Warum NIS2 die Schweiz direkt betrifft?

Die EU-Richtlinie NIS2 entfaltet durch globale Lieferketten eine massive extraterritoriale Wirkung. Kombiniert mit den verschärften Schweizer Gesetzen (revDSG, ISG) entsteht für Stiftungen und KMU ein sofortiger Handlungsbedarf auf Management-Ebene.

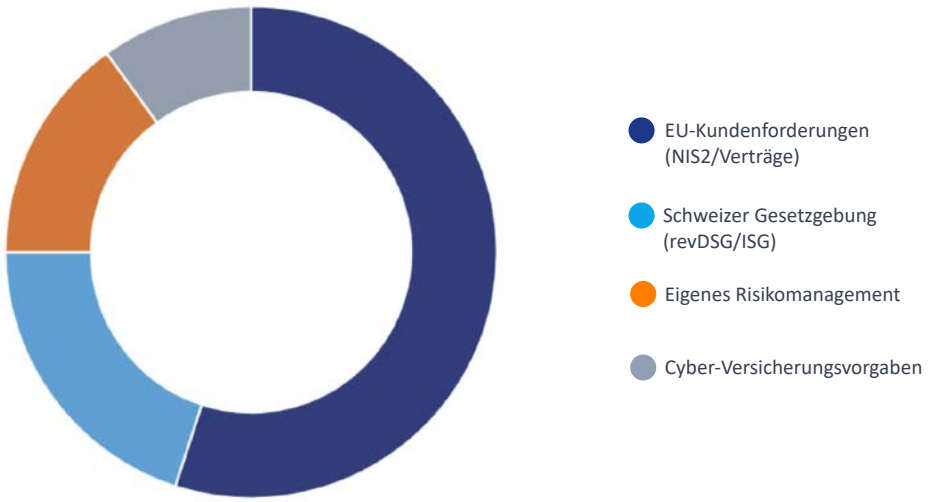
→ Management-Haftung im Fokus!

Der Domio-Effekt in der Lieferkette

Auch wenn die EU-Richtlinie NIS2 in der Schweiz rechtlich nicht direkt gilt, werden Schweizer Unternehmen durch globale Lieferketten faktisch in die Pflicht genommen. EU-Unternehmen (KRITIS) müssen gemäss Artikel 21 (NIS2) die Sicherheit ihrer Lieferkette garantieren. Diese Anforderungen werden vertraglich an Schweizer Zulieferer und Dienstleister weitergegeben. Wer nicht „NIS2-ready“ ist, verliert EU-Aufträge. Kombiniert mit den verschärften Schweizer Gesetzen entsteht ein sofortiger Handlungsbedarf auf Management-Ebene.

EU KRITIS (NIS2 Pflicht) → **Vertragliche** Weitergabe → **Schweizer KMU** (Faktische Pflicht)

Treiber für Cybersicherheit im Schweizer Mittelstand (Schätzung)



Marktforderungen übersteigen zunehmend die reine Inlandsgesetzgebung.

Schweizer Regelwerk vs. NIS2: Ein Direktvergleich

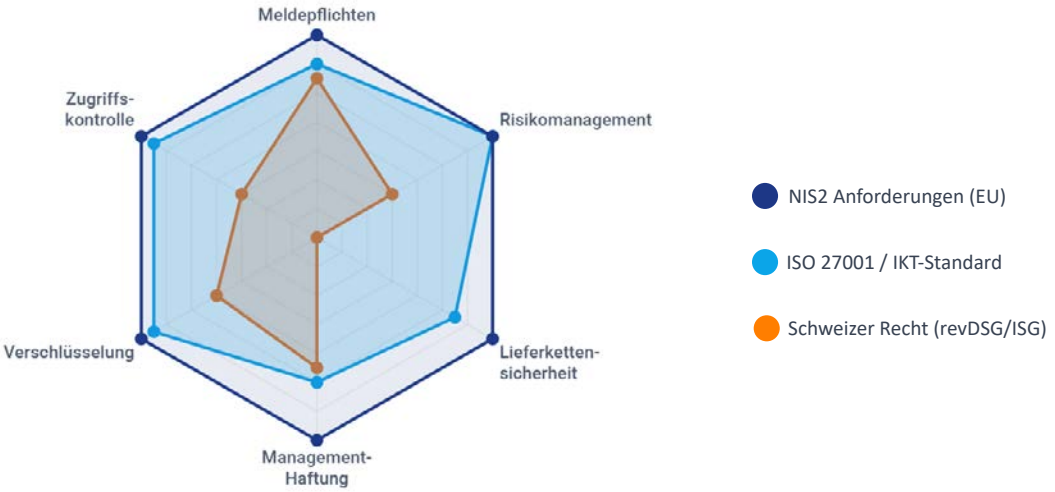
WAS IST PFLICHT? (Gesetzlich)

