

Datenschutzaudit: Diese Bereiche stehen auf dem Prüfstand





Mit einem Datenschutzaudit können Sie Ihre Datenschutzkonformität einer freiwilligen Prüfung unterziehen, um eine DSGVO-Zertifizierung vorzubereiten. Grundlage der Zertifizierung ist Art. 42 DSGVO. Unsere Checkliste hilft Ihnen dabei, sich einen Überblick über den Stand Ihres Datenschutzes zu verschaffen, um sich besser auf das Audit vorbereiten zu können und Datenschutzlücken zu identifizieren.



Hintergrund dieser Checkliste

Die Auditierung führen unabhängige Prüfer und Gutachter durch. Ihr wichtigstes Instrument neben Interviews und Vor-Ort-Prüfungen ist ein Fragenkatalog rund um den Datenschutz im zu prüfenden Unternehmen. Damit Sie sich bestmöglich auf den Zertifizierungsprozess vorbereiten können, stellen wir Ihnen in dieser Checkliste wichtige Teile des Fragenkatalogs für den Datenschutzaudit vor.

Wichtig: Bei dieser unvollständigen Checkliste handelt es sich lediglich um einen Einblick in den Fragebogen. Der Zweck dieser Übersicht ist es, Ihnen zu zeigen, welche Fragen bei einem Audit auf sie zukommen können. Diese Checkliste dient lediglich zur Orientierung, damit Sie sich auf ein Audit vorbereiten können.



Lesetipp:

Mehr zum Thema Datenschutzaudit erfahren Sie in unserem Online-Magazin.



1. Vorbereitung und Planung

- ☐ **Zuständigkeit festlegen:** Gibt es einen internen oder externen Datenschutzbeauftragten?
- ☐ **Audit-Team zusammenstellen:** Wer übernimmt die Analyse und Berichterstattung?

Wichtige Informationen, die Sie benötigen:

- ☐ Organigramm des Unternehmens oder der Unternehmensgruppe
- ☐ Übersicht über Produkte oder Dienstleistungen, die Ihr Unternehmen erbringt
- ☐ Übersicht über sämtliche Standorte des Unternehmens und Standorte, an denen Datenverarbeitungen stattfinden – wichtig: Befinden sich Standorte des Unternehmens außerhalb der EU oder des Europäischen Wirtschaftsraumes („EWR“)?

2. Datenschutzdokumentation

Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO prüfen:

- ☐ Ist es aktuell und vollständig?
- ☐ Wie ist das Verzeichnis dokumentiert?

Informationen über die Zusammenarbeit mit Partnern:

- ☐ Haben Sie eine Liste aller Dienstleister, die für Sie im Rahmen einer Auftragsverarbeitung tätig sind?
- ☐ Falls die Liste der Auftragsverarbeiter unvollständig ist oder nicht existiert, haben Sie eine Liste der Unternehmen und Dienstleister, die für Sie Datenverarbeitungen vornehmen?
- ☐ Ist das Unternehmen auf das Erfordernis einer Datenschutz-Folgenabschätzung vorbereitet?
- ☐ Wurde ein Datenschutzmanagementsystem installiert, um sicherzustellen und nachweisen zu können, dass die Verarbeitung gemäß den Vorgaben der DSGVO erfolgt?

3. Datenschutzorganisation und Prozesse

**Ein besonderer Fokus beim Datenschutzaudit liegt in der Datenschutzorganisation.
Im Folgenden sind nur die wichtigsten Fragen zusammengefasst:**



- ☐ Gibt es eine eigene Datenschutzleitlinie?
- ☐ Wie ist organisatorisch sichergestellt, dass vor jeder Verarbeitung von personenbezogenen Daten geprüft wird, ob die geplante Verarbeitung zulässig ist?
- ☐ Besteht ein Prozess für die Durchführung und Dokumentation von Risikobewertungen und Datenschutz-Folgenabschätzungen?
- ☐ Gibt es im Unternehmen ein aktuelles Rollen- und Rechtekonzept?
- ☐ Ist die private Nutzung von Internetzugang, E-Mail-Postfach, dienstlichem Telefon und ggf. weiteren dienstlichen Geräten klar geregelt?
- ☐ Wie werden Betroffene über ihre Rechte informiert?
- ☐ Welcher Prozess ist für die Bewältigung einer Datenschutzpanne vorgesehen?
- ☐ Werden Einwilligungen korrekt eingeholt, dokumentiert und verwaltet?
- ☐ Werden Datenübertragungen ins Ausland korrekt durchgeführt (z. B. SCCs, TIA vorhanden)?
- ☐ Wie wurde sichergestellt, dass datenschutzrechtliche Belange bei Beginn oder Änderung eines jeden Verarbeitungsprozesses im Unternehmen berücksichtigt werden – Beachtung des Privacy by Design und Privacy by Default nach Art. 25 DSGVO?

