



CyberWehr

RISK MANAGEMENT SOLUTIONS GMBH

Monika Wehr ▪ +41 79 348 55 63 ▪ 8803 Rüslikon, Alte Landstrasse 109

Die Risikoanalyse ISO 27001/2, 31000 - der wichtigste Schritt zur Risikovermeidung

Ausgangssituation

Beide Gesetze, das revidierte Schweizer Datenschutzgesetz als auch die EU-DSGVO, müssen nicht nur konform, sondern auch angemessen, d.h. mit einem **risikobasierten Ansatz auf die individuellen Rahmenbedingungen des Unternehmens abgestimmt, umgesetzt** werden.

Mit dem Fortschritt elektronischer Datenverarbeitungstechnologien und dem Aufkommen immer grösserer Mengen personenbezogener Daten steht die Frage im Raum, wie die **Folgen der Technisierung auf die Persönlichkeitsrechte der Betroffenen** systematisch analysiert und entsprechende Handlungsmaßnahmen ergriffen werden können.

Der Datenschutz sieht in der Risikoanalyse nur diejenigen Risiken, die Einfluss auf natürliche Personen haben. Ein Risiko ist auch im Datenschutz definiert als die Multiplikation des Schadens mit der Eintrittswahrscheinlichkeit. Bei Datenschutz-Risiken bezieht sich der Schaden auf die Person.

Eine Schwachstelle in Ihrer IT-Infrastruktur ist nur dann ein Problem, wenn sie durch Hacker ausgenutzt werden kann. Sie ermöglicht die Verletzung der Sicherheitsziele im Datenschutz, wenn bspw. Sicherheitsmassnahmen fehlen oder eine Bedrohung nicht vollständig abgedeckt wird. Schwachstellen können auch bei Sicherheitsmassnahmen selbst auftreten, bspw. durch fehlerhafte Software-Updates. Sie stellen ein Defizit in den Prinzipien der Umsetzung des Datenschutzes dar.

Wir führen eine unabhängige Risikoanalyse durch, die alle Ihre Daten schützt und gesamtheitlich Ihre Datenschutzstrategie, die IT Infrastruktur, die Organisation und die Rechtskonformität umfasst. Denn nur mittels dieser werden Gefahrenpotentiale aufgedeckt: sie umfasst die Identifikation und die Korrelation von Risiken, die Analyse ihrer Ursachen, deren Eintrittswahrscheinlichkeit, ihre Frequenz, die Bewertung der Risiken und geeignete Massnahmen zur Risikominderung. So werden Risiken kontrollier- und steuerbar.

Die Datenschutzfolgenabschätzung (DSFA)

Mit der DSFA werden besonders **risikoreich «erscheinende» Vorhaben** einer besonderen Risikoprüfung unterzogen und nur bei positivem Prüfungsergebnis für die Datenverarbeitung freigegeben. Es werden darüber hinaus auch Massnahmen zur Risikominderung und -Vermeidung getroffen und umgesetzt.

Wann liegt überhaupt ein für eine DSFA **relevantes Risiko** vor?

- bei der Verarbeitung **besonders schutzwürdiger Daten**, insbesondere im Gesundheitsbereich mit hohem Risiko für die Rechte und Freiheiten natürliche Personen
- **Profiling**: die nutzbare Erstellung des Gesamtbildes einer Persönlichkeit für bestimmte Zwecke, z. B. zur Arbeitsvermittlung oder bei der Tätersuche
- **automatisierten Einzelentscheidungen** oder
- beim Einsatz von **Videokameras**

Bitte beachten Sie, dass in den o.g. Fällen ist die Risikoanalyse gesetzlich zwingend vorgeschrieben ist!