Checkliste ISO 27001

GRASP
Integrated Risk Management

Dieser Leitfaden kann Ihnen bei der Überprüfung der wichtigsten Punkte für die **ISO 27001-Zertifizierung** helfen, beachten Sie jedoch, dass er nicht alle spezifischen Anforderungen Ihres Unternehmens abdeckt. Für eine vereinfachte Zertifizierung bieten wir unsere Softwarelösung GRASP an, die sie bei der effizienten Umsetzung und Verwaltung Ihrer Datenschutzrichtlinien unterstützt.

01 LEITUNG UND VERPFLICHTUNG

	JA	NEIN
Hat das Unternehmen ein Informationssicherheits-managementsystem (ISMS) implementiert?	☐	☐
Gibt es eine formelle Sicherheitsrichtlinie, die von der Unternehmensleitung genehmigt und unterstützt wird?	☐	☐
Wurden die Rollen und Verantwortlichkeiten für die Informationssicherheit festgelegt und dokumentiert?	☐	☐

02 RISIKOMANAGEMENT

	JA	NEIN
Wurden Risikobewertungen für die Informationssicherheit durchgeführt?	☐	☐
Sind angemessene Maßnahmen zur Behandlung identifizierter Risiken implementiert worden?	☐	☐
Wird das Risikomanagement regelmäßig überprüft und aktualisiert?	☐	☐

03 ZUGANGSSTEUERUNG

	JA	NEIN
Werden Zugriffsrechte auf personenbezogene Daten kontrolliert und überwacht?	☐	☐
Gibt es Mechanismen zur sicheren Verwaltung von Zugriffsrechten, z.B. durch die Nutzung von Benutzerkonten und Passwörtern?	☐	☐
Werden Zugriffsrechte bei Bedarf aktualisiert oder widerrufen?	☐	☐

Checkliste ISO 27001

GRASP
Integrated Risk Management

04 DATENSCHUTZ DURCH TECHNIKGESTALTUNG

	JA	NEIN
Werden Datenschutzaspekte bereits bei der Entwicklung von Systemen und Prozessen berücksichtigt?	☐	☐
Werden Standardmaßnahmen zum Schutz personenbezogener Daten implementiert, z.B. Pseudonymisierung oder Verschlüsselung?	☐	☐

05 SCHULUNG UND BEWUSSTSEIN

	JA	NEIN
Werden Mitarbeiter regelmäßig über Datenschutzrichtlinien und -verfahren informiert und geschult?	☐	☐
Gibt es Mechanismen, um das Bewusstsein für Datenschutzrisiken zu schärfen, z.B. durch Schulungen, Schulungsmaterialien oder interne Kommunikation?	☐	☐

06 INCIDENT MANAGEMENT

	JA	NEIN
Gibt es ein Verfahren zur Meldung und Behandlung von Datenschutzverletzungen oder Sicherheitsvorfällen?	☐	☐
Wird das Incident-Management regelmäßig getestet und aktualisiert?	☐	☐

07 ÜBERWACHUNG UND ANALYSE

	JA	NEIN
Werden Sicherheitsmaßnahmen und -ereignisse regelmäßig überwacht und analysiert?	☐	☐
Werden Sicherheitsvorkehrungen wie Firewall-Logs, Zugriffsprotokolle usw. überprüft?	☐	☐

Checkliste ISO 27001

GRASP
Integrated Risk Management

08 COMPLIANCE-MANAGEMENT

	JA	NEIN
Wird die Einhaltung gesetzlicher Anforderungen im Zusammenhang mit dem Datenschutz regelmäßig überprüft und dokumentiert?	☐	☐
Gibt es Mechanismen zur Überprüfung und Aktualisierung der Datenschutzmaßnahmen im Einklang mit sich ändernden Gesetzen und Vorschriften?	☐	☐

09 EXTERNE KOMMUNIKATION UND ZUSAMMENARBEIT

	JA	NEIN
Werden angemessene Sicherheitsmaßnahmen bei der Kommunikation und Zusammenarbeit mit externen Parteien, z.B. Lieferanten oder Kunden, getroffen?	☐	☐
Wird der Datenschutz in Vereinbarungen mit externen Partnern angemessen berücksichtigt?	☐	☐

10 VERBESSERUNG

	JA	NEIN
Werden regelmäßige Überprüfungen und Bewertungen des ISMS durchgeführt, um Verbesserungsmöglichkeiten zu identifizieren?	☐	☐

Erleben Sie höchste Sicherheit mit GRASP

Wenn Sie bei der **ISO 27001-Zertifizierung** zur Vereinfachung eine Software einsetzen möchten, haben wir dafür die richtige Lösung parat. Unsere Softwarelösung **GRASP** bietet Ihnen die nötige Unterstützung, um Ihre Datenschutzrichtlinien effizient umzusetzen und zu verwalten. Kontaktieren Sie uns noch heute, um mehr darüber zu erfahren, wie wir Ihnen helfen können!

Gina Kaulfuss
Chief Sales Officer
gina.kaulfuss@dextradata.com

Mehr über GRASP erfahren