SECJUR

WHITEPAPER
2026

NIS2 & DATENSCHUTZ · WOHLFAHRT, SOZIALE TRÄGER & NGOS

NIS2 & Datenschutz für Wohlfahrt & NGOs: 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. Große Träger im Gesundheits- und Sozialbereich fallen unter NIS2, für alle gelten die besonderen Datenkategorien nach Art. 9 DSGVO und, bei konfessionellen Trägern, der kirchliche Datenschutz. Dieses Whitepaper zeigt, wer wann betroffen ist, welche Risiken bestehen und wie ein ISMS entsteht, das zu knappen Budgets passt.

NIS2 | DSGVO | ISO 27001 | KDG | DSG-EKD

MADE & HOSTED
IN GERMANY

MANAGEMENT SUMMARY

Im gemeinnützigen Sektor ist Sicherheit gelebter Vertrauensschutz.

DAS WICHTIGSTE IN KÜRZE

Zwei Kräfte prägen die Informationssicherheit im gemeinnützigen Sektor. Das NIS2-Umsetzungsgesetz gilt seit dem 6. Dezember 2025 und erfasst große Träger im Gesundheits- und Sozialbereich, etwa wenn sie Krankenhäuser oder Pflegeeinrichtungen betreiben. Parallel gilt für alle der Datenschutz.

Klienten- und Spenderdaten sind besondere Kategorien nach Art. 9 DSGVO mit höchstem Schutzbedarf, konfessionelle Organisationen unterliegen statt der DSGVO dem kirchlichen Datenschutz nach KDG oder DSG-EKD. Reine Advocacy-NGOs fallen selten direkt unter NIS2, werden aber über Geldgeber und die Lieferkette regulierter Auftraggeber gebunden. Ein ISMS nach ISO 27001 deckt diese Anforderungen gemeinsam ab. Wer die Betroffenheit sauber dokumentiert, schafft Klarheit und schützt die Leitung im Zweifel vor Haftung.

WARUM JETZT HANDELN

Der Druck wächst von mehreren Seiten. Öffentliche Zuwendungsgeber und Kostenträger verlangen in Förderbescheiden und Verträgen zunehmend nachweisbaren Datenschutz und Informationssicherheit. Für betroffene Träger endete zudem die BSI-Registrierungsfrist am 31. Juli 2026.

Hinzu kommt die Bedrohungslage. Ransomware trifft soziale Träger hart, weil ihre Dienste, von der Pflege bis zur Beratung, nicht tagelang ausfallen dürfen und die Einrichtungen oft schlecht geschützt sind. Ein Vorfall trifft hier nicht nur die IT, sondern die Würde der Betroffenen und das Vertrauen der Spender. Wer den Nachweis früh aufbaut, begegnet Geldgebern und Aufsicht aus einer Position der Stärke.

EIN AUFBAU, MEHRERE PFLICHTEN

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 einmal aufgebautes ISMS trägt NIS2, DSGVO und den kirchlichen Datenschutz zugleich, auch wenn Teams aus Haupt- und Ehrenamtlichen bestehen und über viele Standorte verteilt arbeiten.

Die folgenden Seiten liefern die Grundlage: den Sektorkontext, die konkreten Risiken rund um Klienten- und Spenderdaten, die Pflichten und eine Roadmap, die mit kleinem Budget funktioniert. So bleibt jeder Euro beim Auftrag, statt in Doppelarbeit zu versickern. Ein klar benannter Verantwortlicher gibt dem Thema zudem ein Gesicht in der Organisation.

BETROFFEN

NIS2

Große Träger über Gesundheits- und Pflegeeinrichtungen sowie über die Lieferkette.

DATENKATEGORIE

Art. 9 DSGVO

Klienten- und Sozialdaten mit höchstem Schutzbedarf, bei Kirchen KDG oder DSG-EKD.

VERHÄLTNISMÄSSIG

1 Aufbau

Ein ISMS deckt NIS2, DSGVO und kirchlichen Datenschutz gemeinsam ab.

BRANCHENKONTEXT

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. Ein ISMS 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. Schon ein Überblick über die genutzten Cloud-Dienste zeigt, wo der Schutz zuerst greifen muss.

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.

Ein ISMS beantwortet einen Großteil dieser Anforderungen mit einem anerkannten Nachweis. Statt jeden Geldgeber einzeln zu überzeugen, legt die Organisation das Zertifikat vor und stärkt 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 in einem System.

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. Ein belastbarer Nachweis sichert das Vertrauen von Klienten, Spendern und Geldgebern und damit die Existenzgrundlage der Organisation.

