Datenschutz – Grundverordnung

und

Qualitätsmanagement ISO 9001

- **Zusammenhang**
- **Integration**
- **rechtssicheres Agieren**

Ing. Walter Kalcher
Qualitätsmanagement

0699 11167439
qm@walterkalcher.at
www.walterkalcher.at

Inhalt

1 Worum geht´s?

- Sie haben schon gehört, dass diese EU – Datenschutz – Grundverordnung mit 25.5.2018 in Kraft tritt?
- Sie sind sich nicht sicher, ob diese auch für Ihr Unternehmen gilt?
- Sie wollen erfahren, WIE Sie diese gesetzlichen Anforderungen einfach und rechtssicher erfüllen können?

2 WAS ist die EU – Datenschutz – Grundverordnung (EU-DSGVO)?

Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (Artikel 1).

- Als Verordnung ist sie in der gesamten EU gültig!
- Sie tritt per 25.5.2018 in Kraft!
- Sie sind als Unternehmen massiv angreifbar, wenn Sie nichts tun (Strafen bis 20 Mio €)!
- Sie verhilft den „Betroffenen" (= Besitzer der personenbezogenen Daten) zu umfassenden Rechten gegenüber Organisationen.

Diese Rechte sind:

Informationspflicht durch den Erheber der Daten
Auskunftsrecht
Recht auf Berichtigung
Recht auf Löschung
Recht auf Einschränkung der Verarbeitung
Recht auf Datenübertragbarkeit
Widerspruchsrecht

Das sind also Anforderungen für Sie als Unternehmer, aber auch IHRE ganz persönlichen Rechte als Person!

Jede Verarbeitung von personenbezogenen Daten durch ein Unternehmen ist damit erfasst! Was auch gleich zur Frage führt:

3 Gilt die EU – Datenschutz – Grundverordnung auch für mein / unser Unternehmen?

Wenn Sie personenbezogene Daten verarbeiten JA!

Jedes Unternehmen verarbeitet
- Kundendaten
- Lieferantendaten
- Mitarbeiterdaten (wenn relevant)
- Daten relevanter Interessens- und Wirtschaftspartner

Selbst für mich als EPU ist diese EU – DSGVO relevant!

4 Was ist unter „Verarbeitung von personenbezogenen Daten" zu verstehen?

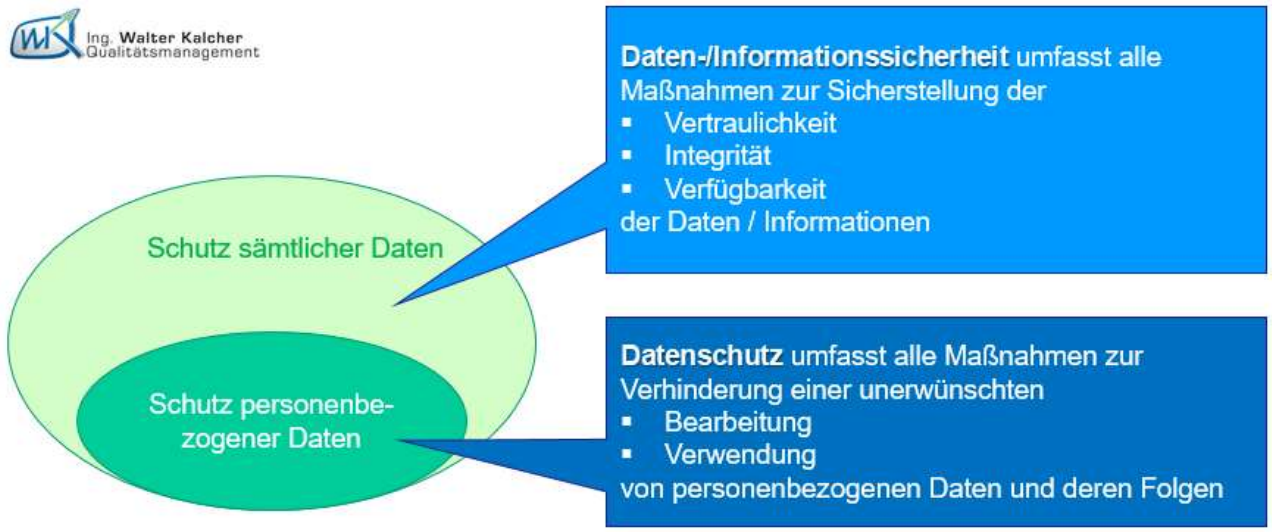
Unter dem Begriff „Verarbeitung" ist im Artikel 4 (2) definiert:
„Verarbeitung" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie
- das Erheben,
- das Erfassen,
- die Organisation,
- das Ordnen,
- die Speicherung,
- die Anpassung oder Veränderung,
- das Auslesen,
- das Abfragen,
- die Verwendung,
- die Offenlegung durch Übermittlung,
- Verbreitung oder eine andere Form der Bereitstellung,
- den Abgleich oder die Verknüpfung,
- die Einschränkung,
- das Löschen oder
- die Vernichtung

