

Praxis-Leitfaden: Datenschutzaudit richtig selbst durchführen.

**9 Tipps, wie Sie die Übersicht über Ihren
Datenschutz zurückgewinnen.**

KUNDEN, DIE UNS BEREITS VERTRAUEN:



CLARK



Herzlich Willkommen!

Schön, dass Sie sich unseren Praxisleitfaden „**Datenschutzaudit richtig selbst durchführen**“ heruntergeladen haben.

Ich habe ihn für Sie erstellt, um Ihnen dabei zu helfen, den Überblick und die Kontrolle über Ihren Datenschutz zurückzuerlangen.

Der Leitfaden enthält **9 wichtige Punkte**, die Sie bei der Durchführung eines internen Datenschutzaudits beachten sollten.

Ein Datenschutzaudit ist ein wesentliches Instrument, um die Datenschutzkonformität eines Unternehmens zu bewerten und zu verbessern. Es hilft, Risiken frühzeitig zu erkennen, Prozesse zu optimieren und gesetzliche Anforderungen zu erfüllen.

Dieser Leitfaden bietet eine **praxisnahe Schritt-für-Schritt-Anleitung** zur Durchführung eines strukturierten Datenschutzaudits.

Ich wünsche Ihnen viel Freude und Erfolg bei der Umsetzung.

Jacqueline Neiazy

Partnerin Datenschutz & Geschäftsführerin



Ich durfte bereits unzählige Datenschutzaudits für Unternehmen aller Größen durchführen und unterstütze viele Betriebe als externe Datenschutzbeauftragte. Deshalb weiß ich genau, welche Herausforderungen bei Datenschutzaudits entstehen und worauf es bei der effizienten Durchführung ankommt. Außerdem beobachte ich häufig, dass Datenschutz-Verantwortliche Schwierigkeiten haben, die Übersicht und Kontrolle über die Datenschutz-Infrastruktur zu behalten. Dieser Leitfaden soll Ihnen dabei helfen, einen Selbstcheck in Ihrem Unternehmen durchzuführen.

Schritt 1: Vorbereitung auf das Audit

TIPP 1: ZIEL DES AUDITS FESTLEGEN

Bevor das Audit startet, muss geklärt werden, welches Ziel erreicht werden soll. Mögliche Audit-Typen, z. B. (nicht abschließend):

- Reifegradmessung: Analyse des aktuellen Datenschutzmanagementsystems (DSMS) und Bewertung des Reifegrads
- Gesamtheitliches Audit: Gesamtbewertung der Datenschutzkonformität des Unternehmens

TIPP 2: KICK-OFF TERMIN MIT FACH-VERANTWORTLICHEN

Im ersten Meeting werden die Fachverantwortlichen der betroffenen Abteilungen über den Ablauf informiert. Hierbei geht es insbesondere um:

- Klärung des Audit-Ziels
- Abstimmung der Interviewtermine mit den relevanten Fachabteilungen

Praxistipp: Bereiten Sie eine prägnante Agenda für den Kick-Off vor, um eine effiziente und zielgerichtete Besprechung sicherzustellen.

TIPP 3: SICHTUNG BESTEHENDER DOKUMENTATIONEN

Zur optimalen Vorbereitung sollten bereits vorhandene Verarbeitungsverzeichnisse (VVT) oder andere Datenschutzdokumentationen gesichtet werden. Dies erleichtert die strukturierte Befragung und spart Zeit.

Praxistipp: Nutzen Sie bestehende Unterlagen, insbesondere VVTs, als Basis für gezielte Fragen in den Interviews. Dies hilft, Redundanzen zu vermeiden und gezielt Schwachstellen zu identifizieren.

Schritt 2: Durchführung der Interviews

TIPP 4: ZIELE DER INTERVIEWS

- Erfassen der Ist-Situation hinsichtlich der Datenschutz-Infrastruktur und Datenflüssen
- Identifikation relevanter Prozesse und Prüfung der Konformität
- Lückenanalyse in bestehenden Datenschutzprozessen

TIPP 5: INTERVIEWABLAUF

- Falls bereits Dokumente vorliegen: Gezielte Fragen zu den Inhalten, Überprüfung auf Aktualität und Vollständigkeit
- Falls keine Dokumentation vorhanden ist: Erfassen und Dokumentieren aller relevanten Prozesse mit Hilfe der Fachabteilungen

Praxistipp: Lassen Sie sich von den Fachabteilungen durch eine Kunden- oder Mitarbeiter-Journey führen. So bekommen Sie einen realistischen Einblick in die Prozesse. Simulieren Sie Anfragen und Vorfälle, um Schwachstellen in der Reaktionsfähigkeit zu erkennen.

