



ISO 27001 • WOHLFAHRT & NGOS

ISO 27001 für gemeinnützige Organisationen: *Vertrauen schützen.*

Wohlfahrtsverbände, soziale Träger und NGOs verwalten die sensibelsten Daten überhaupt: die von Menschen in Notlagen und die ihrer Spender. Genau dieses Vertrauen ist ihre Existenzgrundlage. Zuwendungsgeber und Kostenträger verlangen zunehmend nachweisbare Sicherheit, große Träger fallen unter NIS2, und Ransomware trifft soziale Einrichtungen genauso wie Unternehmen. Dieses Whitepaper zeigt, warum ISO 27001 auch im gemeinnützigen Sektor sinnvoll ist und wie ein ISMS entsteht, das zu knappen Budgets passt.

Im gemeinnützigen Sektor ist Sicherheit *gelebter Vertrauensschutz*.

DAS WICHTIGSTE IN KÜRZE

ISO/IEC 27001 ist der international führende Standard für Informationssicherheits- Managementsysteme (ISMS). Anders als die DSGVO ist er freiwillig. Für Wohlfahrt und NGOs ist er der strukturierte Nachweis, dass die Daten von Klientinnen und Klienten sowie von Spendern geschützt sind, und damit ein Beleg für das Vertrauen, von dem der ganze Sektor lebt.

Ein ISMS ist dabei kein reines IT-Thema. Es ist ein Satz aus klaren Regeln, Verantwortlichkeiten und Nachweisen, der Sicherheit auch dann trägt, wenn Teams aus Haupt- und Ehrenamtlichen bestehen und über viele Standorte verteilt arbeiten.

Weltweit sind über 70.000 Organisationen nach ISO 27001 zertifiziert, mit deutlich steigender Tendenz. Seit dem 31. Oktober 2025 gilt ausschließlich die Fassung von 2022; die ältere Version :2013 ist mit dem Ende der Übergangsfrist ausgelaufen.

WARUM JETZT HANDELN

Der Druck wächst von mehreren Seiten. Öffentliche Zuwendungsgeber und Kostenträger verlangen in Förderbescheiden und Verträgen zunehmend nachweisbaren

Datenschutz und Informationssicherheit. Große Träger im Gesundheits- und Sozialbereich können zudem unter NIS2 fallen, und konfessionelle Organisationen unterliegen dem kirchlichen Datenschutz nach KDG oder DSG-EKD.

Hinzu kommt die Bedrohungslage. Ransomware trifft soziale Träger hart, weil ihre Dienste, von der Pflege bis zur Beratung, nicht tagelang ausfallen dürfen. Dieses Whitepaper ordnet ein, was die Norm verlangt, welche Risiken bestehen und wie der Weg zur Zertifizierung mit kleinem Budget aussieht.

WOFÜR SICH DER SCHRITT LOHNT

Drei Signale sprechen klar für ISO 27001: Zuwendungsgeber oder Kostenträger fordern Nachweise, Sie verarbeiten Gesundheits- und Sozialdaten in großem Umfang, oder Sie wollen das Vertrauen Ihrer Spender dauerhaft sichern. Trifft eines zu, ist das Zertifikat selten eine Frage des Ob, sondern des Wann.

Die gute Nachricht: Der Standard ist verhältnismäßig. Er schreibt kein Konzern-Schutzniveau vor, sondern eines, das zur Größe und zum Risiko der Organisation passt. Ein schlankes, sauber geführtes ISMS reicht für die Zertifizierung aus.

WELTWEIT ZERTIFIZIERT

70.000+

Organisationen sind nach ISO 27001 zertifiziert, mit klar steigender Tendenz.

AKTUELLE FASSUNG

2022

Seit dem 31.10.2025 zählt allein die Fassung von 2022, die Version von 2013 ist ausgelaufen.

KONTROLLEN

93

Maßnahmen im Annex A, in vier Gruppen von organisatorisch bis technisch.



