SECJUR

ISO/IEC 27001 für NGOs & Wohlfahrt

Was Gründer:innen und Geschäftsführer:innen jetzt wissen müssen — von Förderpflichten über Cyberrisiken bis zur Zertifizierung.

Soziale Einrichtungen, Wohlfahrtsverbände und NGOs verarbeiten täglich besonders sensible Daten: Gesundheits- und Sozialdaten, Kontodaten von Spendern, Falldaten von Klient:innen. Gleichzeitig steigen **Anforderungen von Fördergebern, Aufsichtsbehörden und Kooperationspartnern** — und Cyberangriffe auf gemeinnützige Organisationen nehmen zu. **ISO/IEC 27001** ist der internationale Standard für Informationssicherheit und gibt Ihrer Organisation ein strukturiertes Rahmenwerk, um Risiken zu kontrollieren und **Vertrauen gegenüber Stakeholdern nachweisbar zu machen** — statt jeden Fördergeber einzeln zu überzeugen.

Wann ISO 27001 für Ihre Organisation konkret wird:

TREIBER 01

Förderbedingungen & Auflagen

Öffentliche Fördergeber, EU-Programme und private Stiftungen stellen zunehmend Anforderungen an Datensicherheit. Ohne ISMS oder belastbare Roadmap können Organisationen bei Förderanträgen und **Vertragsverlängerungen** herausfallen.

TREIBER 02

Datenschutz & DSGVO-Pflicht

NGOs verarbeiten oft Kategorie-Daten nach Art. 9 DSGVO. Ein zertifiziertes ISMS dokumentiert **technische und organisatorische Maßnahmen** und reduziert das Bußgeldrisiko bei Datenschutzverletzungen erheblich.

TREIBER 03

Cyberrisiken & Betriebsstabilität

Ransomware und Phishing treffen gemeinnützige Organisationen überproportional — häufig mangels IT-Budget. Ein ISMS schafft **Mindeststandards und Notfallprozesse** für den laufenden Betrieb.

TREIBER 04

Vertrauen bei Partnern & Spendern

Unternehmenspartner und institutionelle Spender erwarten nachweisbare Sorgfalt. Ein ISO-Zertifikat ist ein **objektiver Nachweis** — und ersetzt aufwändige Einzelauskünfte gegenüber jedem neuen Partner.

Art. 32 DSGVO

verpflichtet zu **technischen & organisatorischen Maßnahmen** — ISO 27001 liefert den Nachweis

3–6 Monate

typische Umsetzungszeit mit **Plattform & Expert:innen**, statt 12+ Monate im Eigenbau

Ein Zertifikat

ersetzt unzählige Einzelnachweise und beschleunigt das **Onboarding bei Fördergebern** spürbar

SECJUR

Ihr Weg zum ISMS — Schritt 1 bis 6

Die ersten sechs Schritte schaffen das Fundament: Auftrag, Geltungsbereich, Asset-Transparenz und eine belastbare Risikobasis für Ihre Organisation.

SCHRITT 01

Auftrag & Führung sichern

- [ ] **Auslöser dokumentieren** und gegenüber der Geschäftsführung klar aufbereiten
- [ ] **Budget, Ressourcen und Zeitrahmen** formell freigeben lassen
- [ ] **ISMS-Verantwortliche:n benennen** und in der Organisationsstruktur verankern
- [ ] **Sichtbares Commitment der GF** einholen und nach innen kommunizieren
- [ ] **Regelmäßige Berichterstattung** an die Leitungsebene etablieren

SCHRITT 02

Geltungsbereich definieren

- [ ] **Standorte, Abteilungen und Außenstellen** klar abgrenzen und dokumentieren
- [ ] **Sensible Prozesse einbeziehen** — Sozialdaten, Spenderdaten, Klientendaten
- [ ] **Externe Dienstleister und Cloud-Dienste** als Schnittstellen erfassen
- [ ] **Scope dokumentieren** und begründete Ausschlüsse festhalten
- [ ] **Pilot-Scope evaluieren** — z.B. eine Abteilung als ersten Geltungsbereich