HERAUSFORDERUNGEN

Warum die Umsetzung im NGO-Sektor besonders fordert.

Die Anforderungen gelten unabhängig von der Rechtsform. Der gemeinnützige Sektor bringt aber eigene Bedingungen mit. Sechs 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 in direkter Konkurrenz zur eigentlichen Arbeit, und teure Beratung mit langen Projekten passt schlecht zur Mittelverwendung. Hier hilft die Verhältnismäßigkeit: Maßnahmen richten sich nach Größe und Risiko, nicht nach Konzernmaßstab. Geführte Werkzeuge halten den externen Aufwand klein. So bleibt die Investition überschaubar und der Nutzen, vermiedene Ausfälle und gesicherte Förderung, messbar.

HAUPT- UND EHRENAMT GEMISCHT

Soziale Organisationen arbeiten mit Festangestellten, Ehrenamtlichen, Honorarkräften und Freiwilligendienstleistenden. Die Fluktuation ist hoch, viele haben kurzzeitig Zugriff auf sensible Daten. NIS2 und die Norm verlangen geregelte Zugänge, Sensibilisierung und sauberes On- und Offboarding. 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. Einheitliche, einfache Vorgaben verhindern, dass jede Stelle eigene Wege geht.

DÜNNSTE IT-DECKE

Viele Organisationen haben keine eigene IT-Sicherheitsfunktion, oft nicht einmal eine eigene IT-Abteilung. NIS2 und die Norm verlangen 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 Konformität spürbar.

SELEKTIVE BETROFFENHEIT KLÄREN

Nicht jede Organisation fällt unter NIS2. Eine saubere, dokumentierte Prüfung schafft Klarheit: Betreibt der Träger meldepflichtige Einrichtungen, beliefert er regulierte Auftraggeber, erreicht er die Schwellen? Wer das früh klärt, vermeidet Überregulierung und kann die Mittel gezielt einsetzen.

BEDROHUNGSLAGE & RISIKEN

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 verletzliche Menschen sind unmittelbar betroffen. Soziale Träger gelten Angreifern als lohnendes, weil schlecht geschütztes Ziel. Getestete Backups und ein eingeübter Notfallplan entscheiden, wie schnell die Dienste zurückkehren. Wer den Ernstfall nie geübt hat, verliert im Angriff die wertvollste Zeit. Ein aktueller Notfallplan legt vorab fest, wer im Stillstand was entscheidet.

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 sind hier unverzichtbar. Wer weiß, wo die sensibelsten Daten liegen, kann sie zuerst und am stärksten schützen. Eine Protokollierung der Zugriffe macht ungewöhnliche Muster früh sichtbar.

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 sichern die wirtschaftliche Basis. Eine transparente Kommunikation im Ernstfall hält den Schaden für das Vertrauen klein. Ein zweiter, getrennter Datenstand sichert die Spendenverwaltung zusätzlich ab. Wer offen über seine Sicherheitsmaßnahmen berichtet, stärkt das Vertrauen sogar.

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 wirken dem entgegen. Zahlungen sollten nie allein auf Zuruf freigegeben werden, gerade in kleinen Teams. Eine kurze Sensibilisierung für typische Betrugsmaschen schützt gerade neue Ehrenamtliche.

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 schließen diese Lücken. Ein fester Rhythmus zur Rechteprüfung räumt verwaiste Konten zuverlässig aus. Eine einfache Geräteverwaltung sorgt dafür, dass kein Standort vergessen wird.

REGULATORISCHE PFLICHTEN

Was NIS2 und der Datenschutz konkret verlangen.

Zwei Rahmen, ein Kern. NIS2 gilt für betroffene Träger, der Datenschutz nach Art. 9 DSGVO und kirchlichem Recht für alle. Fünf Bausteine muss jede Organisation kennen: Betroffenheit (§28), Risikomanagement (§30), Meldepflichten (§32), Leitungspflichten (§38) und Sanktionen (§65).

§28 · BETROFFENHEIT UND REGISTRIERUNG

Ob eine Organisation unter NIS2 fällt, hängt von Tätigkeit und Größe ab. Träger, die Krankenhäuser oder Pflegeeinrichtungen betreiben, zählen zum Gesundheitssektor und sind ab den Schwellen erfasst, häufig als besonders wichtige Einrichtungen. Wer betroffen ist, registriert sich über das Unternehmenskonto und das BSI-Portal. Alle übrigen bleiben den Datenschutzpflichten verpflichtet. Im Zweifel schafft eine kurze Prüfung Klarheit. Wer die Prüfung dokumentiert, kann Überregulierung ebenso vermeiden wie Versäumnisse.

