Leitfäden zum Anbieterrisiko für die Europäische Union und Mitgliedstaaten

Wie Cyber Crucible EU-weite Regelwerke (GDPR, DORA, NIS2, den AI Act) und mitgliedstaatliche Besonderheiten (Deutschland, Frankreich, Irland, Niederlande, Spanien, Italien, Polen, Schweden) aus Sicht der Lieferantenauswahl unterstützt. Es wird klar dargelegt, welche Nachweise Cyber Crucible besitzt und welche nicht, ohne im Namen des Kunden Compliance-Zusagen zu machen.

Welche EU-Vorschriften wirken sich neben der DSGVO auf die Auswahl eines Sicherheitsanbieters aus?

Kurze Antwort: Neben der DSGVO prägen zunehmend drei EU-Regelwerke die Auswahl von Anbietern: DORA (operative Resilienz für Finanzunternehmen und deren IKT-Dienstleister), NIS2 (Cybersicherheitspflichten für wesentliche und wichtige Einrichtungen, einschließlich der Sicherheit der Lieferkette) und das EU-KI-Gesetz (risikoabgestufte Vorschriften für KI-Systeme). Jedes dieser Regelwerke verlagert Pflichten in Richtung der Anbieter. Das Design von Cyber Crucible — keine Erfassung von Kundeninhalten, lokale Verarbeitung, Option zum On-Premises-Betrieb — unterstützt die Pflichten des Kunden im Rahmen all dieser Regelwerke, ohne dass Cyber Crucible eine Compliance im Namen des Kunden beansprucht.

Die Landschaft im Überblick

- **DSGVO** — die Grundlage für die Verarbeitung personenbezogener Daten in der gesamten EU. Siehe die Country Compliance Guides für die Seite zur DSGVO.
- **DORA** — gilt ab dem 17. Januar 2025 für Finanzunternehmen und, wichtig, für deren IKT-Drittdienstleister.
- **NIS2** — die Mitgliedstaaten sollten die Richtlinie bis Oktober 2024 in nationales Recht umsetzen; Stand 2026 haben dies die meisten getan, während mehrere die nationale Gesetzgebung noch abschließen.
- **EU-KI-Gesetz** — risikoabgestufte Pflichten, die bis 2026–2027 schrittweise in Kraft treten.

Wie Cyber Crucible dazu passt

Das wiederkehrende Thema ist das Risiko der Lieferkette und von Drittanbietern. Da Cyber Crucible keine Kundeninhalte, Zugangsdaten oder Schlüssel erfasst und vollständig innerhalb der Grenzen des Kunden betrieben werden kann, verringert es die Angriffsfläche, die diese Regelwerke eindämmen sollen. Die Seiten in diesem Buch behandeln jedes Regelwerk sowie die größeren Mitgliedstaaten. Dokumentation ist erhältlich unter **dpo@cybercrucible.com**.

Wie unterstützt Cyber Crucible EU-Finanzunternehmen im Rahmen von DORA?

Kurze Antwort: Cyber Crucible ist im Sinne von DORA ein IKT-Drittdienstleister und unterstützt die DORA-Verpflichtungen eines Finanzunternehmens — vertragliche Kontrollen, Vorfallsinformationen und Resilienztests —, während es das IKT-Drittparteirisiko reduziert, da es niemals die Daten des Unternehmens erfasst. DORA gilt ab dem 17. Januar 2025. Cyber Crucible beansprucht nicht, im Namen eines Kunden „DORA-konform" zu sein; die Konformität liegt beim Finanzunternehmen, und Cyber Crucible liefert die Unterstützung und Nachweise, die dessen Programm benötigt.

Wie es das DORA-Programm des Unternehmens unterstützt

- **Reduzierung des IKT-Risikos.** Es werden keine Kundeninhalte, Anmeldedaten oder Schlüssel erfasst, und der Schutz läuft lokal — dies verkleinert die Angriffsfläche von Drittparteien, auf die DORA abzielt.
- **Vertragliche Kontrollen.** Cyber Crucible kann die vertraglichen Bestimmungen berücksichtigen, die DORA für IKT-Drittparteivereinbarungen erwartet (Sicherheit, Zusammenarbeit bei Vorfällen, Prüf- und Informationsrechte, Transparenz bei Unterauftragsvergabe).
- **Zusammenarbeit bei Vorfällen.** Ein dokumentierter Prozess zur Reaktion auf Sicherheitsverletzungen liefert zeitnahe, beweiskräftige Informationen, und ein verbindlicher Benachrichtigungszeitrahmen ist vertraglich verfügbar, um die Meldepflichten des Unternehmens bei Vorfällen zu unterstützen.
- **Resilienz.** Der Endpunktschutz bleibt auch bei einem Ausfall des Management-Backends bestehen, was die Ziele der operationellen Resilienz unterstützt.

