Datenschutzreifegrad – Wirksamkeitsmessung der datenschutzrelevanten Massnahmen

Alle Firmen der Schweiz, welche personenbezogene Daten bearbeiten, müssen das Datenschutzgesetz der Schweiz (DSG) einhalten. Dies führt dazu, dass sich immer mehr Unternehmen mit dem Datenschutz befassen und umfangreiche Dokumentationen etablieren. Doch wie misst man die Wirksamkeit der getroffenen Massnahmen?

Ausgangslage

Die neue Datenschutz-Grundverordnung (DSGVO) der EU ist seit dem 25. Mai 2018 in Kraft. Zugleich wird in der Schweiz ein neues Bundesgesetz über den Datenschutz ausgearbeitet. Dieses Gesetz sollte theoretisch bereits in Kraft sein. Aufgrund der Covid-19 Pandemie wurde das Inkrafttreten der Revision des Datenschutzgesetzes aus dem Jahr 1992 jedoch auf einen noch nicht klar definierten Zeitpunkt vertagt.

Nicht nur wegen der gesetzlichen Anpassungen hat der Datenschutz in den Unternehmen an Stellenwert gewonnen. Sondern auch durch die technische Erneuerung sowie, weil sich Datenschutzvorfälle häufen und somit zu einem immer grösser werdenden Risikofaktor für Unternehmen werden. Um das Risiko eines Image- und Vertrauensverlustes einzudämmen und um darlegen zu können, dass die Datenverarbeitung gesetzlich korrekt vonstattengeht, haben sich immer mehr Unternehmen dazu entschieden, eine Datenschutzzertifizierung und damit verbunden ein Datenschutzmanagementsystem (DSMS) zu etablieren.

Für den Aufbau und die Weiterentwicklung eines DSMS investieren die Unternehmen zunehmend Ressourcen. Um jedoch ein DSMS wirtschaftlich betreiben zu können, fehlen oft die Messgrössen, welche festlegen, ob sich die getroffenen Massnahmen und die Investition lohnen.

Gesetzliche Grundlagen

Alle Unternehmen der Schweiz, welche personenbezogene Daten bearbeiten, unabhängig davon, welcher Branche sie angehören, müssen das Datenschutzgesetz der Schweiz aufgrund von Art. 2 DSG beachten.

Dazu gehört auch die Dokumentation der einzelnen Datenbearbeitungen, welche in ihren Grundzügen bereits im heutigen DSG vorhergesehen ist (Art. 11 lit. a DSG – Register der Datensammlungen). Zudem sieht die Gesetzesrevision (E-DSG) eine weitergehende Dokumentationspflicht vor, welche in Zukunft alle Schweizer Unternehmen umsetzen müssen, um eine rechtlich korrekte Datenbearbeitung sicherstellen zu können (vgl. Art. 11 E-DSG – Verzeichnis der Bearbeitungstätigkeiten).

Bereits heute müssen Unternehmen, welche in der Schweiz ansässig sind und gemäss dem Territorialprinzip (Art. 3 – Räumlicher Anwendungsbereich DSGVO) unter die DSGVO fallen weitergehende Dokumentationspflichten nach der DSGVO realisieren (vgl. DSGVO, Art. 30 – Verzeichnis von Verarbeitungstätigkeiten).

Datenschutzreifegrad

Ob internes Audit, Revision oder gar Zertifizierung, ein Problem welches viele Datenschutzbeauftragte oder die Verantwortlichen für das DSMS haben, ist, dass es ihnen schwerfällt, die Wirksamkeit der getroffenen Massnahmen zu messen und die Resultate in einem nachvollziehbaren Format darstellen zu können. Kein in der Schweiz gängiges Datenschutzgütesigel oder Zertifikat bietet seinen Anwendern eine Möglichkeit die Wirksamkeit mit Hilfe von vorgegeben Kriterien zu messen. Es fehlt an standardisierten und etablierten Messgrössen.

Es gibt bereits einige, wenn auch nicht ausschliesslich, auf den Datenschutz ausgerichtete Reifegradmodelle, welche das Thema Datenschutz betrachten und den höheren Reifegradstufen Beachtung schenken.

Ein Reifegrad soll einer Unternehmung grundsätzlich dabei helfen, die Prozesse und deren Output periodisch messbar zu machen. Somit kann sichergestellt werden, dass die Metriken (bspw. KPI (key performance indicator)) der Messung immer gleichbleiben, um so die Messergebnisse über die Zeit hinweg vergleichen zu können.

Die Ursprünge des Reifegradmodells liegen im Bereich der Software-Entwicklung. Dort werden sie eingesetzt, um die Qualität der in einem Unternehmen implementierten Prozesse zu bewerten. Relevante Beispiele für solche Modelle sind CMMI (Capability Maturity Model Integration) und SPICE (Software-Prozess Improvement and Capability Determination). Allgemein beschreiben Reifegradmodelle eine aktuelle Situation mit komplexen Zusammenhängen und sind reduziert auf wesentliche Merkmale. Die Modelle beschreiben den Weg von einem Ist-Zustand zu einem Soll-Zustand mithilfe von definierten Ebenen innerhalb einer bestimmten Dimension.

Die Verwendung von Reifegradmodellen zur Messung von Prozessen ist bereits erprobt und hat sich etabliert. Die Idee dahinter kann nun für die Bestimmung der Wirksamkeit der getroffenen datenschutzrelevanten Massahmen abstrahiert werden, um Auditoren, Revisoren oder der Geschäftsleitung aufzuzeigen, dass sich die Investition in den Datenschutz und das DSMS lohnen.

Erfahrungsgemäss eignen sich KPI gut um die Wirksamkeit periodisch zu messen. Die KPI's gilt es, da sie nicht direkt einer Norm entnommen werden können, für das Unternehmen selbst zu definieren. Als gute Indikatoren gelten beispielsweise der Umsetzungsgrad der notwenigen Dokumentation, die Bearbeitungszeiten von Auskunftsbegehren oder aber die Anzahl von datenschutzrelevanten Vorfällen in der Unternehmung. Diese Aufzählung ist natürlich nur als Denkanstoss gedacht und erhebt keinen Anspruch auf Vollständigkeit.

Eine Grundvoraussetzung der Indikatoren ist dabei, dass sie sich an den vorher definierten Datenschutzzielen orientieren. Diese Ziele sollen von der Geschäftsleitung anhand der Unternehmensstrategie abgeleitet werden, damit die Datenschutzziele die Ziele der gesamten Unternehmung unterstützend abbilden.

Fazit

Zusammenfassend lässt sich sagen, dass es von Vorteil wäre, die Wirksamkeit der getroffenen Massnahmen im Rahmen des Datenschutzes mithilfe eines Datenschutzreifegradmodells messen zu können. Somit würde über die Zeit sichergestellt, dass die Messungen immer mit den gleichen Vorgaben vorgenommen werden. Die Grundlage für eine Vergleichbarkeit über die Zeit hinweg ist so sicherstellt. Dies würde vielen internen Verantwortlichen für den Datenschutz sowie auch den Auditoren und Revisoren, welche die Systeme prüfen, dabei helfen, die getroffenen Massahmen einschätzen zu können. Zudem würde es eine Verhandlungsgrundlage gegenüber der Geschäftsleitung schaffen, um die notwenigen Ressourcen für den Ausbau und die Aufrechterhaltung des DSMS sicherzustellen.