§30 · DIE TECHNISCHEN UND ORGANISATORISCHEN MASSNAHMEN

Verlangt werden angemessene Maßnahmen: Risikoanalyse, Vorfallbehandlung, Backup und Notfallplan, Lieferkettensicherheit, Zugriffskontrolle, Kryptografie und Multifaktor-Authentifizierung. Dieselben Maßnahmen erfüllen zugleich die technisch-organisatorischen Pflichten aus DSGVO und kirchlichem Datenschutz. Wer den Datenschutz bereits dokumentiert, bringt vieles mit. Entscheidend ist, dass jede Maßnahme nicht nur existiert, sondern nachweisbar gelebt und regelmäßig überprüft wird.

§32 · MELDEFRISTEN

Für betroffene Träger gilt eine gestufte Meldepflicht an das BSI: Frühwarnung binnen 24 Stunden, Meldung binnen 72 Stunden, Abschlussbericht binnen eines Monats. Parallel greift bei Datenpannen die 72-Stunden-Meldung an die Datenschutzaufsicht. Nur ein vorab geübter Prozess hält diese Fristen. Ein vorbereitetes Meldeformular und klare Zuständigkeiten sparen im Ernstfall wertvolle Minuten.

§38 · LEITUNG TRÄGT DIE VERANTWORTUNG

Vorstand und Geschäftsführung müssen die Maßnahmen billigen, ihre Umsetzung überwachen und sich schulen lassen. Die Verantwortung ist nicht delegierbar, auch nicht an den externen IT-Dienstleister. Wo bereits ein Datenschutzbeauftragter wirkt, lässt sich daran gut anknüpfen. Das dokumentierte Engagement ist im Ernstfall ein Nachweis gelebter Sorgfalt. Regelmäßige, kurze Schulungen von Vorstand und Leitung sind ausdrücklich Teil dieser Pflicht.

§65 · SANKTIONEN UND VERHÄLTNISMÄSSIGKEIT

Für betroffene Einrichtungen drohen unter NIS2 empfindliche Bußgelder, für Datenschutzverstöße nach Art. 9 DSGVO ebenso. Schwerer wiegt hier oft der Verlust von Vertrauen und Förderung. Zugleich gilt die Verhältnismäßigkeit: geschuldet ist ein Schutzniveau, das zu Größe und Risiko passt. Ein dokumentierter, gelebter Prozess ist im Prüffall die beste Verteidigung. Wer Lücken kennt und plant, wird selbst bei einem Vorfall milder bewertet als eine untätige Organisation.

UMSETZUNG IN DER PRAXIS

In sechs Schritten mit Augenmaß und kleinem Budget.

Die Umsetzung lässt sich planen. Diese Reihenfolge baut aufeinander auf und nutzt vorhandene Datenschutzstrukturen, statt bei null zu beginnen. Realistisch führt der Weg in wenigen Monaten zu einem auditbereiten Stand.

Wer den Datenschutz schon dokumentiert, hat das Schwierigste begonnen. *NIS2 und ISO 27001 bauen darauf auf.*

1 · BETROFFENHEIT UND GELTUNGSBEREICH

Prüfen, ob und über welche Einrichtungen die Organisation unter NIS2 fällt, 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 Aufwand und 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. Betroffene Träger nehmen zusätzlich die Registrierung beim BSI vor.

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. Eine gute Analyse trennt das Wichtige vom Nebensächlichen.

4 · MASSNAHMEN UMSETZEN

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. Klare, einfache Vorgaben wirken über alle Standorte hinweg. Zentrale Vorgaben wirken sofort über alle Standorte hinweg.

5 · MELDE- UND NOTFALLPROZESS

Die Meldeketten für NIS2 und für Datenpannen einrichten, Zuständigkeiten klären und den Notfallplan testen. Im Ernstfall zählt jede Stunde, und nur geübte Abläufe halten die Fristen und die Dienste. Eine kurze Übung pro Jahr zeigt, wo es noch hakt.