Die ehrliche Grenze

DORA erlaubt es den Europäischen Aufsichtsbehörden zudem, **kritische** IKT-Drittdienstleister (CTPPs) für die direkte EU-Aufsicht zu benennen. Cyber Crucible ist nicht als CTPP benannt und stellt sich auch nicht als solcher dar. Es unterstützt die Verpflichtungen des Finanzunternehmens; es übernimmt sie nicht.

Wie unterstützt Cyber Crucible die NIS2-Pflichten für wesentliche und wichtige Einrichtungen?

Kurzantwort: Für eine Organisation, die im Rahmen von NIS2 als wesentliche oder wichtige Einrichtung eingestuft ist, unterstützt Cyber Crucible die erforderlichen Risikomanagementmaßnahmen – Endpunktschutz, Zugriffskontrolle, Verschlüsselung und Vorfallsbehandlung – und unterstützt die Erwartungen der Richtlinie an die Sicherheit der Lieferkette, da es keine Kundendaten erfasst und innerhalb der Grenzen der Einrichtung betrieben werden kann. Cyber Crucible unterstützt diese Pflichten; es zertifiziert sie nicht und übernimmt sie nicht.

Wie es NIS2-Maßnahmen unterstützt

- **Maßnahmen zum Cybersicherheitsrisikomanagement.** Autonome Endpunktprävention, MFA-gestützter Zugriff und Verschlüsselung entsprechen mehreren der grundlegenden Maßnahmen der Richtlinie.
- **Sicherheit der Lieferkette.** Als Anbieter, der keine Kundeninhalte erfasst und eine On-Premises-Bereitstellung anbietet, reduziert Cyber Crucible das Lieferkettenrisiko, das NIS2 von Einrichtungen zu managen verlangt, anstatt es zu erhöhen.
- **Unterstützung bei Vorfallsbehandlung und -meldung.** Ein dokumentierter Prozess zur Reaktion auf Sicherheitsverletzungen hilft der Einrichtung, die Fristen von NIS2 für Frühwarnungen und Benachrichtigungen einzuhalten.

Die ehrliche Grenze

Die NIS2-Pflichten liegen bei der wesentlichen oder wichtigen Einrichtung, nicht bei einem einzelnen Sicherheitstool. Die Umsetzung durch die Mitgliedstaaten fiel unterschiedlich aus: Bis 2026 hatten die meisten Staaten die Richtlinie in nationales Recht umgesetzt, während mehrere – darunter Frankreich, Irland, die Niederlande und Spanien – dies noch abschlossen. Cyber Crucible verfügt über keine NIS2-„Zertifizierung“; es stellt unterstützende Kontrollnachweise unter NDA bereit.

Wie verhält sich Cyber Crucible zum EU AI Act?

Kurze Antwort: Cyber Crucible setzt KI ausschließlich während der Entwicklung ein (im Rahmen der Genetic-AI-Forschungsarbeit) und verwendet zur Laufzeit feste, deterministische Heuristiken – es gibt kein live agierendes KI-Modell, das auf dem Endpunkt des Kunden Entscheidungen trifft. Cyber Crucible bringt daher kein hochriskantes oder allzweckfähiges KI-System in die Umgebung des Kunden ein. Der Kunde bleibt selbst dafür verantwortlich, seine eigenen Pflichten im Rahmen des EU AI Act zu bewerten, dessen Anforderungen bis 2026–2027 schrittweise in Kraft treten.

Warum die Architektur hier von Bedeutung ist

- **Kein zur Laufzeit ausgeführtes KI-System beim Kunden.** Der Endpunkt führt deterministische Kernel-Heuristiken aus, kein live agierendes Modell – es gibt also kein auf dem Gerät befindliches KI-System, das der Kunde im Sinne des Gesetzes klassifizieren und regeln müsste.
- **Ausschließlich zur Entwicklungszeit.** Die KI-Arbeit findet in der internen Entwicklungsumgebung von Cyber Crucible anhand interner Forschungsdatensätze statt; es werden keine Kundeninhalte, Zugangsdaten oder Schlüssel zum Trainieren, Speisen oder Feinabstimmen eines Modells verwendet.
- **Transparenz.** Da das Laufzeitverhalten deterministisch und testbar statt probabilistisch ist, lässt es sich einfach beschreiben und dokumentieren.