Der gemeinnützige Sektor lebt *von Vertrauen und Daten.*

Wohlfahrt und NGOs arbeiten mit den Daten von Menschen in verletzlichen Situationen und mit dem Vertrauen ihrer Förderer. Beides ist kostbar und gefährdet. ISO 27001 macht den Schutz dieser Daten nachweisbar, ohne den Auftrag aus dem Blick zu verlieren.

Wer Menschen in Not begleitet, verwaltet ihr Schicksal in Daten. *Dieser Schatz verpflichtet.*

HOCHSENSIBLE DATEN ALS ALLTAG

Soziale Träger verarbeiten Gesundheits-, Sozial- und oft auch religiöse Daten, dazu Angaben zu Kindern, Geflüchteten, Pflegebedürftigen und Menschen in Krisen. Das sind besondere Kategorien nach Art. 9 DSGVO mit höchstem Schutzbedarf. Hinzu kommen Spenderdaten und Bankverbindungen.

Diese Daten liegen zunehmend in digitalen Klienten- und Spendenverwaltungen, oft in der Cloud und über viele Einrichtungen verteilt. Die Digitalisierung verbessert die Arbeit und vergrößert die Angriffsfläche zugleich.

GELDGEBER STELLEN ANFORDERUNGEN

Öffentliche Förderung und Leistungsverträge mit Kostenträgern sind die Finanzierungsbasis vieler Träger. Zuwendungsgeber knüpfen ihre Mittel zunehmend an den Nachweis von Datenschutz und Informationssicherheit, und in Ausschreibungen sozialer Leistungen wird ein ISMS zum Pluspunkt oder zur Bedingung.

ISO 27001 beantwortet einen Großteil dieser Anforderungen mit einem anerkannten Nachweis. Statt jeden Geldgeber einzeln zu überzeugen, legt die Organisation das Zertifikat vor und stärkt zugleich ihre Position im Wettbewerb um Mittel.

GESETZ UND KIRCHLICHES RECHT

Große Träger im Gesundheits- und Sozialbereich können unter NIS2 fallen, etwa wenn sie Krankenhäuser oder Pflegeeinrichtungen betreiben. Konfessionelle Organisationen unterliegen statt der DSGVO dem kirchlichen Datenschutz nach KDG oder DSG-EKD, der inhaltlich vergleichbare Anforderungen stellt. Ein ISMS bündelt all das.

WAS AUF DEM SPIEL STEHT

Vertrauen ist im gemeinnützigen Sektor die wichtigste Währung. Ein Datenvorfall mit Klientendaten beschädigt die Würde der Betroffenen, und ein Vorfall mit Spenderdaten kann die Finanzierung gefährden. Sicherheit schützt hier den Auftrag selbst.



Warum ISO 27001 im NGO-Sektor *besonders fordert.*

Die Anforderungen der Norm gelten unabhängig von der Rechtsform. Der gemeinnützige Sektor bringt aber eigene Bedingungen mit. Fünf Eigenheiten machen die Umsetzung speziell, und für jede gibt es einen pragmatischen Umgang.

KNAPPE MITTEL, KLARER ZWECK

Jeder Euro soll dem Auftrag dienen, nicht der Verwaltung. Ausgaben für Sicherheit stehen damit in direkter Konkurrenz zur eigentlichen Arbeit, und teure Beratung mit langen Projekten passt schlecht zur Mittelverwendung.

Hier hilft die Verhältnismäßigkeit der Norm: Maßnahmen richten sich nach Größe und Risiko, nicht nach Konzernmaßstab. Geführte Werkzeuge halten den externen Aufwand klein und binden das Team nur dort, wo seine Entscheidung nötig ist.

HAUPT- UND EHRENAMT GEMISCHT

Soziale Organisationen arbeiten mit Festangestellten, Ehrenamtlichen, Honorarkräften und Freiwilligendienstleistenden. Die Fluktuation ist hoch, viele haben kurzzeitig Zugriff auf sensible Daten.