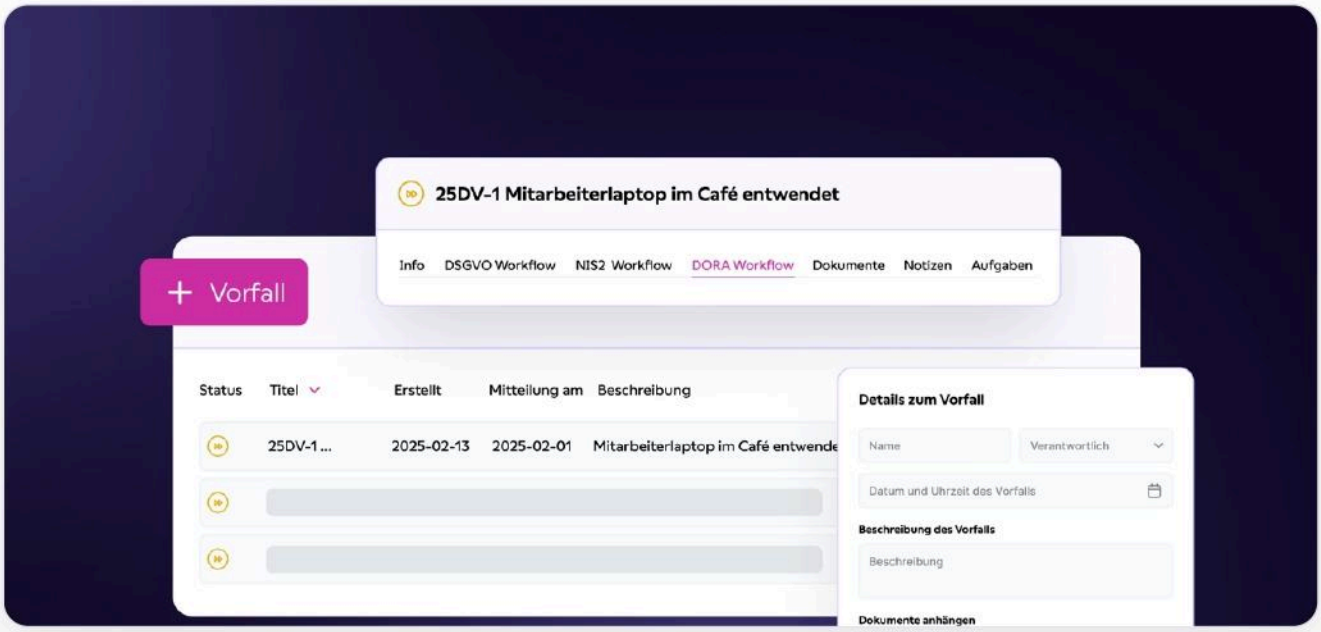
6 · PRÜFEN, NACHWEISEN, VERBESSERN

Internes Audit und Managementbewertung prüfen die Wirksamkeit, Korrekturmaßnahmen schließen Lücken. Wer den Datenschutz bereits dokumentiert, kennt diese Logik. Wer die Schleife einmal vollständig durchläuft, ist zugleich reif für die ISO-27001-Zertifizierung und stärkt die Position gegenüber Zuwendungsgebern. Der Aufwand von heute trägt so gleich mehrere Nachweise von morgen.

WIE SECJUR ES EINFACH MACHT

Vom Pflichtenrahmen zur auditbereiten Umsetzung.

Das Digital Compliance Office (DCO) führt gemeinnützige Organisationen durch NIS2, DSGVO und den kirchlichen Datenschutz zugleich: Risiken, Maßnahmen, Meldeprozess und Nachweise an einem Ort, mehrere Frameworks parallel. Statt teurer Beratung arbeiten Sie in einer Oberfläche, gehostet in Deutschland und selbst nach ISO 27001 zertifiziert. Teams berichten von bis zu 50 Prozent schnellerer Umsetzung gegenüber klassischer Beratung.



Klienten- & Spenderdaten

Module für Zugriffskontrolle, Verschlüsselung und den Schutz besonderer Datenkategorien nach Art. 9 DSGVO und kirchlichem Recht.

Haupt- & Ehrenamt

Awareness, geregelte Zugänge und sauberes Offboarding, die auch bei hoher Fluktuation und über viele Standorte hinweg tragen.

Mehrere Pflichten

NIS2, DSGVO, KDG/DSG-EKD und ISO 27001 laufen auf einem ISMS, gemeinsame Maßnahmen werden nur einmal gepflegt statt mehrfach.

SO LÄUFT DIE EINFÜHRUNG

Der Einstieg ist schlank und günstig. Sie legen den Geltungsbereich fest, das DCO führt durch jede Anforderung, und wo eine Expertin nötig ist, schalten wir sie zu. Sie entscheiden, das System dokumentiert im Hintergrund. So entsteht ein auditbereiter Nachweis in Wochen statt in Quartalen, ohne den Auftrag zu bremsen.

Konkret beginnt es mit einer geführten Aufnahme. Das DCO fragt Betroffenheit, Assets und bestehende Datenschutzmaßnahmen ab und leitet daraus die offenen Punkte ab. Jeder Schritt ist mit einer Vorlage hinterlegt, sodass niemand vor einem leeren Blatt sitzt.