SCHRITT 03

Asset-Register aufbauen

- [ ] **IT-Systeme, Server und Endgeräte** vollständig erfassen und dokumentieren
- [ ] **Anwendungen und Datenbanken** mit Schutzbedarf klassifizieren
- [ ] **Sensible Datenarten kennzeichnen** — Sozialdaten nach Art. 9 DSGVO besonders
- [ ] **Verantwortlichkeiten** und Ansprechpartner je Asset zuweisen
- [ ] **Externe Auftragsverarbeiter** und deren Datenzugriffe vollständig erfassen

SCHRITT 04

Risiken bewerten

- [ ] **Bedrohungsszenarien identifizieren** — Phishing, Ransomware, Datenpannen
- [ ] **Eintrittswahrscheinlichkeit und Schadenshöhe** für jeden Risikoeintrag bewerten
- [ ] **NGO-spezifische Risiken priorisieren** — Ehrenamt, veraltete IT, fehlende Prozesse
- [ ] **Risikoakzeptanzkriterien** gemeinsam mit der Geschäftsführung abstimmen
- [ ] **Risikobehandlungsplan erstellen** und Maßnahmen mit Terminen belegen

SCHRITT 05

Maßnahmen festlegen (SoA)

- [ ] **Controls aus Anhang A auswählen** und auf die eigene Organisation anpassen
- [ ] **Statement of Applicability (SoA) erstellen** mit Begründung je Control
- [ ] **Maßnahmenplan aufsetzen** mit konkreten Terminen und Verantwortlichen
- [ ] **Budget und Kapazitäten** je Maßnahme realistisch zuordnen
- [ ] **Fortschritt regelmäßig überprüfen** und den Plan aktuell halten

SCHRITT 06

Leitlinien & Richtlinien erstellen

- [ ] **IS-Leitlinie verabschieden** und für alle Mitarbeitenden zugänglich machen
- [ ] **Zugriffs- und Passwortrichtlinien** sowie Clean-Desk-Policy einführen
- [ ] **Incident-Response-Plan dokumentieren** inklusive 72h-Meldepflicht Art. 33 DSGVO
- [ ] **Homeoffice-Regelung** und Umgang mit externen Datenträgern festlegen
- [ ] **Kirchliches Datenschutzrecht prüfen** — KDG (kath.) oder DSG-EKD (evang.)

SECJUR

Ihr Weg zum ISMS — Schritt 7 bis 12

Die zweite Hälfte bringt das ISMS in den Betrieb: technische Maßnahmen, Schulung, internes Audit, Zertifizierung und laufender Betrieb.

SCHRITT 07

Technische Maßnahmen umsetzen

- [ ] **Zugriffsrechte vergeben** nach Need-to-know-Prinzip und regelmäßig überprüfen
- [ ] **Patch- und Schwachstellenmanagement** für alle Systeme strukturiert aufsetzen
- [ ] **Backups und Wiederherstellung** regelmäßig testen und Ergebnisse dokumentieren
- [ ] **Verschlüsselung aktivieren** für sensible Daten at rest und in transit
- [ ] **Monitoring und Logging einrichten** für sicherheitsrelevante Systeme und Zugriffe

SCHRITT 08

Dienstleister absichern

- [ ] **Auftragsverarbeiter identifizieren** die Zugriff auf personenbezogene Daten haben
- [ ] **AVV nach Art. 28 DSGVO abschließen** mit allen relevanten Auftragsverarbeitern
- [ ] **Sicherheitsanforderungen** vertraglich verankern und nachweisbar machen
- [ ] **Fernwartungszugänge kontrollieren** und sämtliche Zugriffe protokollieren
- [ ] **Dienstleister-Sicherheit** regelmäßig bewerten und bei Bedarf nachfordern

SCHRITT 09

Mitarbeitende schulen

- [ ] **Pflichtschulung durchführen** zu Informationssicherheit für alle Mitarbeitenden
- [ ] **Phishing-Simulationen** und Awareness-Tests regelmäßig einplanen
- [ ] **Ehrenamtliche und Honorarkräfte** explizit in die Schulungsmaßnahmen einbeziehen
- [ ] **Incident-Response-Prozess schulen** und Meldewege praxisnah kommunizieren
- [ ] **Schulungsnachweise dokumentieren** und lückenlos aufbewahren