Die Norm verlangt geregelte Zugänge, Sensibilisierung und sauberes On- und Offboarding (Annex A 5.18, 6.3, 6.5). Gerade im Ehrenamt sind klare, einfache Regeln und kurze Schulungen der Schlüssel.

DEZENTRALE STANDORTE

Verbände und Träger arbeiten oft an vielen Standorten: Beratungsstellen, Wohngruppen, Kitas, Pflegeeinrichtungen. Jede Stelle hat eigene Geräte und Zugänge, eine zentrale IT-Steuerung fehlt häufig. Das erschwert einheitliche Sicherheit und verlangt klare, übertragbare Vorgaben (Annex A 5.9 bis 5.11).

DÜNNSTE IT-DECKE

Viele Organisationen haben keine eigene IT-Sicherheitsfunktion, oft nicht einmal eine eigene IT-Abteilung. Die Norm verlangt aber Struktur, Dokumentation und Wirksamkeitskontrolle, nicht Heldentaten Einzelner. Werkzeuge, die durch die Anforderungen führen und dokumentieren, ersetzen hier ein Stück weit das fehlende Fachwissen.

DATENSCHUTZ IST BEREITS THEMA

Anders als in manchen Branchen ist der Datenschutz bei sozialen Trägern meist schon verankert, oft mit Datenschutzbeauftragten und Erfahrung aus DSGVO oder kirchlichem Recht. Diese Strukturen lassen sich auf das ISMS übertragen und verkürzen den Weg zur Zertifizierung.



Wo der gemeinnützige Sektor *konkret angreifbar ist.*

Die Risiken sind selten abstrakt. Sie hängen an hochsensiblen Daten, an knappen Ressourcen und an einer dezentralen, oft ehrenamtlich getragenen Struktur. Fünf Szenarien tauchen in der Praxis immer wieder auf.

1 · RANSOMWARE LEGT DIENSTE LAHM

Der häufigste Ernstfall. Werden Klienten- und Verwaltungssysteme verschlüsselt, stehen Pflege, Beratung und Betreuung still, und besonders verletzbare Menschen sind unmittelbar betroffen. Soziale Träger gelten Angreifern als lohnendes, weil schlecht geschütztes Ziel. Getestete Backups und ein eingeübter Notfallplan (Annex A 8.13, 5.29) entscheiden, wie schnell die Dienste zurückkehren.

2 · DIEBSTAHL VON KLIENTENDATEN

Gesundheits-, Sozial- und religiöse Daten besonders schutzbedürftiger Menschen sind hochsensibel. Ein Abfluss verletzt die Würde der Betroffenen, ist ein schwerer Verstoß nach Art. 9 DSGVO und kann Menschen in Gefahr bringen, etwa Geflüchtete oder Betroffene von Gewalt. Verschlüsselung und strenge Zugriffskontrolle (Annex A 8.24, 8.2 bis 8.5) sind hier unverzichtbar.

3 · SPENDERDATEN UND VERTRAUENSVERLUST

Spenderdaten samt Bankverbindungen sind ein attraktives Ziel. Wird das Vertrauen der Förderer

durch einen Vorfall erschüttert, brechen Spenden weg, und die Finanzierung gerät ins Wanken. Schutz der Spendendaten und transparente Sicherheit (Annex A 8.2 bis 8.5, 5.34) sichern die wirtschaftliche Basis.

4 · BETRUG UND CEO-FRAUD

Gefälschte Zahlungsanweisungen und vorgetäuschte Vorstandsmails zielen auf Spenden- und Projektkonten. Gerade in vertrauensvollen, wenig formalisierten Strukturen haben solche Angriffe Erfolg. Klare Freigabeprozesse, Awareness und Mehrfaktor-Anmeldung (Annex A 5.17, 6.3, 8.5) wirken dem entgegen.