- **Neues Datenschutzgesetz (revDSG)**
  Meldepflicht bei Datenschutzverletzungen. Persönliche Bussen für Geschäftsleitung & Stiftungsräte bis zu CHF 250'000.
- **Meldepflicht für Cyberangriffe (ab 2025)**
  Obligatorische Meldung an das BACS (Bundesamt für Cybersicherheit) innerhalb von 24h für KRITIS-Betreiber in der Schweiz.
- **Informationssicherheitsgesetz (ISG)**
  Legt den Grundstein für die Sicherheit von Bundesdaten und KRITIS.
- **Zwingende B2B-Verträge**
  Vertragliche Verpflichtung zur Umsetzung von NIS2-Massnahmen durch EU-Kunden.

WAS IST STARK EMPFOHLEN?

- **ISO/IEC 27001:2022 Zertifizierung**
  Deckt rund 70-80% der NIS2-Anforderungen ab. Gilt als stärkster Einzelnachweis der Sorgfaltspflicht (Management-Haftung).
- **IKT-Minimalstandard (BACS)**
  108 Massnahmen basierend auf dem NIST CSF. Freiwillig, gilt aber vor CH-Gerichten zunehmend als Massstab für Sorgfalt.
- **Governance & Schulung**
  Regelmässige Sensibilisierung der Geschäftsleitung und des Stiftungsrates, um persönliche Haftungsrisiken zu minimieren.
- **Vorfallreaktionsplan (Incident Response)**
  Etablierte, getestete Prozesse, um die strengen 24h-Meldepflichten operativ erfüllen zu können.

Konvergenz der Standards: Abdeckung der NIS2-Ziele



Die Schweizer Rechtslage allein genügt oft nicht für EU-Kunden. ISO 27001 schliesst die Lücke massgeblich.

Der Weg zur Compliance

Die Grafik zeigt deutlich: Wer sich ausschliesslich auf das Schweizer Recht (revDSG, ISG) beschränkt, weist erhebliche Lücken in der Lieferkettensicherheit und im umfassenden Risikomanagement auf.
Die Umsetzung des **IKT-Minimalstandards** oder, noch besser, einer **ISO 27001** Zertifizierung schliesst diese Lücken pragmatisch. Für Schweizer Unternehmen bedeutet dies: Die Vorbereitung auf NIS2 (durch EU-Kunden gefordert) deckt gleichzeitig alle Schweizer Regularien optimal ab und minimiert das persönliche Haftungsrisiko der Organe drastisch.

CYBERSICHERHEIT & COMPLIANCE · WHITEPAPER

NIS2, ISG & revDSG
Was gilt in der Schweiz und in Liechtenstein?

Stand: April 2026
Liechtenstein: CSG seit 1.2.2025
Schweiz: KRITIS-Meldepflicht seit 1.4.2025
Deutschland: NIS2UmsuCG seit 1.3.2025

LIECHTENSTEIN
NIS2 vollständig umgesetzt via CSG. EWR-Pflichtrecht. ~1'800–2'200 betroffene Einrichtungen. Aufsicht: Stabsstelle Cyber-Sicherheit.

SCHWEIZ
Eigenständiges Recht: revDSG + ISG + KRITIS-Meldepflicht. NIS2 gilt nicht direkt, konvergiert aber faktisch.

WARUM JETZT HANDELN
Persönliche Haftung der Geschäftsleitung ist in beiden Ländern real. Sanktionen gegen Privatvermögen. Kein Versicherungsschutz für fahrlässige Untätigkeit.

