systemQM

Datenschutz KMU 1.0

Prüfliste

für kleine und mittlere Unternehmen

in Orientierung an den Anforderungen der EU-DSGVO und des BDSG 2018

als Ergänzung zum internen Qualitätsmanagement

Die herausgebende Stelle

systemQMe.V.
Barbarossa Str.29
D-76855 Annweiler

E-Mail: info@system-qm.de
Web: www.system-qm.de

Aus der Vereinssatzung
§ 3 (Zweck des Vereins)

Zweck des Vereins ist die Unterstützung von Organisationen im Gesundheitswesen, der Wohlfahrtspflege und der Bildung für die Bereiche Qualitätsmanagement, Qualitätssicherung, Arbeitsschutz und Risikomanagement.

Der Satzungszweck wird insbesondere verwirklicht durch die Bereitstellung von Managementsystemen, von Instrumenten zur Qualitätssicherung und zum Risikomanagement sowie durch Fachveranstaltungen zur Thematik.

Grundlagen

Das Verfahren systemQM Datenschutz KMU 1.0 orientiert sich an den Vorgaben

- Europäischen Datenschutz-Grundverordnung
- BDSG 2018

Version **1.0**

Datum **01.12.2018**

Schutzgebühr: 59,80 € zzgl. 19 % MwSt.

Vorbemerkung

Voraussetzungen zur Anerkennung

- Umsetzung der Anforderungen gemäß den Vorgaben des Manuals **systemQM Datenschutz 1.0**

Zertifizierungsablauf

- Auswahl einer mit **systemQM** e.V. kooperierenden Zertifizierungsstelle, deren Eignung sichergestellt ist (siehe www.system-qm.de)
- Durchführung eines externen Audits anhand der Kriterien der Checkliste **systemQM Datenschutz 1.0**
- Bestandteile des externen Audits:
  - Dokumentenprüfung durch die Zertifizierungsstelle
  - Vor-Ort-Audit durch nachweislich im Verfahren systemQM geschulte Auditoren der Zertifizierungsstelle

Gültigkeit

- Drei Jahre
- Jährliches Überwachungsaudit
- Re-Zertifizierungsaudit alle 3 Jahre

Vorbemerkung

Allgemeine Anmerkung

Aus Gründen der einfachen Lesbarkeit wird die männliche Form verwendet.

Zentrale Abkürzungen

Art.	Artikel
AV	Auftragsverarbeiter
BDSG	Bundesdatenschutzgesetz
DS	Datenschutz
DSB	Datenschutzbeauftragte/r
EU-DSGVO	Europäische Datenschutz-Grundverordnung
Kap.	Kapitel
MA	Mitarbeiter/in
TOM	technische und organisatorische Maßnahmen

Bewertung Erfordernis

1 =	Nichterfüllung ist akzeptabel
2 =	Nichterfüllung ist akzeptabel, aber nicht zu empfehlen
3 =	Nichterfüllung ist nur in Ausnahmefällen akzeptabel
4 =	Nichterfüllung ist nicht akzeptabel

Inhaltsverzeichnis

1 Datenschutzorganisation im Betrieb

1.1 Datenschutzmanagement

Nr.	Aufgabe	Erfüllt	Nicht erfüllt	Bewertung Erfordernis
1.1 A	Es wurden Zuständigkeiten eindeutig und widerspruchsfrei zugewiesen.			2
1.1 B	Wenn [1.1 A] ja: Es wurden Ressourcen für die Zuständigen zur Verfügung gestellt.			4
1.1 C	Wenn [1.1 A] ja: Die Zuständigkeiten wurden dokumentiert.			3
1.1 D	Wenn [1.1 A] ja: Die Zuständigkeiten werden regelmäßig geprüft.			3
1.1 E	Richtlinien für Mitarbeiter wurden erstellt und den Mitarbeitern zur Verfügung gestellt.			1
1.1 F	Richtlinien für bestimmte Datenverarbeitungen wurden erstellt und den mit den Datenverarbeitungen bestimmten Beschäftigten/ Vertragspartnern zur Verfügung gestellt.			1
1.1 G	Wenn [1.1 E] und/oder [1.1 F] ja: Die Richtlinien werden regelmäßig überprüft.			1
1.1 H	Dokumentierte Prozesse zur Etablierung, Änderung und Beendigung einer Datenverarbeitung wurden erstellt.			3
1.1 I	Wenn [1.1 H] ja: Die Prozesse werden regelmäßig überprüft.			3
1.1 J	Eine Übersicht aller DS-relevanten Pflichten wurde erstellt.			4

1.2 Datenschutzbeauftragter

Nr.	Aufgabe	Erfüllt	Nicht erfüllt	Bewertung Erfordernis
1.2 A	Der Verantwortliche beschäftigt mind. 10 MA ständig mit einer Datenverarbeitung oder führt besonders risikogefährdete Tätigkeiten gemäß Art. 37 Abs. 1 durch.			1
1.2 B	Wenn [1.2 A] ja: Ein DSB wurde benannt.			4
1.2 C	Wenn [1.2 A] nein: Ein DSB wurde benannt.			2
1.2 D	Wenn [1.2 B] oder [1.2 C] ja: Die Kontaktdaten des DSB wurden der Aufsichtsbehörde mitgeteilt.			4
1.2 E	Wenn [1.2 B] oder [2.2 C] ja: Die Kontaktdaten des DSB wurden veröffentlicht (Homepage, DS-Informationen).			4

1.3 Dokumentation, Rechenschaftspflicht

wird bei den jeweiligen Pflichten abgefragt

1.4 Verhaltensregeln und Zertifizierungen

Nr.	Aufgabe	Erfüllt	Nicht erfüllt	Bewertung Erfordernis
1.4 A	Es bestehen Verhaltensregeln.			1
1.4 B	Wenn [1.4 A] ja: Alle getroffenen Maßnahmen wurden an diesen Verhaltensregeln ausgerichtet.			3
1.4 C	Der Verantwortliche wurde gem. EU-DSGVO zertifiziert.			1