Die ehrliche Abgrenzung

Cyber Crucible behauptet nicht, dass das Produkt „EU-AI-Act-konform“ ist, und trifft diese Feststellung auch nicht anstelle des Kunden. Diese Seite beschreibt, wie das Produkt funktioniert, damit die eigene AI-Act-Bewertung des Kunden dies korrekt berücksichtigen kann. Dies stellt keine Rechtsberatung dar.

Wie unterstützt Cyber Crucible die Datenschutz- und Sicherheitsanforderungen in Deutschland?

Kurze Antwort: In Deutschland unterstützt Cyber Crucible die Verpflichtungen einer Organisation gemäß der GDPR und dem Bundesdatenschutzgesetz (BDSG), indem keine Kundeninhalte, Zugangsdaten oder Schlüssel erfasst werden und die Verarbeitung auf dem Endgerät erfolgt. Für Organisationen, die dem deutschen Cybersicherheitsregime unterliegen (der BSI-Gesetzesrahmen, im Zuge der Umsetzung von NIS2), unterstützt das Design mit lokaler Verarbeitung und On-Premises-Fähigkeit deren Sicherheits- und Lieferkettenverpflichtungen.

Wie die Ausrichtung erfolgt

- **GDPR + BDSG.** Datenminimierung, Verschlüsselung und Zugriffskontrolle unterstützen den deutschen Datenschutzstandard; eine Datenverarbeitungsvereinbarung ist verfügbar.
- **Datenresidenz.** Die On-Premises-Bereitstellung hält personenbezogene Daten dort, wo es erforderlich ist, in Deutschland; keine Kundeninhalte werden zur Sicherheitsverarbeitung ins Ausland übertragen.
- **Cybersicherheitsregime.** Deutschland setzt NIS2 in seinen BSI-Gesetzesrahmen um; Cyber Crucible unterstützt die Risikomanagement- und Lieferkettenmaßnahmen betroffener Einrichtungen.

Die ehrliche Grenze

Die Compliance liegt bei der Organisation und, soweit relevant, bei ihrem Datenschutzbeauftragten und der zuständigen Aufsichtsbehörde. Cyber Crucible verfügt über keine deutsche Zertifizierung und unterstützt diese Pflichten, übernimmt sie jedoch nicht. Dokumentation ist auf Anfrage erhältlich.

Wie unterstützt Cyber Crucible die Anforderungen an den Datenschutz in Frankreich?

Kurze Antwort: In Frankreich unterstützt Cyber Crucible die Verpflichtungen einer Organisation im Rahmen der GDPR und des Loi Informatique et Libertés (durchgesetzt von der CNIL), indem Daten minimiert und lokal verarbeitet werden. Da keine Kundeninhalte, Anmeldedaten oder Schlüssel erfasst werden, haben die meisten von der CNIL durchgesetzten Verpflichtungen in ihrem Verwahrungsbereich nur minimale Angriffsfläche.

Wie die Ausrichtung erfolgt

- **GDPR + nationales Recht.** Verschlüsselung, Zugriffskontrolle und Datenminimierung unterstützen die französische Grundlage; eine Vereinbarung zur Auftragsverarbeitung ist verfügbar.
- **Datenresidenz.** Der On-Premises-Einsatz hält personenbezogene Daten dort in Frankreich, wo dies erforderlich ist.
- **Cybersicherheitsregime.** Die französische Umsetzung von NIS2 befand sich Stand 2026 noch im laufenden Gesetzgebungsverfahren; Cyber Crucible unterstützt die Sicherheits- und Lieferkettenmaßnahmen betroffener Einrichtungen im Rahmen des jeweils verabschiedeten Regelwerks.

Die ehrliche Grenze

Die CNIL ist eine aktive Aufsichtsbehörde; die Compliance liegt in der Verantwortung der Organisation, und Cyber Crucible unterstützt sie, ohne eine französische Zertifizierung zu beanspruchen. Dokumentation ist auf Anfrage erhältlich.

Wie unterstützt Cyber Crucible die Anforderungen an den Datenschutz in Irland?

Kurzantwort: In Irland unterstützt Cyber Crucible die Verpflichtungen eines Unternehmens im Rahmen der GDPR und des Data Protection Act 2018 (durchgesetzt durch die Data Protection Commission), indem keine Kundeninhalte, Zugangsdaten oder Schlüssel erfasst werden und die Verarbeitung auf dem Endpunkt erfolgt. Irland ist die federführende Aufsichtsbehörde für viele multinationale Unternehmen, was die Anforderungen an die Prüfung von Anbietern erhöht; der minimale Datenfußabdruck hält das Risiko auf Anbieterseite gering.