Es ist also jeglicher Umgang mit personenbezogenen Daten als Datenverarbeitung zu sehen.

Sehen Sie die Sache positiv!

Gehen Sie einmal grundsätzlich davon aus, dass diese EU-DSGVO Sie und Ihr Unternehmen trifft.

Wenn Sie durch organisatorische und technische Maßnahmen den Schutz der personenbezogenen Daten erhöhen, so erhöhen Sie insgesamt den Schutz Ihres gesamten Datenbestands im Unternehmen, der wohl ebenso schützenwert wie wertvoll sein wird.



Fakt ist:

- Sie verbessern Ihren organisatorischen Umgang mit Daten
- Sie verbessern Ihre Unternehmenssicherheit durch Datensicherheitsmanagement
- Die Umsetzung der Anforderungen ist gar nicht zu schwierig

Durch die Anforderung der EU-DSGVO nach organisatorischen und technischen Maßnahmen bekommt das Thema einen klaren strategischen Fokus. Denn Datensicherheit ist ja von existentieller Bedeutung für das Unternehmen.

5 Was hat die EU – DSGVO mit Qualitätsmanagement zu tun?

Qualitätsmanagement nach ISO 9001 fokussiert grundsätzlich auf die beständige Erfüllung von Kundenanforderungen und die Erhöhung von Kundenzufriedenheit.

Sie legt dazu die Anforderungen fest, die für die gesamte Organisation gelten – einschließlich die Erfüllung von gesetzlichen und behördlichen Anforderungen.

Für mich ist Qualitätsmanagement nach ISO 9001 eine Bedienungsanleitung, wie ein Unternehmen organisiert werden kann.

In der ISO 9001:2015 kommt unter Punkt 8.5.3. „Eigentum der Kunden oder der externer Anbieter" unter ANMERKUNG explizit der Begriff „***personenbezogene Daten***" vor.

6 Warum redet ein Qualitätsmanager bei der EU – DSGVO mit?

Ich bin langjährig

- operativer
- beratender und
- auditierender (Quality Austria)

Qualitätsmanager und berate Kunden im Aufbau und Pflege eines Qualitätsmanagementsystems nach ISO 9001.
Dabei ist stets auch die Integrierung der relevanten gesetzlichen Anforderungen in ein Qualitätsmanagementsystem (KEINE Rechtsberatung!) Thema.

Ich bin durch eine Informationsveranstaltung eher zufällig auf das Thema Datenschutz – Grundverordnung gestoßen. Von einem Juristen wurde diese an sich komplexe Rechtsmaterie kompetent und launig vorgetragen.

Bald wurde mir klar, dass die Anforderungen /einzelne Artikel dieser Datenschutz – Grundverordnung gut zu den einzelnen Normelementen der ISO 9001 passen.