5 · DEZENTRALE, OFFENE ZUGÄNGE

Über viele Standorte hinweg sammeln sich geteilte Konten, alte Berechtigungen und ungesicherte Geräte an, besonders bei hoher Fluktuation im Ehrenamt. Jeder vergessene Zugang ist ein Risiko. Rollenbasierte Rechte, sauberes Offboarding und Geräteverwaltung (Annex A 5.15, 5.18, 8.1) schließen diese Lücken.



Was ISO 27001 *konkret verlangt.*

Die Norm besteht aus zwei Teilen: den Management-Anforderungen in den Kapiteln 4 bis 10, die zertifiziert werden, und dem Annex A mit 93 Sicherheitsmaßnahmen, aus denen risikobasiert ausgewählt wird. Fünf Bausteine bilden den Kern.

KONTEXT UND GELTUNGSBEREICH (KAP. 4)

Am Anfang steht die Frage, was geschützt werden soll. Die Organisation bestimmt internen und externen Kontext, die Erwartungen wichtiger Parteien wie Klienten, Spender, Zuwendungsgeber und Aufsicht und legt den Geltungsbereich des ISMS fest (Kap. 4.3).

Im gemeinnützigen Sektor ist der Zuschnitt entscheidend. Ein klarer Scope, etwa die zentrale Klienten- und Spendenverwaltung, hält die Zertifizierung schlank und bezahlbar. Ein zu weit gefasster Geltungsbereich ist der häufigste vermeidbare Fehler.

FÜHRUNG UND POLITIK (KAP. 5)

Die Norm macht Sicherheit zur Leitungsaufgabe. Vorstand und Geschäftsführung verabschieden die Informationssicherheitsleitlinie, stellen Ressourcen bereit und weisen Rollen zu (Kap. 5.1 bis 5.3). Wo bereits ein Datenschutzbeauftragter wirkt, lässt sich daran gut anknüpfen.

RISIKEN UND SOA (KAP. 6)

Das Herzstück. Die Organisation legt eine wiederholbare Methode für die Risikoeinschätzung fest, bewertet ihre Risiken rund um Klienten- und Spenderdaten und

entscheidet je Risiko über die Behandlung (Kap. 6.1.2 und 6.1.3). Das Ergebnis mündet in die Erklärung zur Anwendbarkeit, die für jede der 93 Maßnahmen begründet, ob sie gilt.

Schutz besonderer Datenkategorien, Zugriffskontrolle und Sensibilisierung stehen dabei fast immer oben auf der Liste.

BETRIEB UND MASSNAHMEN (KAP. 8, ANNEX A)

Die ausgewählten Maßnahmen werden umgesetzt und gelebt. Der Annex A gliedert sie in vier Gruppen: 37 organisatorische, 8 personenbezogene, 14 physische und 34 technische Maßnahmen. Im gemeinnützigen Sektor stehen Zugriffskontrolle, Verschlüsselung, Awareness und Backup im Vordergrund.

BEWERTUNG UND VERBESSERUNG (KAP. 9, 10)

Ein ISMS endet nicht mit der Einführung. Internes Audit und Managementbewertung (Kap. 9.2 und 9.3) prüfen regelmäßig die Wirksamkeit, Korrekturmaßnahmen schließen Lücken (Kap. 10.2). Wer Datenschutz bereits dokumentiert, kennt diese Logik und kann sie übertragen.



In sechs Schritten *zum Zertifikat.*

Der Weg zur Zertifizierung lässt sich planen. Diese Reihenfolge baut aufeinander auf und nutzt vorhandene Datenschutzstrukturen, statt bei null zu beginnen. Realistisch sind je nach Reife drei bis sechs Monate bis zum Audit.

