KATLEX
DATENSCHUTZ-MANAGEMENT
Ihr zuverlässiger Leitfaden durch die DSGVO.

Checkliste Datenschutzmanagement

KATLEX Datenschutz-Management GmbH

KATLEX Datenschutz-Management GmbH

Wolbecker Windmühle 55
48167 Münster
Tel.: 02506-9320600
E-Mail: info@katlex.de
www.katlex.de

Inhalt

Allgemeiner Datenschutz im Unternehmen

	JA
Haben Sie in Ihrem Unternehmen einen externen oder internen Datenschutzbeauftragten?	☐
Fachbeispiel: Das Unternehmen XY hat mehr als 20 Mitarbeiter und verarbeitet personenbezogene Daten. Des Weiteren überwacht das Unternehmen das Firmengelände mittels Videokameras und filmt dabei zwangsläufig auch die eigenen Mitarbeiter. Zukünftig sollen Verarbeitungstätigkeiten durchgeführt werden, die eine Datenschutz-Folgeabschätzung benötigen.	
Priorität der Maßnahme:	1
Sensibilisieren Sie Ihre Mitarbeiter regelmäßig bezüglich aktuellen Datenschutzthemen? Besitzen Ihre Mitarbeiter ein Grundverständnis für den Datenschutz?	☐
Fachbeispiel: Das Unternehmen XY schult seine Mitarbeiter mindestens alle zwei Jahre zu Datenschutz-Grundlagen und aktuellen Themen des Datenschutzes.	
Priorität der Maßnahme:	1
Überprüfen Sie regelmäßig das aktuelle Datenschutzniveau Ihres Unternehmens und führen ein Datenschutzaudit durch?	☐
Fachbeispiel: Das Unternehmen XY führt jedes Jahr ein Datenschutzaudit mit unabhängigen Auditoren durch (Vermeidung von Interessenskonflikten). Aus dem durchgeführten Audit resultieren Handlungsempfehlungen, die das Unternehmen XY zeitnah umsetzt, um ein DSGVO-konformes Datenschutzniveau zu gewährleisten.	
Priorität der Maßnahme:	1

IT-Infrastruktur aus Datenschutzsicht

	JA
Setzen Sie in Ihrem Unternehmen eine geeignete Firewall ein, die mit aktuellen Updates versorgt wird?	☐
Fachbeispiel: Das Unternehmen XY sichert seine IT-Infrastruktur vor Schadhaften Programmen oder unbefugtem Zugriff durch ein geeignetes Sicherheitskonzept ab. Dieses Sicherheitskonzept beinhaltet auch den Einsatz einer Firewall, die regelmäßig auf den neuesten Softwarestand geupdatet wird.	
Priorität der Maßnahme:	1
Haben Sie Ihre Endgeräte (Laptops, PC's, Smartphones, Tablets, etc.) ausreichend abgesichert, z. B. durch Sicherheitssoftware die möglichen schadhaften Code identifiziert?	☐
Fachbeispiel: Das Unternehmen XY sichert seine Endgeräte durch den Einsatz geeigneter Anti-Virus-Programme ab.	
Priorität der Maßnahme:	1
Ist der Zugriff auf die IT-Infrastruktur durch Authentifizierungsmethoden (z. B. Zwei-Faktor-Authentifizierung) je Arbeitsplatz abgesichert?	☐
Fachbeispiel: Max Mustermann, Mitarbeiter des Unternehmens XY, meldet sich an seinen Systemen mit einer Zwei-Faktor-Authentifizierung an. Er benötigt dafür sowohl ein Passwort, als auch ein Token.	
Priorität der Maßnahme:	2
Vergeben Sie Passwortrichtlinien für Ihre Mitarbeiter?	☐
Fachbeispiel: Das Unternehmen XY hat für die Passwortvergabe Richtlinie entwickelt. Demnach müssen die Passwörter eine bestimmte Länge, Groß- und Kleinbuchstaben und Sonderzeichen beinhalten.	
Priorität der Maßnahme:	1

Haben Sie ein Konzept für Zugriffsberechtigungen implementiert?

JA ☐

Fachbeispiel:
Max Mustermann darf innerhalb seiner Organisation nur auf die Dateien Zugreifen, die für seine Abteilung und seine Position bestimmt sind. Alle anderen Zugriffe auf Dateien sind ihm technisch untersagt.

Priorität der Maßnahme: 1

Haben Sie einen Prozess für Datenschutzvorfälle definiert?

☐

Fachbeispiel:
Sollte es in dem Unternehmen XY einen Datenschutzvorfall geben (z. B. E-Mail mit personenbezogenen Daten wurde an den falschen Empfänger versendet), gibt es einen Prozess der die Dokumentation und Meldung bei der Datenschutzbehörde beinhaltet.

Priorität der Maßnahme: 1

Ist der Kern Ihrer IT-Infrastruktur durch Zutrittskontrollen abgesichert?

☐

Fachbeispiel:
Der Serverraum des Unternehmens XY darf nur mit entsprechender Berichtigung und Authentifizierung betreten werden.