01 DIREKTVERGLEICH: SCHWEIZ · LIECHTENSTEIN · DEUTSCHLAND

DIMENSION	CH SCHWEIZ	LI LIECHTENSTEIN	DE DEUTSCHLAND
Rechtsbindung	Eigenständig: revDSG, ISG, KRITIS-Meldepflichtverordnung	NIS2-PFLICHTIG CSG seit 1.2.2025	NIS2-PFLICHTIG NIS2UmsuCG seit 1.3.2025
Meldepflicht	24H an BACS (nur KRITIS)	24H / 72H / 1 MONAT NIS2-System	24H / 72H / 1 MONAT an BSI
Management-Schulung	-	PFLICHT Art. 20 Abs. 2 NIS2	PFLICHT Art. 20 Abs. 2 NIS2UmsuCG
DORA (Finanzsektor)	-	GILT SEIT 1.2.2025 für FMA Institute	GILT SEIT 17.1.2025 lex specialis zu NIS2

Das revidierte Datenschutzgesetz (DSG) seit Sept 2023 verlangt adäquate Datensicherheit nach EU Standards. Zudem trat Jan 2024 das **Bundes-Informationssicherheitsgesetz (ISG)** in Kraft, das für Bundesbehörden und Betreiber kritischer Infrastrukturen (u.a. Banken, Versicherer, Gesundheitswesen, Energie, Verkehr) ein **ISMS nach ISO 27001** verlangt. Damit steigt der Compliance-Druck auch auf grössere Organisationen in der Schweiz, sich nach NIS2-ähnlichen Vorgaben zertifizieren zu lassen.

UNTERNEHMEN (SEKTORENFOKUS)

- **Energie & Wasser:** Strom, Gas, Fernwärme, Trink- und Abwasser
- **Gesundheitswesen:** Krankenhäuser, Pharma, Labore, Medtech
- **Transport:** Luftfahrt, Schiene, Schifffahrt, ÖPNV
- **Digitale Infrastruktur:** Cloud, RZ, Vertrauensdienste, DNS
- **Bank- & Finanzwesen:** Kreditinstitute und Handelsplätze
- **Verarbeitendes Gewerbe:** Maschinenbau, Kfz, Elektronik
- **Lebensmittel:** Produktion, Verarbeitung und Grosshandel
- **Entsorgung:** Abfallbewirtschaftung
- **Chemikalien:** Herstellung und Vertrieb
- **Post- & Kurierdienste**
- **Digitale Dienste:** Marktplätze, Suchmaschinen, Soziale Netzwerke

STIFTUNGEN & NON-PROFITS

Eine Stiftung ist dann betroffen, wenn sie eine wirtschaftliche Tätigkeit ausübt und in einen der genannten Sektoren fällt:

- **Stiftungen im Gesundheitswesen:** Krankenhäuser/Pflege (ab 50 MA NIS2-pflichtig)
- **Forschungsstiftungen:** Sofern keine reine akademische Grundlagenforschung
- **Bildungsstiftungen:** Meist ausgenommen, ausser bei digitaler Infrastruktur
- **Abgrenzung:** Gemeinnützigkeit schützt nicht vor Audit-Pflichten bei Erreichen der Schwellenwerte

BETROFFEN SIND:

- Stiftungen mit EU-Niederlassungen, Projektträgern oder Tochterorganisationen
- Stiftungen, die IT- oder Cloud-Services nutzen
- Stiftungen, die kritische, relevante oder gesellschaftliche Leistungen bieten
- Stiftungen, die personenbezogene oder medizinische Daten verwalten
- Stiftungen mit indirekter Betroffenheit als Lieferanten oder Partner

02 MELDEPFLICHTEN IM DETAIL

LI LIECHTENSTEIN & DE DEUTSCHLAND — NIS2-DREISTUFENSYSTEM

24 h
Frühwarnung
Erste Einschätzung: Böswillige Handlung? Grenzüberschreitende Auswirkungen möglich?

72 h
Vorfallmeldung
Schweregrad, Auswirkungen, Kompromittierungsindikatoren (IoCs), betroffene Dienste

1 M
Abschlussbericht
Detailbeschreibung, Ursachenanalyse, ergriffene Massnahmen

Adressat LI / DE
CSIRT.LI (Stabsstelle Vaduz, Meldeportal) / BSI (meldung.bsi.bund.de)

CH SCHWEIZ — EIGENSTÄNDIGES SYSTEM

24 h
KRITIS-Meldung
Cyberangriff mit möglichen Auswirkungen auf kritische Infrastruktur an BACS. Gilt seit 1.4.2025.

