In drei Schritten meine Datenschutz-Compliance prüfen

Audit-Light Ratgeber als Grundlage zu Datenschutz-Sicherheitscheck gemäss Art. 24 und 32 DSGVO der EU-Datenschutzgrundverordnung

Wir möchten Ihnen mit diesem **Audit-Light** helfen, selbst eine erste Kontrolle der Datenschutzkonformität durchzuführen.

Die Datenschutz-Richtlinie betrifft vor allem den **Schutz der persönlichen Daten**. Damit eng verbunden ist auch die **IT Sicherheit**, denn wenn Ihre Daten durch Fehler verloren gehen oder in die falschen Hände geraten, sind potentiell auch die personenbezogenen Daten betroffen.

Das hier ist kein voller Audit, es soll Ihnen lediglich die erste Auskunft darüber geben, wir sicher Ihr Unternehmen in Sachen Datenschutz aufgestellt ist. Dieser Schnelltest zeigt auf, wo Sie weitergehende Überprüfung einleiten müssen. Die DSGVO wird immer dann angewendet, wenn sie Daten von Menschen aus dem EU Raum bearbeiten.

Unten finden Sie geschlossene Fragen, die Sie für sich mit JA, NEIN, oder ICH WEISS NICHT, beantworten sollen. Wenn Sie sich bei allem sicher fühlen und immer JA sagen können, könnte bei Ihnen alles in Ordnung sein. Sollten Sie jedoch Zweifel haben oder keine Antwort wissen, sollen Sie einen Audit durchführen lassen.

Ein Audit offenbart Ihnen auch die verbesserungswürdigen oder kritischen Gebiete.

info@drkpi.com +41 44 2721876 CyTRAP Labs GmbH Röntgenstrasse 49 CH-8005 Zürich

Erste Schritte

Stellen wir sicher, dass alle Mitarbeiter auf das Datengeheimnis verpflichtet sind?

- Sind externe wie interne MitarbeiterInnen verpflichtet?
- Wurden MitarbeiterInnen geschult und informiert, was Datenschutz wirklich bedeutet?
- Wurden MitarbeiterInnen geschult und informiert, wie sie sich in Situationen wie beispielsweise im Telefonat mit Kunden verhalten sollen?

Datensicherheit: Haben wir den Grundschutz sichergestellt mit folgenden Vorkehrungen:

- Haben wir mögliche Risiken eruiert und deren Prävention sichergestellt?
- Haben wir einen Notfallplan (z.B. bei einem Data Breach, wer wird wann informiert)?
- Sind alle MitarbeiterInnen über den Notfallplan informiert?
- Haben wir verantwortliche Personen für diverse IT-Sicherheitsaspekte benannt?
- Wurden Regeln aufgestellt, wer zu welchen Daten über welche Applikationen Zugriff hat (Privacy by Design)?
- Wurden Regeln aufgestellt, wer zu welchen Räumen oder Servern oder Datensammlungen Zutritt oder Zugang hat?
- Sind alle Regelwerke dokumentiert, sicher aufbewahrt und für alle bei Bedarf zugänglich?

info@drkpi.com +41 44 2721876 CyTRAP Labs GmbH Röntgenstrasse 49 CH-8005 Zürich

Dokumentation von IT-Verfahren, Software, IT-Konfiguration

Haben wir einen Datenschutzverantwortlichen:

- der sich um die Software und alle relevanten Verfahren kümmert?
- Verhält sich diese Person oder Anbieter datenschutzkonform?

Läuft unsere interne und externe Datenübertragung sicher?

Haben wir Massnahmen eingeleitet, um uns gegen Schadsoftware zu schützen?

Nutzen wir sichere interne und externe Datenträger?

Stellen wir sicher und kontrollieren wir, dass vor, während und nach Wartungs- oder Reparaturarbeiten auf den Datenschutz geachtet wird?

Haben wir Risiken im Griff, beispielsweise:

- Dass intern programmierten Applikationen keine Schwachstellen/Vulnerabilities haben?
- Extern eingekaufte oder in der Cloud genutzte Software Programme / Applikationen keine Schwachstellen / Vulnerabilities haben?
- Das systematische Risiko für Viren, Malware und Ransomware Infektion nicht zu hoch ist?
- Wird das kontrolliert, überprüft, dokumentiert?

info@drkpi.com +41 44 2721876 CyTRAP Labs GmbH Röntgenstrasse 49 CH-8005 Zürich

Internet, E-Mail, personenbezogen Daten

Ist unsere Internetseite datenschutzkonform?

Ist unser E-Mail Marketing datenschutzkonform?

Können wir die Datenschutzkonformität im Kontakt mit EU-Ländern jederzeit gewährleisten bzw. belegen?

Wenn wir geschäftliche Kontakte zu US Firmen haben, können wir jederzeit belegen, dass wir datenschutzkonform sind?

Sammeln wir personenbezogene Daten von Dritten (Emailadressen für unseren Newsletter, beispielsweise)? Wenn ja, ist

- die Sammlung dieser Informationen DSGVO-konform?
- deren Speicherung DSGVO-konform?

Sind alle Mitarbeiter informiert, wie sie mit der Sammlung, Speicherung, Weiterverarbeitung und Löschung dieser Daten umgehen sollen?

Ressourcen:

- https://drkpi.com/dsgvo - Wiki Seite
- https://drkpi.com/category/datensicherheit/ - Datenschutz, Malware, Ransomware, Blockchain
- https://drkpi.com/?p=16483 mehr zum Thema inkl. pdf Datei für den drkpi® DSGVO Audit Light Ratgeber

info@drkpi.com +41 44 2721876 CyTRAP Labs GmbH Röntgenstrasse 49 CH-8005 Zürich