4. Datensicherheit

- ☐ Wie ist der Zugang zu personenbezogenen Daten geregelt?
- ☐ Besteht ein IT-Sicherheitskonzept?
- ☐ Besteht ein externer Zugriff auf einzelne oder alle Systeme im Netzwerk (z. B. für Home-Office, E-Mail-Abruf oder Fernwartung)?
- ☐ Wie wird die Einhaltung aktueller technischer Standards gewährleistet?
- ☐ Werden aktuelle Checklisten zur Auswahl von technischen und organisatorischen Maßnahmen mit einer risikoorientierten Betrachtungsweise auf Basis von Art, Umfang sowie den Zwecken der Verarbeitung und der unterschiedlichen Eintrittswahrscheinlichkeit sowie Schwere der Risiken für die Rechte und Freiheiten geführt?
- ☐ Gibt es Mechanismen, um Betroffenenrechte wie Auskunft, Löschung oder Berichtigung zu gewährleisten?

5. Abschluss und Maßnahmen



- ☐ **Audit-Bericht erstellen:** Sind alle Ergebnisse dokumentiert, inklusive Abweichungen und Empfehlungen?
- ☐ **Ergebnisse besprechen:** Welche Handlungsempfehlungen lassen sich ableiten?
- ☐ **Verbesserungsmaßnahmen planen:** Gibt es konkrete To-Dos und Fristen für die Umsetzung?

DSGVO-Check mit datenschutzexperte.de

Ein Datenschutzaudit ist Ausgangspunkt für Ihr individuelles Datenschutzkonzept – mit oder ohne Zertifizierung ist dieses Konzept für jedes Unternehmen unverzichtbar. Es dokumentiert datenschutzrechtliche Maßnahmen und bezieht sich auf die gesamte Organisation oder einzelne Prozesse. Voraussetzung für das Erstellen eines Datenschutzkonzepts ist neben dem Datenschutzaudit auch eine GAP-Analyse.

Dabei unterstützen wir Sie gern!



Sie haben Fragen? Wir helfen Ihnen weiter!

Sie wünschen eine unverbindliche Beratung zu
Datenschutzsoftware in Ihrem Unternehmen und
dem Thema externer Datenschutzbeauftragter?
Rufen Sie uns gerne an oder schreiben Sie uns
eine E-Mail!

datenschutzexperte.de
+49 (0)89 2500 392 20
info@datenschutzexperte.de



Alexander Ingelheim
Geschäftsführung

datenschutzexperte.de ist Ihr Partner im Datenschutz.

Wir glauben, dass Datenschutz nicht teuer und komplex sein muss. Mit unseren auf KMU zugeschnittenen Lösungen beraten wir Sie als externer Datenschutzbeauftragter. Alternativ unterstützen wir sowohl interne oder externe Datenschutzbeauftragte mit unserer smarten SaaS-Plattform Proliance 360. So lässt sich Datenschutz einfach und pragmatisch umsetzen. Wir sind ein junges Münchner Unternehmen mit mehr als 70 Mitarbeitern und helfen bereits über 2.000 Unternehmen, die Herausforderungen der DSGVO zu meistern. Sprechen Sie uns gerne an.

Copyright © 2025 PROLIANCE GmbH

Wir behalten uns alle Rechte an diesem Dokument vor. Dieses Paper sowie Teile davon dürfen nicht ohne schriftliche Einwilligung der PROLIANCE GmbH reproduziert oder in kommerzieller Weise verwendet werden. Es dient lediglich als Leitfaden und erhebt keinen Anspruch auf Vollständigkeit und/oder Rechtsverbindlichkeit. Trotz höchster Sorgfalt bei der Erstellung des Textes übernehmen wir keine Haftung oder Verantwortung dafür, dass dieser fehlerfrei ist. Dieses Dokument ersetzt keine individuelle Rechtsberatung; für eine persönliche Beratung kontaktieren Sie bitte einen unserer Legal Consultants oder einen Rechtsanwalt.



Join the movement
Wir sind Mitglied