SCHRITT 10

Internes Audit & Review

- [ ] **Auditplan erstellen** Scope festlegen und unabhängige Auditor:innen benennen
- [ ] **Nichtkonformitäten erfassen** bewerten, priorisieren und schriftlich festhalten
- [ ] **Managementbewertung abhalten** mit der Geschäftsführung und dokumentieren
- [ ] **Wirksamkeit der Controls prüfen** und Schwachstellen systematisch adressieren
- [ ] **Korrekturmaßnahmen einleiten** und Umsetzung konsequent nachverfolgen

SCHRITT 11

Zertifizierungsaudit bestehen

- [ ] **DAkkS-akkreditierte Stelle wählen** und frühzeitig beauftragen
- [ ] **Stage-1-Audit vorbereiten** — alle Nachweise und Dokumentation bereitstellen
- [ ] **Offene Punkte aus Stage 1** systematisch nachbessern und schließen
- [ ] **Stage-2-Audit begleiten** und Audit-Findings strukturiert abarbeiten
- [ ] **Zertifikat kommunizieren** gegenüber Fördergebern, Partnern und Spendern

SCHRITT 12

ISMS am Leben halten

- [ ] **KVP verankern** — kontinuierliche Verbesserung als festen Prozess etablieren
- [ ] **Jährliche Überwachungsaudits** einplanen und Rezertifizierung alle 3 Jahre vorbereiten
- [ ] **Neue Mitarbeitende und Ehrenamtliche** direkt ins ISMS und die Schulungen aufnehmen
- [ ] **Incident-Learnings einarbeiten** und Erkenntnisse systematisch dokumentieren
- [ ] **ISMS-Kennzahlen berichten** und Fortschritte regelmäßig an die GF kommunizieren

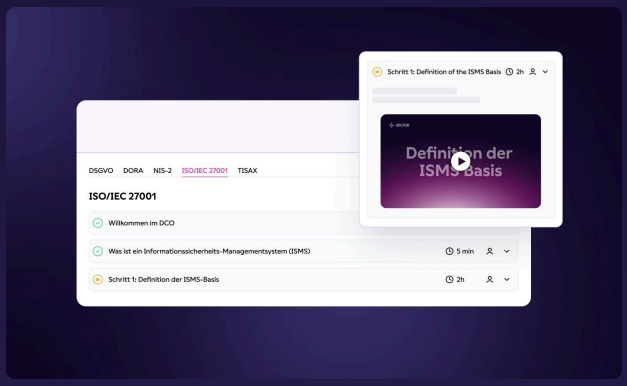
SECJUR

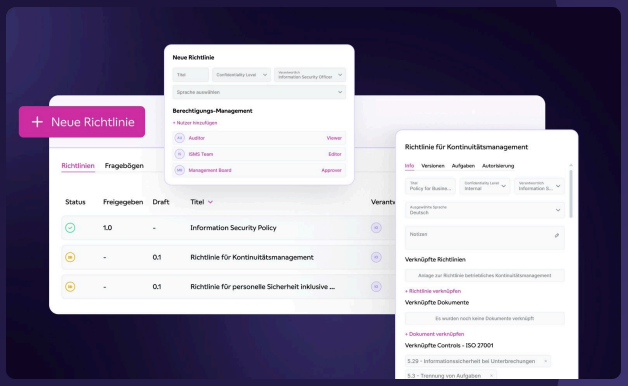
Wie SECJUR die ISO/IEC 27001 zum Kinderspiel macht

Mit der **SECJUR Automatisierungsplattform** und unseren **TÜV-zertifizierten Expert:innen** setzen Sie ISO 27001 in Rekordzeit um:

- Automatisierte Erstellung und Verwaltung Ihres ISMS
- Integriertes Risikomanagement & Lieferantenbewertungen
- Audit-Readiness auf Knopfdruck

Damit sparen Sie hunderte Stunden Aufwand – und sichern sich den entscheidenden Wettbewerbsvorteil bei großen Kundenprojekten.





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