SECJUR

NIS2 für Wohlfahrt & NGOs

Warum gemeinnützige Organisationen NIS2 nicht ignorieren dürfen, und wie Readiness auch mit kleinem Budget gelingt.

»NGO« oder »Wohlfahrt« ist kein eigener NIS2-Sektor, trotzdem sind viele gemeinnützige Organisationen betroffen. Wohlfahrtsverbände, die **Krankenhäuser, Pflege oder Rettungsdienste** betreiben, fallen über den Sektor Gesundheit unter NIS2. Andere geraten als Dienstleister und Lieferanten betroffener Einrichtungen oder über die öffentliche Verwaltung in den Anwendungsbereich. Hinzu kommt: **sensible Spender-, Klienten- und Mitgliederdaten** erfordern ohnehin ein hohes Sicherheitsniveau.

In diesen vier Situationen wird NIS2 für gemeinnützige Organisationen konkret:

BETROFFENHEIT

Ehrlich prüfen

- Kein eigener Sektor, aber häufig indirekt betroffen
- Über betriebene Einrichtungen (Gesundheit, Rettungsdienst)
- Als Lieferant betroffener Stellen oder über die öffentliche Verwaltung
- Saubere Einordnung nach §28 NIS2UmsuCG schafft Klarheit

BEGRENZTE RESSOURCEN

Angemessenes Mindestmaß

- Kleine IT-Teams, Ehrenamtliche und schmale Budgets sind die Regel
- Genau das macht Organisationen zum attraktiven Ziel
- NIS2 verlangt kein Großkonzern-Setup
- Aber ein dokumentiertes Mindestmaß an Risikomanagement und Notfallvorsorge

SENSIBLE DATEN & DSGVO

Zwei Regime greifen ineinander

- Spender-, Klienten-, Patienten- und Mitgliederdaten sind hochsensibel
- Ein Vorfall kann NIS2 und DSGVO gleichzeitig auslösen
- Meldepflichten nach Art. 33 DSGVO und §32 NIS2UmsuCG
- Ein integrierter Ansatz spart Aufwand und schützt Vertrauen

VORSTANDSVERANTWORTUNG

Nicht delegierbar

- Leitung (Vorstand, Geschäftsführung) trägt die Verantwortung (§38)
- Verantwortung für Maßnahmen und deren Überwachung
- Schulungspflicht für die Leitungsebene
- Nicht vollständig an Dienstleister oder Ehrenamt delegierbar

Indirekt

NGOs sind kein eigener Sektor: Betroffenheit entsteht über Einrichtungen, Lieferkette und Verwaltung

24 h

Frist für die Erstmeldung erheblicher Sicherheitsvorfälle bei betroffenen Organisationen

DSGVO +

Sensible Spender- und Klientendaten erfordern Sicherheit, unabhängig von der NIS2-Pflicht

SECJUR

NIS2-Readiness in 6 Schritten

Von der ehrlichen Betroffenheitsprüfung bis zur Notfallvorsorge, pragmatisch und auf begrenzte Ressourcen gemeinnütziger Organisationen zugeschnitten.

SCHRITT 01

Betroffenheit klären

- [ ] **Prüfen,** ob Einrichtungen (Klinik, Pflege, Rettungsdienst) einen NIS2-Sektor berühren
- [ ] **Rolle** als Dienstleister/Lieferant betroffener Stellen bewerten
- [ ] **Bezug** zur öffentlichen Verwaltung und zu Förderstrukturen prüfen
- [ ] **Einordnung** nach §28 NIS2UmsuCG schriftlich dokumentieren
- [ ] **Ergebnis** bei Unsicherheit fachlich gegenprüfen lassen

SCHRITT 02

Daten & Systeme erfassen

- [ ] **Spender-, Klienten-, Mitglieder-** und Patientendaten inventarisieren
- [ ] **Kritische Systeme** (CRM, Spendentools, Fachverfahren) dokumentieren
- [ ] **Cloud-Dienste** und externe IT-Dienstleister auflisten
- [ ] **Verantwortlichkeiten,** auch im Ehrenamt, klar festlegen
- [ ] **Übersicht** zentral und aktuell halten