Wer den Datenschutz schon dokumentiert, hat das Schwierigste begonnen. *ISO 27001 baut darauf auf.*

1 · GELTUNGSBEREICH FESTLEGEN

Kontext klären und den Scope eng schneiden: welche Verwaltung, welche Systeme, welche Standorte. Ein klarer Geltungsbereich ist die Grundlage für alles Weitere und der wirksamste Hebel, um den Aufwand und die Kosten niedrig zu halten.

2 · FÜHRUNG UND LEITLINIE

Vorstand und Geschäftsführung verabschieden die Sicherheitsleitlinie, benennen eine verantwortliche Person und stellen Ressourcen bereit. Wo ein Datenschutzbeauftragter besteht, lässt sich die Rolle gut verbinden.

3 · RISIKEN ANALYSIEREN

Assets erfassen, von der Klienten- und Spendenverwaltung über genutzte Cloud-Dienste bis zu den Geräten an den Standorten. Risiken bewerten, besondere Datenkategorien gewichten und die Erklärung zur Anwendbarkeit erstellen. Eine gute Analyse macht den Aufwand planbar.

4 · MASSNAHMEN UMSETZEN

Die ausgewählten Annex-A-Maßnahmen einführen und dokumentieren. Mit den wirksamsten und günstigsten Hebeln beginnen: Zugriffskontrolle, Mehrfaktor-Anmeldung, Backup und Awareness für Haupt- und Ehrenamt. Jede Maßnahme so festhalten, dass sie im Audit Bestand hat.

5 · INTERN AUDITIEREN UND BEWERTEN

Vor dem Zertifizierungsaudit prüft ein internes Audit die Wirksamkeit, die Managementbewertung zieht Bilanz. Diese Schleife einmal vollständig zu durchlaufen ist Pflicht und zugleich die beste Generalprobe.