Wo es schnell gehen muss, arbeitet das Team die wirksamsten Maßnahmen zuerst ab und verteilt den Rest planbar. Der Fortschritt bleibt jederzeit sichtbar, für Haupt- und Ehrenamt.

EIN FUNDAMENT, MEHRERE NACHWEISE

Weil sich NIS2, DSGVO, kirchlicher Datenschutz und ISO 27001 weitgehend überschneiden, deckt das DCO sie gemeinsam ab. Über 60 Integrationen holen Nachweise automatisch aus Ihren Systemen, sodass haupt- und ehrenamtlich Tätige an einer Quelle arbeiten statt an parallelen Tabellen.

Für eine Organisation heißt das weniger Doppelarbeit. Der Datenschutznachweis und, wo nötig, der NIS2-Nachweis entstehen aus demselben Aufbau, statt in getrennten Projekten.

Und weil die Belege aktuell bleiben, ist die Organisation für die nächste Prüfung durch Zuwendungsgeber oder Aufsicht vorbereitet, ohne kurzfristig Unterlagen zusammensuchen zu müssen. Aus einer Pflicht wird so ein dauerhafter Vertrauensbeweis.

VERTRAUEN & ERGEBNISSE

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 alleine kaum zu stemmen, auch weil ein Großteil der Arbeit im Ehrenamt geschieht. Durch die Zusammenarbeit mit SECJUR können wir uns auf *das Wesentliche konzentrieren.*"

Paul Jäde
Vorstand, Changing Cities e.V.

CHANGING CITIES

REFERENZEN AUS WOHLFAHRT, SOZIALEN TRÄGERN UND NGOS

Pestalozzi Stiftung · Der Kinderschutzbund · PARTNER DRK Service | Deutsches Rotes Kreuz · CHANGING CITIES

AUDIT-ERFOLG
100%
Erfolgsquote in bisherigen Zertifizierungsaudits.

ZEITERSPARNIS
50%
Weniger Aufwand gegenüber klassischer Beratung.

INTEGRATIONEN
60+
Native API-Anbindungen, von Microsoft 365 bis GitHub.

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, 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.

Wo Fachwissen fehlt, schalten sich Expertinnen und Experten gezielt zu, statt ein dauerhaftes Beratungsmandat zu verlangen. Das hält die Kosten im Rahmen und die Kontrolle im Haus, gerade bei kleinen Trägern.

Und die Plattform denkt in der Realität des gemeinnützigen Alltags und priorisiert die Maßnahmen mit der größten Wirkung.

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.

Ein gelebtes ISMS macht Sicherheit vom Prüfthema zum Vertrauensbeweis. Nachweise gegenüber Zuwendungsgebern sind schneller erbracht, Aufsichtsfragen verlieren ihren Schrecken, und Spender sehen belegt, dass ihre Daten sicher sind.

Weil dieselbe Struktur die DSGVO-Pflichten, den kirchlichen Datenschutz und die NIS2-Anforderungen gemeinsam bedient, deckt ein Projekt mehrere Anforderungen ab. Das senkt den Aufwand und hält die Organisation auch nach dem Audit jederzeit nachweisfähig.

So wird aus einer Pflicht ein dauerhafter Schutz von Würde, Vertrauen und Förderung.

SECJUR

Mit SECJUR zu 100 % NIS2-Compliance

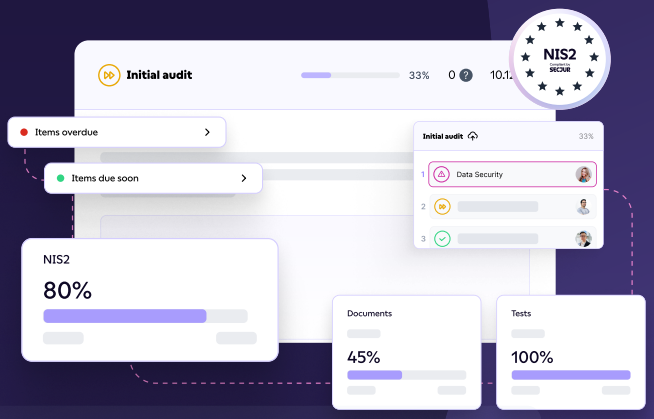
Mit der Durchsetzung der NIS2-Richtlinie in 2026 rücken zehntausende Unternehmen neu in den regulatorischen Fokus. Die Anforderungen an Informationssicherheit, Risikomanagement und Managementverantwortung steigen spürbar – ebenso wie die Erwartungen von Aufsichtsbehörden und Geschäftspartnern.

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