Da auch mich als EPU diese Verordnung trifft, habe ich mich in die Materie vertieft und eingearbeitet. Zwar bin ich kein IT – Techniker, aber als jahrzehntelanger Anwender von Office-, ERP- und diversen weiteren Softwareprodukten, sowie Anwender eigener Hardware habe ich Erfahrung sammeln dürfen. Daher kann ich mir unter technischen Datenschutz durchaus etwas vorstellen, maße mir aber eben keine tieferen IT – Kompetenz an.

Mein Ansatz in meiner Beratungstätigkeit als Qualitätsmanager ist die Unterstützung von Unternehmen

- beim Verstehen der gesetzlichen Anforderungen
- der Umsetzung durch geeignete Maßnahmen
- sowie die Verankerung im Qualitätsmanagementsystem durch geeignete Dokumentation einschließlich Schulung und Information.

Das alles unter Einbindung der Geschäftsleitung, des Qualitätsmanagements und selbstverständlich des IT - Personals.

Eine extrem starke gesetzliche Anforderung mit weitreichenden Auswirkungen quer durch ein Unternehmen sehe ich nun durch die EU – DSGVO gegeben.

7 Wie kann ein Qualitätsmanager bei der Umsetzung der EU – DSGVO unterstützen?

Unternehmen mit einem lebenden und dokumentierten Qualitätsmanagementsystem nach ISO 9001 können

- Prozesse und Verfahren
- Richtlinien und Politiken
- Dokumentations- und Nachweispflichten
- Verantwortungen und Befugnisse und
- vieles anderes mehr

zur Erfüllung der EU-DSGVO, so strukturiert und gemanagt in ihre Unternehmensorganisation nachhaltig verankern.

8 Korrelationstabelle DSGVO – ISO 9001:2015

Nachstehend habe ich Ihnen eine Korrelationstabelle erstellt, wie ich die einzelnen Artikel der DSGVO den relevanten Normelementen der ISO 9001:2015 zuordne.

Nr.	DSGVO - Artikel (wesentlichste)	ISO 9001:2015			
1	Gegenstand und Ziele	4.3.	6.2.	7.1.6.	8.5.3.
2	Sachlicher Anwendungsbereich	4.1.	4.2.	4.3.	
3	Räumlicher Anwendungsbereich	4.1.	4.2.	4.3.	
4	Begriffsbestimmungen	7.1.6.	7.2.	7.3.	
5	Grundsätze für die Verarbeitung personenbezogener Daten	4.4.	5.2.	7.5.	
6	Rechtmäßigkeit der Verarbeitung	7.5.	8.2.		
7	Bedingungen für die Einwilligung	7.5.	8.2.		
8	Bedingungen für die Einwilligung eines Kindes in Bezug auf Dienste der Informationsgesellschaft	7.5.	8.2.		
9	Verarbeitung besonderer Kategorien personenbezogener Daten	7.5.	8.2.		
10	Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten	7.5.	8.2.		
11	Verarbeitung, für die eine Identifizierung der betroffenen Person nicht erforderlich ist	7.5.	8.2.		
12	Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person	7.4.	7.5.	8.2.1.	

Nr.	DSGVO - Artikel (wesentlichste)	ISO 9001:2015			
13	Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person	7.4.	7.5.	8.2.1.	
14	Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden	7.4.	7.5.	8.2.1.	
15	Auskunftsrecht der betroffenen Person	7.4.	7.5.	8.2.1.	
16	Recht auf Berichtigung	7.4.	7.5.	8.2.1.	
17	Recht auf Löschung („Recht auf Vergessenwerden“)	7.4.	7.5.	8.2.1.	
18	Recht auf Einschränkung der Verarbeitung	7.4.	7.5.	8.2.1.	
19	Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung	7.4.	7.5.	8.2.1.	
20	Recht auf Datenübertragbarkeit	7.4.	7.5.	8.2.1.	
21	Widerspruchsrecht	7.4.	7.5.	8.2.1.	
22	Automatisierte Entscheidungen im Einzelfall einschließlich Profiling	7.4.	7.5.	8.2.1.	
23	Beschränkungen	---			
24	Verantwortung des für die Verarbeitung Verantwortlichen	5.3.			
25	Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen	7.1.3.	8.1.		
26	Gemeinsam für die Verarbeitung Verantwortliche	5.3.			
27	Vertreter von nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeitern	5.3.			
28	Auftragsverarbeiter	8.4.			
29	Verarbeitung unter der Aufsicht des Verantwortlichen oder des Auftragsverarbeiters	5.3.			
30	Verzeichnis von Verarbeitungstätigkeiten	7.1.6.	7.5.	8.1.	
31	Zusammenarbeit mit der Aufsichtsbehörde	7.4.			
32	Sicherheit der Verarbeitung	6.1.	7.1.3.	8.1.	
33	Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde	7.4.	8.7.		
34	Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person	7.4.	8.1.	8.2.1.	
35	Datenschutz-Folgenabschätzung	6.1.	9.1.		