Wie es sich einfügt

- **GDPR + DPA 2018.** Datenminimierung, Verschlüsselung und Zugriffskontrolle unterstützen die irische Grundlage; eine Auftragsverarbeitungsvereinbarung (Data Processing Agreement) ist verfügbar.
- **Datenresidenz.** Die On-Premises-Bereitstellung hält personenbezogene Daten in Irland, wo dies erforderlich ist.
- **Cybersicherheitsregime.** Die Umsetzung der NIS2 in Irland befand sich Stand 2026 noch in der Finalisierung; Cyber Crucible unterstützt die Maßnahmen betroffener Einrichtungen im Rahmen des jeweils verabschiedeten Rahmenwerks.

Die ehrliche Grenze

Die Data Protection Commission ist eine bedeutende federführende Behörde in der EU; die Einhaltung der Vorschriften liegt in der Verantwortung des Unternehmens. Cyber Crucible verfügt über keine irische Zertifizierung und unterstützt diese Pflichten. Dokumentation ist auf Anfrage erhältlich.

Wie unterstützt Cyber Crucible die Anforderungen an den Datenschutz in den Niederlanden?

Kurze Antwort: In den Niederlanden unterstützt Cyber Crucible die Verpflichtungen einer Organisation im Rahmen der GDPR und des niederländischen GDPR-Umsetzungsgesetzes (durchgesetzt von der Autoriteit Persoonsgegevens), indem Daten und Verarbeitung auf dem Endpunkt minimiert werden. Es werden keine Kundeninhalte, Zugangsdaten oder Schlüssel erfasst, sodass die meisten Verpflichtungen in seinem Verantwortungsbereich kaum Angriffsfläche haben.

Wie es sich einordnet

- **GDPR + nationale Umsetzung.** Verschlüsselung, Zugriffskontrolle und Datenminimierung unterstützen den niederländischen Standard; eine Vereinbarung zur Auftragsverarbeitung ist verfügbar.
- **Datenresidenz.** Eine On-Premises-Bereitstellung hält personenbezogene Daten dort, wo dies erforderlich ist, in den Niederlanden.
- **Cybersicherheitsregime.** Die niederländische Umsetzung von NIS2 (das Cyberbeveiligingswet) befand sich Stand 2026 noch in der Finalisierung; Cyber Crucible unterstützt die Maßnahmen betroffener Einrichtungen im Rahmen des Regelwerks in seiner jeweils verabschiedeten Form.

Die ehrliche Grenze

Die Compliance liegt bei der Organisation und, soweit relevant, bei der Autoriteit Persoonsgegevens. Cyber Crucible verfügt über keine niederländische Zertifizierung und unterstützt diese Pflichten. Dokumentation ist auf Anfrage erhältlich.

Wie unterstützt Cyber Crucible die Datenschutzanforderungen in Spanien?

Kurzantwort: In Spanien unterstützt Cyber Crucible die Verpflichtungen einer Organisation im Rahmen der GDPR und des Organgesetzes zum Datenschutz (LOPDGDD, durchgesetzt von der AEPD), indem keine Kundeninhalte, Zugangsdaten oder Schlüssel erfasst und Daten lokal verarbeitet werden. Da sich nur minimale personenbezogene Daten in seiner Obhut befinden, gibt es für die meisten von der AEPD durchgesetzten Pflichten wenig Angriffsfläche.

Wie die Ausrichtung erfolgt

- **GDPR + LOPDGDD.** Datenminimierung, Verschlüsselung und Zugriffskontrolle unterstützen die spanische Basisanforderung; eine Auftragsverarbeitungsvereinbarung ist verfügbar.
- **Datenresidenz.** Die On-Premises-Bereitstellung hält personenbezogene Daten dort in Spanien, wo dies erforderlich ist.
- **Cybersicherheitsregime.** Die spanische Umsetzung der NIS2 befand sich Stand 2026 noch im Gesetzgebungsverfahren; Cyber Crucible unterstützt betroffene Einrichtungen bei den Maßnahmen gemäß dem jeweils verabschiedeten Rahmenwerk.

Die ehrliche Grenze

Die AEPD gehört zu den aktiveren Aufsichtsbehörden der EU; die Einhaltung der Vorschriften obliegt der Organisation. Cyber Crucible verfügt über keine spanische Zertifizierung und unterstützt diese Pflichten. Dokumentation ist auf Anfrage erhältlich.

Wie unterstützt Cyber Crucible die Anforderungen an den Datenschutz in Italien?