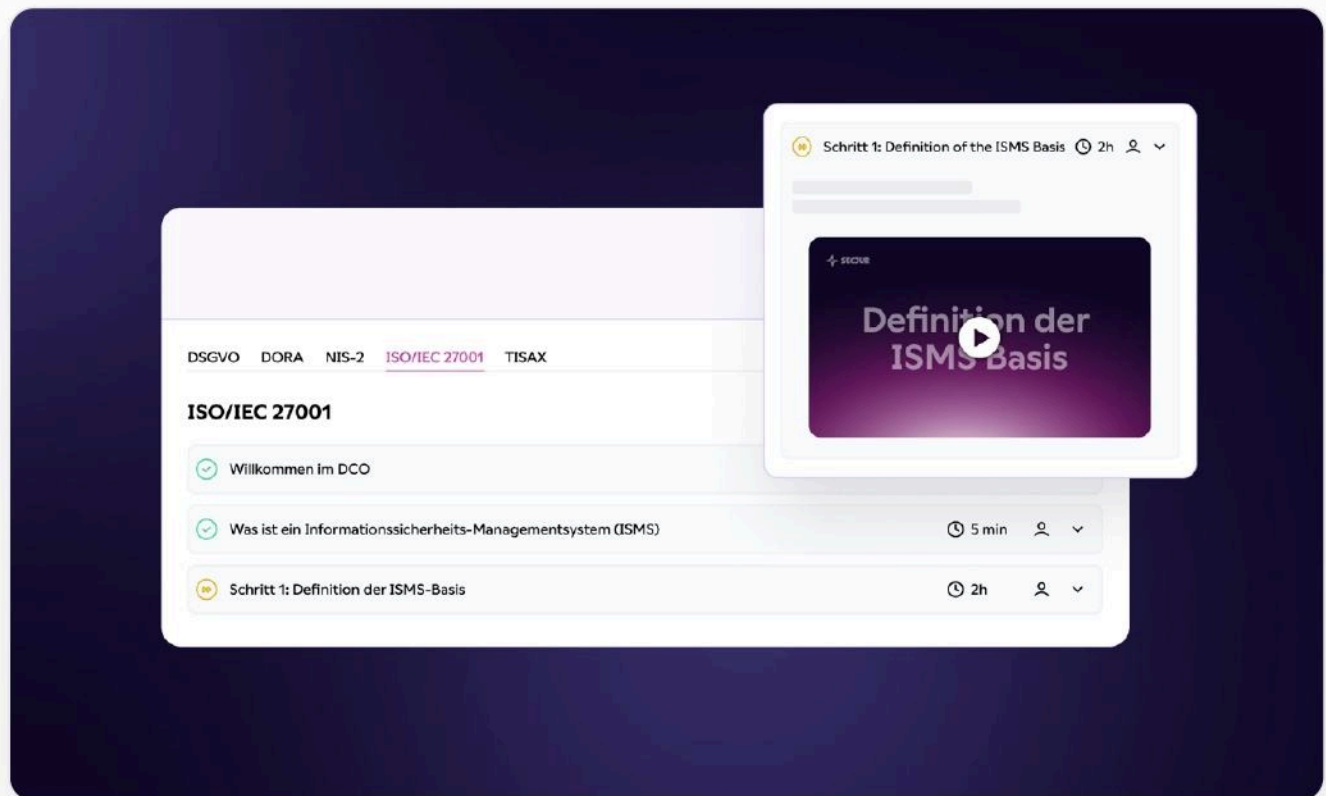
6 · ZERTIFIZIERUNGSAUDIT BESTEHEN

Das externe Audit läuft in zwei Stufen: Dokumentenprüfung (Stage 1) und Wirksamkeitsprüfung (Stage 2). Danach folgt das Zertifikat, gültig für drei Jahre mit jährlichen Überwachungsaudits. Es stärkt zugleich die Position gegenüber Zuwendungsgebern.



Vom Vertrauensauftrag zur *auditbereiten Umsetzung*.

Das Digital Compliance Office (DCO) führt gemeinnützige Organisationen durch die gesamte ISO-27001-Umsetzung: Geltungsbereich, Risikoanalyse, Maßnahmen, interne Audits und Nachweise an einem Ort. Statt teurer Beratung und einem Dutzend Tabellen arbeiten Sie in einer Oberfläche, gehostet in Deutschland und selbst nach ISO 27001 zertifiziert. Organisationen berichten von bis zu 50 Prozent schnellerer Umsetzung gegenüber klassischer Beratung.



Geführter Aufbau

Der Navigator führt Schritt für Schritt durch die Kapitel 4 bis 10, ohne Vorwissen vorauszusetzen, ideal für Teams ohne eigene IT-Sicherheitsfunktion.

Datenschutz & Risiko

Geführte Risikoanalyse mit Fokus auf Klienten- und Spenderdaten, die an vorhandene DSGVO- oder KDG-Strukturen anknüpft.

Nachweise & Geldgeber

Revisionssichere Dokumentation und ein voller Audit-Trail, mit dem Zertifizierungsaudit und Nachweise gegenüber Zuwendungsgebern gelingen.

SO LÄUFT DIE EINFÜHRUNG

Der Einstieg ist schlank und bezahlbar. Sie legen den Geltungsbereich fest, das DCO führt Sie durch jede Anforderung, und wo eine Expertin nötig ist, ist sie zugeschaltet. Sie entscheiden, das System dokumentiert im Hintergrund. So entsteht ein auditbereites ISMS, ohne dass Mittel vom eigentlichen Auftrag abfließen.

AUS DEUTSCHLAND, AN IHRE STRUKTUREN ANSCHLUSSFÄHIG

Alle Daten liegen in Deutschland, der Betrieb ist selbst nach ISO 27001 zertifiziert. Das DCO knüpft an vorhandene Datenschutzarbeit nach DSGVO oder KDG an und deckt, wo nötig, auch NIS2 mit ab. Über 60 Integrationen holen Nachweise automatisch aus Ihren Systemen.

