenner ist, dass 2026 nicht nur weitere Rechtsakte näher rücken, sondern konkrete organisatorische, technische und dokumentationsbezogene Pflichten in den Fokus rücken, die sich nicht mehr sinnvoll erst kurz vor Anwendbarkeit aufbauen lassen.

KANZLEIPERSPEKTIVE

Mandanten werden 2026 weniger nach abstrakter Einordnung fragen, sondern nach belastbarer Priorisierung, Governance, Auditfähigkeit und dokumentierbarer Umsetzung.

Genau deshalb eignet sich dieses Thema als Leit-Arbeitsprobe für ein Digital-Law Update, ein projektbezogenes Deep-Dive-Memo und nachgelagerte Dokumentenentwürfe.

AI Act

TEIL 1

Der AI Act ist das zentrale horizontale EU-Regelwerk für Künstliche Intelligenz und wird stufenweise wirksam. Für die Beratungspraxis in Österreich ist 2026 der eigentliche Wendepunkt, weil viele Unternehmen erst jetzt erkennen, dass der AI Act nicht nur Entwickler von KI-Modellen trifft, sondern ganze Liefer- und Einsatzketten. Betroffen sein können Anbieter, Einführer, Händler, Betreiber bzw. Deployers, Bevollmächtigte sowie in bestimmten Konstellationen auch Produkthersteller mit KI-Komponenten.

Wer betroffen ist

Die Erstprüfung sollte nicht mit der Frage beginnen, ob ein Mandant „AI-Unternehmen“ ist, sondern ob er KI entwickelt, integriert, einkauft, betreibt, vertreibt oder Ergebnisse im Rechts- oder Geschäftsverkehr verwendet. Typische österreichische Mandanten mit Berührungspunkten sind Softwarehäuser, SaaS-Anbieter, HR-Tech-Unternehmen, Industrie- und IoT-Anbieter, FinTechs, Health-Tech-Unternehmen, Händler digitaler Produkte und klassische Mittelständler mit KI-gestützten Personal-, Risiko-, Support- oder Compliance-Prozessen.

Fristen und typische Lücken

Für Mandate ist die Fristenkommunikation zentral: Verbote und AI-Literacy-Pflichten gelten bereits seit Februar 2025, GPAI-bezogene Pflichten seit August 2025, und ab 2. August 2026 wird der Großteil des Regimes anwendbar. Typische Lücken liegen weniger bei abstrakten Rechtskenntnissen als bei der Zuordnung von Rollen, Systemen, Transparenzpflichten, Governance, Dokumentation und Schulungskonzepten.

NIS2

TEIL 2

Bei NIS2 verschiebt sich die Diskussion 2026 in Österreich vom politischen Umsetzungsdefizit zur operativen Audit- und Nachweisfähigkeit. Genau hier wird Q2/2026 für Kanzleien geschäftlich interessant: Mandanten wollen nicht mehr nur wissen, ob NIS2 irgendwann kommt, sondern ob sie voraussichtlich als wesentliche oder wichtige Einrichtung einzustufen sind, welche Nachweise vorbereitet werden sollten und wie tief interne Kontrollen dokumentiert sein müssen.

Wer als wesentlich oder wichtig fällt

Für die österreichische Beratungspraxis ist entscheidend, dass die Einordnung nicht nur sektoral, sondern auch größen- und bedeutungsbezogen erfolgt. Aus Kanzleisicht empfiehlt sich ein zweistufiger Prüfpfad: zuerst sektor- und größenbezogene Vorqualifikation, danach Sondertatbestände, Gruppenstrukturen, Outsourcing und Kritikalität im Liefer- oder Versorgungsgefüge.

Was im Audit geprüft wird

Für die Auditvorbereitung müssen nicht nur technische Schutzmaßnahmen, sondern auch operative und organisatorische Nachweise, Governance, Zuständigkeiten, dokumentierte Prozesse, Vorfallswege und belastbare Nachweisführung vorhanden sein. Daraus entstehen unmittelbar verkaufbare Produkte: NIS2-Scoping-Memos, Audit-Readiness-Checklisten, Board-Briefings und Policy-Templates.

CRA

TEIL 3

Der Cyber Resilience Act ist für viele österreichische Mandanten noch unterschätzt, obwohl seine Berichtspflichten schon vor der vollen allgemeinen Anwendbarkeit scharf werden. Hersteller müssen ab 11. September 2026 aktiv ausgenutzte Schwachstellen und schwere Sicherheitsvorfälle melden. Die Frühwarnung hat innerhalb von 24 Stunden zu erfolgen; innerhalb von 72 Stunden ist eine vollständige Meldung nachzureichen.

SBOM und Security-by-Design

Der CRA treibt das Thema Software Bill of Materials von einer technischen Best Practice in den Bereich regulatorischer Erwartung und technischer Dokumentation. Gleichzeitig ist der CRA kein reines Meldegesetz, sondern ein Produkt-Compliance-Regime mit Security-by-Design-, Schwachstellenmanagement- und Updatepflichten. Für Kanzleien entsteht daraus eine starke Brücke zwischen Rechtsberatung, Produktentwicklung und Lieferkettenmanagement.

Mandantenfragen der nächsten 6 Monate

PRAXISFOKUS

AI Act
Fallen wir darunter, obwohl wir nur fremde Tools einsetzen? Welche Rollen, Inventare und Transparenzhinweise müssen wir sofort klären?

NIS2
Sind wir voraussichtlich wesentlich oder wichtig? Welche Nachweise und internen Kontrollen müssen wir schon jetzt auditfähig dokumentieren?

CRA
Sind unsere Softwareprodukte CRA-relevant? Wie bauen wir belastbare 24-Stunden-Melde- und Eskalationsprozesse auf?

Dokumentationsbedarf
Welche Policies, Checklisten, Rollenmatrizen, Supplier-Fragebögen und Vertragsklauseln müssen kurzfristig vorbereitet werden?

Quellenbasis

- European Commission, AI Act | Shaping Europe’s digital future.
- AI Act Service Desk, Timeline for the Implementation of the EU AI Act.
- European Commission, NIS2 Directive implementation in Austria.
- European Commission, Cyber Resilience Act – Reporting obligations.
- WKO, NISG 2026 – neue Pflichten zur Cybersicherheit für Unternehmen.
- Österreichische Praxis- und Advisory-Quellen zur AI-Act-, NIS2- und CRA-Umsetzung.

LexReg Research · Henry Oswald
Arbeitsprobe für Kanzleien mit Fokus auf IT, Datenschutz und Digitalregulatorik