Kurze Antwort: In Italien unterstützt Cyber Crucible die Verpflichtungen einer Organisation im Rahmen der GDPR und des italienischen Datenschutzgesetzes (Privacy Code), das von der Garante durchgesetzt wird, indem Daten und Verarbeitung auf dem Endpunkt minimiert werden. Es werden keine Kundeninhalte, Zugangsdaten oder Schlüssel erfasst, sodass die meisten Verpflichtungen nur minimale Berührungspunkte in seinem Verantwortungsbereich haben.

Wie die Ausrichtung erfolgt

- **GDPR + Privacy Code.** Verschlüsselung, Zugriffskontrolle und Datenminimierung unterstützen den italienischen Basisstandard; eine Vereinbarung zur Auftragsverarbeitung (Data Processing Agreement) ist verfügbar.
- **Datenresidenz.** Der On-Premises-Einsatz hält personenbezogene Daten in Italien, sofern dies erforderlich ist.
- **Cybersicherheitsregime.** Italien gehörte zu den früheren Mitgliedstaaten, die NIS2 in nationales Recht umgesetzt haben; Cyber Crucible unterstützt die Risikomanagement- und Lieferkettenmaßnahmen betroffener Einrichtungen.

Die ehrliche Grenze

Die Garante ist eine aktive Aufsichtsbehörde; die Einhaltung der Vorschriften liegt in der Verantwortung der Organisation. Cyber Crucible verfügt über keine italienische Zertifizierung und unterstützt diese Pflichten. Dokumentation ist auf Anfrage erhältlich.

Wie unterstützt Cyber Crucible die Datenschutzanforderungen in Polen?

Kurze Antwort: In Polen unterstützt Cyber Crucible die Verpflichtungen einer Organisation im Rahmen der GDPR und des polnischen Gesetzes zum Schutz personenbezogener Daten (durchgesetzt von der UODO), indem keine Kundeninhalte, Zugangsdaten oder Schlüssel erfasst werden und die Verarbeitung auf dem Endpunkt erfolgt. Der minimale Datenumfang hält die meisten Verpflichtungen auf einer geringen Angriffsfläche.

Wie es sich einfügt

- **GDPR + nationales Recht.** Datenminimierung, Verschlüsselung und Zugriffskontrolle unterstützen die polnische Grundlage; eine Vereinbarung zur Auftragsverarbeitung ist verfügbar.
- **Datenresidenz.** Die On-Premises-Bereitstellung hält personenbezogene Daten dort, wo erforderlich, in Polen.
- **Cybersicherheitsregime.** Polen hat sein Rahmenwerk für das Nationale Cybersicherheitssystem (KSC) aktualisiert, um NIS2 widerzuspiegeln; Cyber Crucible unterstützt die Maßnahmen betroffener Einrichtungen im Rahmen des jeweils übernommenen Regelwerks.

Die ehrliche Grenze

Die Compliance liegt bei der Organisation und, soweit relevant, bei der UODO. Cyber Crucible verfügt über keine polnische Zertifizierung und unterstützt diese Pflichten. Dokumentation ist auf Anfrage erhältlich.

Wie unterstützt Cyber Crucible die Anforderungen an den Datenschutz in Schweden und den nordischen Ländern?

Kurzantwort: In Schweden und der weiteren nordischen Region unterstützt Cyber Crucible die Verpflichtungen einer Organisation gemäß der DSGVO und den nationalen Umsetzungsgesetzen (in Schweden durchgesetzt von der IMY), indem Daten und Verarbeitung auf dem Endpunkt minimiert werden. Da keine Kundeninhalte, Zugangsdaten oder Schlüssel erfasst werden, haben die meisten Verpflichtungen in ihrem Verantwortungsbereich kaum Angriffsfläche.

Wie die Ausrichtung erfolgt

- **DSGVO + nationale Umsetzung.** Verschlüsselung, Zugriffskontrolle und Datenminimierung unterstützen die nordische Grundlinie; eine Auftragsverarbeitungsvereinbarung ist verfügbar.
- **Datenresidenz.** Die On-Premises-Bereitstellung hält personenbezogene Daten im Land, wo dies erforderlich ist.
- **Cybersicherheitsregelung.** Die nordischen Mitgliedstaaten haben NIS2 in eigenem Tempo in nationales Recht umgesetzt; Cyber Crucible unterstützt die Maßnahmen betroffener Einrichtungen im Rahmen des jeweils übernommenen Regelwerks.

Die ehrliche Grenze

Die Compliance liegt in der Verantwortung der Organisation und der zuständigen nationalen Aufsichtsbehörde. Cyber Crucible verfügt in keinem nordischen Land über eine nationale Zertifizierung und unterstützt diese Pflichten, statt sie zu übernehmen. Dokumentation ist auf Anfrage erhältlich.