Nr.	DSGVO - Artikel (wesentlichste)	ISO 9001:2015			
36	Vorherige Konsultation	7.4.			
37	Benennung eines Datenschutzbeauftragten	5.3.			
38	Stellung des Datenschutzbeauftragten	5.3.			
39	Aufgaben des Datenschutzbeauftragten	5.3.			
40	Verhaltensregeln	4.1.	5.2.	7.4.	
41	Überwachung der genehmigten Verhaltensregeln	4.1.	5.2.	7.4.	
42	Zertifizierung	4.1.	5.2.	7.4.	
43	Zertifizierungsstellen	4.1.	5.2.	7.4.	
44	Allgemeine Grundsätze der Datenübermittlung	4.1.			
45	Datenübermittlung auf der Grundlage eines Angemessen-heitsbeschlusses	4.1.			
46	Datenübermittlung vorbehaltlich geeigneter Garantien	4.1.			
47	Verbindliche interne Datenschutzvorschriften	4.1.			
48	Nach dem Unionsrecht nicht zulässige Übermittlung oder Offenlegung	4.1.			
49	Ausnahmen für bestimmte Fälle	4.1.			
50	Internationale Zusammenarbeit zum Schutz personenbe-zogener Daten	4.1.			
	51 - 59 gilt für Aufsichtsbehörde 60 - 76 gilt zwischen den Aufsichtsbehörden				
77	Recht auf Beschwerde bei einer Aufsichtsbehörde	7.1.6.	6.1.		
78	Recht auf wirksamen gerichtlichen Rechtsbehelf gegen eine Aufsichtsbehörde	7.1.6.	6.1.		
79	Recht auf wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter	7.1.6.	6.1.		
80	Vertretung von betroffenen Personen	7.1.6.	6.1.		
81	Aussetzung des Verfahrens	7.1.6.	6.1.		
82	Haftung und Recht auf Schadenersatz	7.1.6.	6.1.		
83	Allgemeine Bedingungen für die Verhängung von Geldbu-ßen	7.1.6.	6.1.		
84	Sanktionen	7.1.6.	6.1.		

Bewertung der Leistung (9) sowie Verbesserung (10) spielt natürlich im operativen Betrieb ständig eine Rolle in der Überwachung, Korrektur, Verbesserung.

Von der Leitung – die ja auch im Rahmen dieser Verordnung die Verantwortung trägt – sind sämtliche Aspekte in Kontext, Politik, Ziele bis hin zur Managementbewertung zu behandeln.

9 Mein Angebot an Sie!

Beginnen können ist Stärke. Vollenden können ist Kraft.

Laotse

Machen Sie als Qualitätsmanager dieses Thema zu Ihrem Thema!

Sensibilisieren Sie die Ihre Leitung, die IT und weitere relevante Rollen in Ihrem Unternehmen.

In einem kostenfreien Erstgespräch gebe ich Ihnen gerne weitere Anregungen und Informationen, sowie beantworte ich gerne Ihre Fragen.

Ihr

Ing. Walter Kalcher

0699 11167439
qm@walterkalcher.at
www.walterkalcher.at

Unternehmensqualität strategisch steigern