Schritt 3: Audit-Findings und Berichterstellung

TIPP 6: SOLL-IST-VERGLEICH

Nach den Interviews erfolgt der Abgleich des IST-Zustands mit den datenschutzrechtlichen Anforderungen:

- Definition des Soll-Zustands anhand gesetzlicher Vorgaben und Best Practices.
- Vergleich mit den ermittelten Audit-Ergebnissen.
- Festhalten von Abweichungen und potenziellen Risiken

TIPP 7: DOKUMENTATION UND PRIORISIERUNG

- Dokumentation der Findings im Audit-Bericht
- Falls Prozesse konform sind: Bestätigung der Einhaltung
- Falls Verbesserungspotential besteht: Empfehlung konkreter Maßnahmen
- Falls Verstöße identifiziert werden: Eskalation & Festlegung eines Aktionsplans
- Risikobewertung und Priorisierung der Findings

Praxistipp: Nutzen Sie eine Priorisierungsmatrix, um die identifizierten Risiken nach Dringlichkeit und Auswirkungen zu bewerten und Handlungsbedarfe klar zu kommunizieren.

Schritt 4: Nachbereitung und Schulungen

TIPP 8: NACHBEREITUNG DES AUDITS

- Maßnahmenplan erstellen: Klärung der Zuständigkeiten und Fristen für die Umsetzung der empfohlenen Maßnahmen
- Follow-up-Termine festlegen: Regelmäßige Überprüfung der Fortschritte und gegebenenfalls Anpassung der Maßnahmen
- Dokumentation der Umsetzung: Nachweise über Verbesserungen sammeln, um Compliance gegenüber Aufsichtsbehörden belegen zu können
- Lückenanalyse in bestehenden Datenschutzprozessen

TIPP 9: SCHULUNG UND SENSIBILISIERUNG

- Schulung der Mitarbeitenden basierend auf den Audit-Ergebnissen, um das Datenschutzbewusstsein zu stärken
- Erstellung von Richtlinien und Leitfäden für betroffene Abteilungen, sofern erforderlich

Praxistipp: Integrieren Sie Datenschutz in bestehende Schulungsprogramme, um kontinuierliche Awareness zu gewährleisten. Nutzen Sie das Audit auch als Awareness-Maßnahme.

CHECKLISTE

Wann muss ein Datenschutzaudit durchgeführt werden?

In folgenden Fällen ist ein Audit besonders empfehlenswert:

- ✓ Zweifel an der Effektivität des Datenschutzmanagementsystems, durchgeführter Datenschutz-Folgenabschätzungen, Prozesse zum Umgang mit Betroffenenanfragen und an gelegter Verzeichnisse von Verarbeitungstätigkeiten
- ✓ Keine spezifischen Datenschutzmaßnahmen für einzelne Unternehmensbereiche wie IT, Marketing, Vertrieb, HR
- ✓ Umfangreiche Auftragsverarbeitungsverträge
- ✓ Gefahren für die IT-Sicherheit, drohende oder mögliche Hackerangriffe
- ✓ Zweifel an ausreichenden Sicherheitsvorkehrungen für Server und Büros

Über ISiCO

Datenschutz und IT-Sicherheit sind mehr als nur Compliance – sie sind der Schlüssel zu nachhaltigem Unternehmenserfolg. Seit 2011 unterstützen wir Unternehmen aus allen Branchen dabei, Datenschutz, Informationssicherheit und Datenstrategie ganzheitlich und wirtschaftlich sinnvoll zu gestalten. Mit tiefgehendem Fachwissen, strategischer Beratung und einem klaren Verständnis für digitale Geschäftsmodelle entwickeln wir Lösungen, die praxisnah und zukunftssicher sind.

Unser Ansatz: Als eine der führenden Unternehmensberatungen in Deutschland bieten wir Unternehmen jeder Größe maßgeschneiderte Strategien und begleiten sie als externe Datenschutz- und Informationssicherheitsbeauftragte. Namhafte Unternehmen, internationale Verbände und Institutionen aus stark regulierten Branchen vertrauen auf unsere Expertise.

Wir beraten nicht nach Standard, sondern mit Augenmaß und fachlicher Exzellenz – immer maßgeschneidert auf Ihre Ziele optimiert. Wir bieten Ihnen praxisorientierten Schutz, der Ihr Unternehmen für die Zukunft stärkt und gleichzeitig Risiken minimiert.

Unser Ziel: Unternehmen langfristig schützen und wirtschaftlichen Erfolg sichern.

Warum ISiCO?

- Führende Beratung in Datenschutz & IT-Sicherheit
- Nur praxisnahe & wirtschaftlich sinnvolle Lösungen
- Tiefes Branchenverständnis & strategische Weitsicht
- Expertise für digitale Geschäftsmodelle & neue Technologien
- **BONUS:** Mit caralegal eine starke Software-Lösung für effizientes Datenschutzmanagement

Sie kommen nicht weiter?

**Vereinbaren Sie Ihren kostenfreien
30-Minuten-Schnell-Check mit mir.**

Nutzen Sie die Gelegenheit, ohne großen Aufwand und Verpflichtung herauszufinden, wie Sie die Kontrolle im Datenschutz zurückgewinnen können.



JACQUELINE NEIAZY

Partnerin Datenschutz & Geschäftsführerin

Anfrage Datenschutzaudit-Schnell-Check ▶

T +49 (0)30 21 30 028-0

E neiazy@isico.de