SCHRITT 03

Basis-Schutz umsetzen

- [ ] **Mehr-Faktor-Authentifizierung** für alle wichtigen Zugänge aktivieren
- [ ] **Regelmäßige Backups** einrichten und Wiederherstellung testen
- [ ] **Zugriffsrechte** nach Rollen vergeben (Need-to-know)
- [ ] **Angemessene Maßnahmen** nach §30 NIS2UmsuCG dokumentieren
- [ ] **Bekannte Schwachstellen** zeitnah schließen

SCHRITT 04

Datenschutz verzahnen

- [ ] **VVT** aktualisieren
- [ ] **TOMs** für besondere Datenkategorien (Art. 9 DSGVO) prüfen
- [ ] **Doppelte Meldepflichten** NIS2 + DSGVO in einem Prozess bündeln
- [ ] **DSB und IT-Verantwortliche:n** zusammenbringen
- [ ] **Nachweise** für beide Regime zentral ablegen

SCHRITT 05

Notfall & Meldung

- [ ] **Einfachen Incident-Response-Plan** erstellen und im Team teilen
- [ ] **Meldeweg** an Behörde/BSI klären (falls betroffen) und testen
- [ ] **Notfallkontakte** und Eskalation auf einer Seite festhalten
- [ ] **Wiederanlauf** für kritische Dienste (z. B. Pflege-IT) sicherstellen
- [ ] **Ernstfall** regelmäßig im Team durchsprechen

SCHRITT 06

Leitung & Ehrenamt

- [ ] **Vorstand/Geschäftsführung** in Risikoentscheidungen einbinden (§38)
- [ ] **Awareness-Schulung** für Haupt- und Ehrenamtliche etablieren
- [ ] **Verantwortung** nicht vollständig an Dienstleister delegieren
- [ ] **Maßnahmen** jährlich auf Wirksamkeit überprüfen
- [ ] **Verbesserungen** nachhalten und dokumentieren

SECJUR

Häufige Stolperfallen und Quick Wins

Was Wohlfahrt und NGOs bei NIS2 typischerweise unterschätzen, und womit sich mit kleinem Budget schnell Wirkung erzielen lässt. Links die Fallen, rechts die Hebel.

STOLPERFALLE 01

»Uns betrifft das nicht«

- [ ] **Betroffenheit** über Einrichtungen oder Lieferkette übersehen
- [ ] **Annahme,** NGOs seien generell ausgenommen
- [ ] **Keine dokumentierte Prüfung,** Nachweis fehlt im Ernstfall
- [ ] **Ehrliche Prüfung** schafft früh Klarheit

QUICK WIN 01

MFA & Passwortmanager

- [ ] **Kostenlose MFA** für alle wichtigen Konten aktivieren
- [ ] **Passwortmanager** statt geteilter Logins einführen
- [ ] **Sofort spürbarer Schutz** ohne Budget
- [ ] **Größte Wirkung** pro investierter Stunde

STOLPERFALLE 02

Ehrenamt ohne Awareness

- [ ] **Wechselnde Ehrenamtliche** ohne Sicherheitsschulung
- [ ] **Geteilte Logins** und schwache Passwörter im Umlauf
- [ ] **Phishing** trifft engagierte, aber ungeschulte Helfer:innen
- [ ] **Kurze, regelmäßige Awareness** senkt das Risiko spürbar

QUICK WIN 02

DSGVO-Synergie nutzen

- [ ] **Bestehende VVT und DSFA** für die NIS2-Prüfung verwenden
- [ ] **Ein Prozess** für beide Meldepflichten aufsetzen
- [ ] **Doppelaufwand** vermeiden, ein Rahmenwerk genügt
- [ ] **Vorhandene Nachweise** gezielt wiederverwenden