14 T
Ergänzungsbericht
Vervollständigung der Erstmeldung. Keine explizite Abschlussfrist wie NIS2.

rasch
Datenpanne (revDSG)
Meldung an EDÖB bei hohem Risiko für Betroffene. Empfehlung: 72h analog DSGVO.

Adressat & Geltungsbereich
BACS (meldung.bacs.admin.ch) / EDÖB. Nur KRITIS. Sanktion: CHF 100'000 bei Nichtmeldung.

03 DIE 10 MINDESTMASSNAHMEN (ART. 21 NIS2) — VERBINDLICH IN LI, BEST PRACTICE IN CH

1 **Risikoanalyse & Sicherheitsrichtlinien**
ISMS, jährliches Risikoregister, dokumentierter Behandlungsplan !

2 **Incident Management**
IRP mit 24h-Meldefähigkeit, Tabletop-Übung jährlich, Eskalationspfade !

3 **Business Continuity**
3-2-1-Backup (offline!), BIA, RTO/RPO, jährlichlicher Restore-Test !

4 **Supply Chain Security**
Lieferantenregister, Cybersecurity-Klauseln, Audit-Rechte, Meldefristen Dienstleister !

5 **IT-Erwerb, Entwicklung, Wartung**
Patch-Management: kritisch 48–72h, wichtig 7 Tage, Asset-Inventar

6 **Wirksamkeitsbewertung**
Interne Audits, Penetrationstest jährlich, KPIs (MTTD, MTTR, Patch-Rate)

7 **Cyberhygiene & Schulungen**
Awareness jährlich, Management-Schulung dokumentiert (Art. 20 Abs. 2) !

8 **Kryptographie & Verschlüsselung**
AES-256 at rest, TLS 1.2+, Schlüsselmanagement, Kryptographie-Policy

9 **Personalsicherheit & Zugangskontrolle**
RBAC, Least Privilege, Joiner-Mover-Leaver, sofortige Zugangssperrung

10 **MFA & sichere Kommunikation**
Phishing-resistente MFA (FIDO2/TOTP), kein SMS-OTP, für alle Remote-Zugänge & Cloud !

! Orange markierte Massnahmen werden in Audits am häufigsten als unzureichend bewertet.

04 SANKTIONSRAHMEN

LI WESENTLICHE EINRICHTUNG

CHF 10 Mio.

oder 2% des weltweiten Jahresumsatzes

+ CHF 100'000/Tag Zwangsgeld
+ bis 3 Jahre Funktionssperre

LI WICHTIGE EINRICHTUNG

CHF 7 Mio.

oder 1,4% des weltweiten Jahresumsatzes

Persönliche Haftung Stiftungsrat/GF
Keine D&O-Abdeckung für Vorsatz

CH SCHWEIZ

CHF 250k

revDSG – gegen natürliche Personen

Art. 754 OR: unlimitierte Privathaftung
CHF 100'000 bei KRITIS-Nichtmeldung

In der Schweiz richten sich revDSG-Sanktionen ausdrücklich gegen **natürliche Personen**. Die OR-Haftung nach Art. 754 ist **unlimitiert** – Privatvermögen, Liegenschaften, Altersvorsorge inklusive. Dies ist strukturell schärfer als die EU-Obergrenzen.

05 SPEZIALTHEMA: STIFTUNGEN

Warum Stiftungsräte besonders exponiert sind

HAFTUNG OHNE KORREKTIV

STRUKTURELLE RISIKEN

- Keine Aktionäre / Gesellschafter als Kontrollkorrektiv
- IT vollständig ausgelagert = Supply-Chain-Risiko nach NIS2
- Sensible Daten: Begünstigte, Spender, Gesundheitsbezug
- Ressourcenknappheit: keine dedizierte IT-Security
- Oft in regulierten Sektoren tätig (Gesundheit, Finanzen)

LI WER FÄLLT UNTER NIS2?