Über 500 Unternehmen *arbeiten mit SECJUR.*

Soziale Träger, Verbände, Stiftungen und digitale Dienstleister erfüllen mit dem DCO ihre regulatorischen Anforderungen mit weniger Aufwand und höherer Geschwindigkeit. Ein Beispiel aus dem gemeinnützigen Sektor:

„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.



REFERENZEN AUS WOHLFAHRT, SOZIALEN TRÄGERN UND NGOS



Der Kinderschutzbund



Deutsches
Rotes
Kreuz



AUDIT-ERFOLG

100%

Erfolgsquote in bisherigen Zertifizierungsaudits.

SCHNELLER

50%

Weniger Aufwand gegenüber klassischer Beratung.

INTEGRATIONEN

60+

Native API-Anbindungen, von Microsoft 365 bis JIRA.

STANDARDS

10+

Frameworks parallel abgedeckt, ohne Doppelarbeit.

WARUM GEMEINNÜTZIGE ORGANISATIONEN SECJUR WÄHLEN

Der Reiz liegt in der Geschwindigkeit und in den geringen Kosten. Statt teurer Beratung führt ein klarer Pfad durch jede Anforderung der Norm, mit Vorlagen, die zur Größe der Organisation passen. Das Team bleibt beim Auftrag, das ISMS entsteht parallel.

Nachweise entstehen dabei ohne zusätzliche Personaldecke. Über native Integrationen zieht das DCO Belege automatisch aus den bestehenden Systemen, sodass haupt- und ehrenamtlich Tätige an einer Quelle arbeiten statt an parallelen Tabellen.

MEHR ALS EIN ZERTIFIKAT

Am Ende steht nicht nur das Zertifikat an der Wand, sondern eine Organisation, die die Daten ihrer Klienten und Spender schützt und gegenüber Geldgebern souverän auftritt. Genau das sichert Vertrauen und Förderung.

Weil dieselbe Struktur die DSGVO-Pflichten und die ISO-27001-Anforderungen gemeinsam bedient, deckt ein Projekt mehrere Anforderungen ab. Das senkt den Aufwand und hält die Organisation auch nach dem Audit jederzeit nachweisfähig.

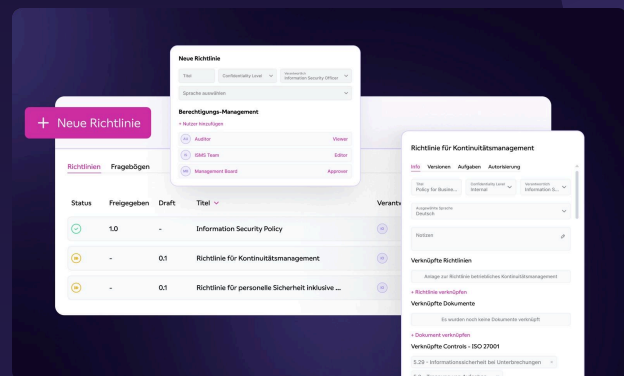
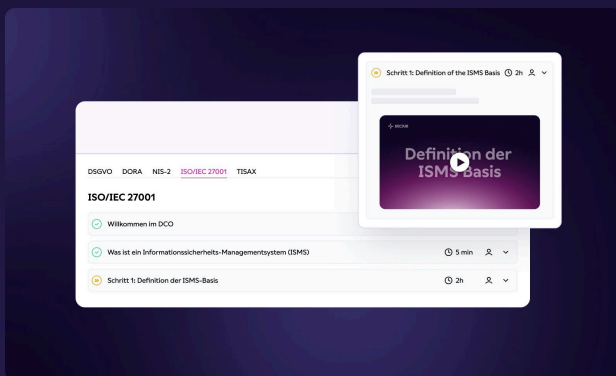


Wie SECJUR die ISO/IEC 27001 zum Kinderspiel macht

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



Der Kinderschutzbund



Deutsches
Rotes
Kreuz

**CHANGING
CITIES**

www.secjur.com