STOLPERFALLE 03

Spenderdaten unterschätzt

- [ ] **Sensible Daten** in unsicheren Tools und Tabellen
- [ ] **Keine klare Verantwortung** für Datenschutz
- [ ] **Ein Datenleck** beschädigt das Vertrauen nachhaltig
- [ ] **Klare Zuständigkeit** und sichere Tools schützen den Ruf

QUICK WIN 03

Notfallplan als 1-Seiter

- [ ] **Wer-macht-was** im Vorfall auf einer A4-Seite festhalten
- [ ] **Notfallkontakte** und Backup-Wiederherstellung notieren
- [ ] **Enorm stressreduzierend,** gerade für kleine Teams
- [ ] **Von Unsicherheit** zu handlungsfähiger Meldekette

SECJUR

Mit SECJUR zu 100 % NIS2-Compliance

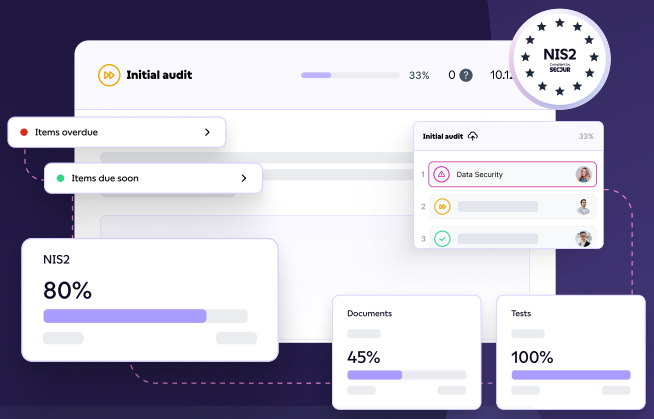
Mit der Durchsetzung der NIS2-Richtlinie in 2026 rücken zehntausende Unternehmen neu in den regulatorischen Fokus. Die Anforderungen an Informationssicherheit, Risikomanagement und Managementverantwortung steigen spürbar – ebenso wie die Erwartungen von Aufsichtsbehörden und Geschäftspartnern.

Mit dem Digital Compliance Office von SECJUR und unseren zertifizierten Expert:innen setzen Sie die Anforderungen der NIS2-Richtlinie strukturiert und effizient um. Bestehende Sicherheits- und Governance-Strukturen werden gezielt eingebunden und systematisch weiterentwickelt.

- Aufbau und Betrieb eines NIS2-konformen ISMS inkl. Risiko- und Incident-Management
- Klare Verantwortlichkeiten, Dokumentation und Nachweise für Behörden
- Profitieren Sie von der dedizierten Erfahrung unserer TÜV-geprüften Expert:innen

Reduzieren Sie manuellen Aufwand deutlich, gewinnen Transparenz über Ihren Compliance-Status und schaffen eine belastbare Grundlage für regulatorische Prüfungen und anspruchsvolle Kundenanforderungen.

Für unsere Bestandskunden bieten wir attraktive Konditionen, um frühzeitig Klarheit zu schaffen und NIS2-Readiness planbar umzusetzen.



→ **Jetzt informieren**

Mit SECJUR zur automatisierten Compliance

“Der gesetzeskonforme Umgang mit personenbezogenen Daten wäre für uns auf Grund der Vielzahl an unterschiedlichen Sachverhalten alleine kaum zu stemmen, auch weil ein Großteil der Arbeit im Ehrenamt geschieht. Durch die Zusammenarbeit mit SECJUR können wir uns jetzt auf das Wesentliche konzentrieren.”

Paul Jäde
Vorstand, Changing Cities e.V.

CHANGING CITIES

FÜHRENDE UNTERNEHMEN VERTRAUEN AUF SECJUR

Pestalozzi Stiftung

Der Kinderschutzbund

PARTNER
DRK Service | Deutsches Rotes Kreuz

CHANGING CITIES

www.secjur.com