- Finanzstiftungen mit Bank-/Anlageaktivitäten >50 MA
- Stiftungen im Gesundheitswesen >10 Mio. EUR
- Treuhandgesellschaften als ICT-Dienstleister B2B
- Familienstiftungen: Prüfung nach Sektor & Grösse
- Kleine gemeinnützige Stiftungen: meist nicht direkt betroffen

HAFTUNG STIFTUNGSRAT

- **LI:** BJR (Art. 182 PGR) schützt nur bei nachweislicher Information
- **LI:** 3-jährige Funktionssperre bei wiederh. Verstössen
- **CH:** Art. 84 ZGB, objektiver Sorgfaltsmassstab
- **CH:** Art. 754 OR, unlimitierte Privathaftung, Beweislastumkehr
- Delegation an IT reicht nicht – GF-Ebene bleibt verantwortlich

5 SOFORTMASSNAHMEN

- Scoping-Check: Fällt die Stiftung unter CSG (LI)?
- Stiftungsratsprotokoll mit Cybersecurity-Beschluss
- Management-Schulung (Art. 20 NIS2) + Teilnahmedokumentation
- IT-Dienstleister-Audit: Vertragscheck auf Cybersecurity-Klauseln
- Incident Response Plan mit 24h-Meldefähigkeit testen

06 HANDLUNGSPLAN NACH ZEITHORIZONT

PHASE 1
0–30 Tage

- MFA für alle Cloud-Dienste & VPN aktivieren
- Backup-Restore tatsächlich testen (offline Kopie!)
- Verantwortlichkeit in Geschäftsleitung benennen
- Notfallkontaktliste (CSIRT.LI / BACS / Anwalt)
- Öffentliche Ports / Shadow IT scannen

PHASE 2
1–3 Monate

- Gap-Analyse gegen Art. 21 NIS2 / IKT-Minimalstandard
- Incident Response Plan + Tabletop-Übung
- IT-Lieferanten-Inventar & Vertragscheck
- Management-Schulung (dokumentiert)
- ISMS-Basisdokumentation: Richtlinien, Risikoregister

PHASE 3
3–12 Monate

- ISO 27001 Implementierung starten
- Externer Penetrationstest
- Supply Chain: ISO 27001 / SOC 2 bei Lieferanten einfordern
- Monitoring / Managed SOC einführen
- Registrierung BSI / Stabsstelle abschliessen

PHASE 4
12–24 Monate

- ISO 27001 Zertifizierung abschliessen
- Quartalsweise KPI-Berichterstattung an Leitungsorgane
- Externe Audits alle 2–3 Jahre etablieren
- Regulatorisches Monitoring: KRITIS-G Schweiz, NIS2-Anpassungen
- Cyber-Versicherung prüfen & optimieren

07 FRAMEWORK-VERWEISE: WELCHE STANDARDS DECKEN NIS2 AB

I ISO/IEC 27001:2022

- ✓ Deckt ~70–80% der NIS2-Anforderungen ab
- ✓ Stärkster Einzelnachweis in CH, LI und DE
- ✓ Anerkannt als Sorgfaltspflichtmassstab vor Gericht
- ✓ Pflichthafte Management-Review-Zyklen (Kap. 9.3)
- ✓ Zertifizierung durch akkreditierte Stelle empfohlen

K IKT-Minimalstandard BACS (CH)

- ✓ 108 Massnahmen auf Basis NIST CSF – freiwillig aber massgeblich
- ✓ Schwellen: Identify, Protect, Detect, Respond, Recover
- ✓ Obligatorisch für Strom- und Gasbranche
- ✓ Geplante KRITIS-G Schweiz orientiert sich an NIS2 + IKT-Minimalstandard
- ✓ Best Practice für CH-Gerichte als Sorgfaltsmassstab

N NIST CSF 2.0 (Feb. 2024)

- ✓ Neu: Governanz-Funktion (GV) als 6. Säule
- ✓ International anerkannt, kein Zertifikat, aber Strukturgeber
- ✓ NIS2 Mapping: GV.RM = Art. 21(a), RS.MA = Art. 21(b)
- ✓ BSI IT-Grundschutz deckt NIS2 ebenfalls vollständig ab
- ✓ Für KMU: BSI Basis-Absicherung als pragmatischer Einstieg

Rechtsstand April 2026 · LI: CSG/CSV seit 1.2.2025 · CH: KRITIS-Meldepflicht seit 1.4.2025 · DE: NIS2UmsuCG seit 1.3.2025

Crisanto Farese
+41 41 748 60 10
crisanto.farese@profetas.ch

Lassen Sie sich von uns beraten!

nis2-audit.ch

profetas. wirtuosa. emitec datacom