Priorität der Maßnahme: 1

Werden gespeicherte personenbezogenen Daten regelmäßig überprüft und gelöscht, um die Löschfristen einzuhalten?

☐

Fachbeispiel:
In regelmäßigen Abständen wird in dem Unternehmen XY überprüft, welche personenbezogenen Daten gelöscht werden müssen.

Priorität der Maßnahme: 1

Haben Sie einen IT-Notfallplan entwickelt?

☐

Fachbeispiel:
Das Unternehmen XY hat einen IT-Notfallplan entwickelt, um im Fall eines Brandes innerhalb einer angemessenen Zeit auf das CRM / ERP-System zugreifen können.

Priorität der Maßnahme: 1

Kundendaten Datenschutz

	JA
Haben Sie die Einwilligungen Ihrer Kunden / Interessenten für den Versand von Werbemails?	☐
Fachbeispiel: Das Unternehmen XY informiert seine Kunden formal rechtmäßig bei Vertragsabschluss, dass sie Informationen zu ähnlichen Produkten oder Dienstleistungen erhalten werden.	
Priorität der Maßnahme:	1

Können Sie Kundenanfragen bzgl. des Datenschutzes kurzfristig bearbeiten (Betroffenenrechte)?	☐
Fachbeispiel: Das Unternehmen XY hat von einem seiner Kunden den Auftrag bekommen seine personenbezogenen Daten zu löschen und hat die Löschung kurzfristig realisiert. Im Nachgang erhält der Kunde Informationen zur Löschung.	
Priorität der Maßnahme:	1

Informieren Sie Ihre Kunden regelmäßig über Ihre Datenverarbeitungstätigkeiten? Haben Sie für die Informationspflicht Prozesse in Ihrem Unternehmen definiert?	☐
Fachbeispiel: Das Unternehmen XY unterrichtet seine Kunden bei Erhebung über deren Verarbeitungstätigkeiten in dem Unternehmen und hält somit die Informationspflicht ein.	
Priorität der Maßnahme:	1

Dienstleister Datenschutz

Haben Sie und Ihre Dienstleister gültige Auftragsverarbeitungsverträge abgeschlossen?	JA ☐
Fachbeispiel: Das Unternehmen XY hat mit jedem seiner Dienstleister Auftragsverarbeitungsverträge abgeschlossen, die Datensätze des Unternehmens verarbeiten.	
Priorität der Maßnahme:	1

Haben Sie Ihre Dienstleister auf das Datengeheimnis verpflichtet?	☐
Fachbeispiel: Das Unternehmen XY hat seine Dienstleister formal rechtmäßig verpflichtet keine Daten des Unternehmens an Dritte weiter zu geben.	
Priorität der Maßnahme:	1

Mitarbeiter Datenschutz

Erheben Sie die Daten Ihrer Mitarbeiter nur zu folgendem Zwecke: Aufnahme, Beendigung und Durchführung des Beschäftigungsverhältnisses?	☐
Fachbeispiel: Das Unternehmen XY erhebt die Daten der nur wenn ein Mitarbeiter das Unternehmen verlässt, beitritt oder das Beschäftigungsverhältnis besteht.	
Priorität der Maßnahme:	1

Haben Sie eine schriftliche Einwilligung Ihrer Mitarbeiter für die Erhebung von personenbezogenen Daten?	☐
Fachbeispiel: Das Unternehmen XY hat jedem Mitarbeiter eine schriftliche Einwilligung zur Erhebung von personenbezogenen Daten vorgelegt. Diese wurde von dem jeweiligen Mitarbeiter unterschrieben und archiviert.	
Priorität der Maßnahme:	1

Dokumentation nach DSGVO

Haben Sie ein Verzeichnis von Verarbeitungstätigkeiten?	JA
	☐

Fachbeispiel:
Das Unternehmen XY hat alle Verarbeitungstätigkeiten aufgelistet und beschrieben. Somit kann jeder Zeit Auskunft über die Verarbeitungstätigkeiten erteilt werden.

Priorität der Maßnahme:	1

Haben Sie die Verarbeitungstätigkeiten auf die Notwendigkeit einer Datenschutzfolgeabschätzung (DSFA) geprüft?	☐

Fachbeispiel:
Das Unternehmen XY führt eine Schwellwertanalyse bzgl. aller Verarbeitungstätigkeiten durch.

Priorität der Maßnahme:	1

Dokumentieren Sie Ihre technischen und organisatorischen Maßnahmen?	☐

Fachbeispiel:
Das Unternehmen XY dokumentiert alle technischen und organisatorischen Maßnahmen, die zur Einhaltung der Sicherheitsziele (z. B. Integrität und Vertraulichkeit) beitragen.

Priorität der Maßnahme:	1

NOTIZEN

Haben Sie **Fragen?**

Vereinbaren Sie Ihre kostenlose Erstberatung zum Thema Datenschutzmanagement.

KATLEX Datenschutz-Management GmbH

Wolbecker Windmühle 55
48167 Münster
Tel.: 02506-9320600
E-Mail: info@katlex.de
www.katlex.de