audatis®
Datenschutz und Informationssicherheit | CONSULTING

Whitepaper

Datenschutzmanagement

Inhalt

Zusammenfassung

Mit vollständiger Inkraftsetzung der DS-GVO am 25.05.2018 kam zunehmend auch der Begriff des Datenschutzmanagements, kurz DSMS auf. Diese nur vermeintlich neue gesetzliche Anforderung ergibt sich insbesondere aus den folgenden Normen:

- Art. 5 Abs. 2 DS-GVO: Es besteht die Pflicht dauerhaft zum Nachweis der Einhaltung der Vorschriften der DS-GVO befähigt zu sein.
- Art. 32 Abs. 1 lit. d) DS-GVO: Die Wirksamkeit der initial implementierten technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten muss regelmäßig überprüft, bewertet und evaluiert werden.
- Art. 83 Abs. 2 lit. k) DS-GVO: Ein DSMS kann Im Fall der Verhängung von Sanktionen als mildernder Umstand Berücksichtigung finden.

Ob die Implementierung eines DSMS eine gesetzliche Pflicht darstellt, ist durchaus umstritten. Eine Empfehlung zur Implementierung wird aber ausnahmslos ausgesprochen.

Wer Antworten und Lösungsansätze zu diesen Fragen sucht, wird ebendiese im vorliegenden Whitepaper finden.

Problemstellung

Obwohl das DSMS sinnvollerweise durch ein IT-System unterstützt wird ist es selbst gerade kein IT-System. Vielmehr handelt es sich bei einem DSMS um einen Prozess der kontinuierlichen risikobasierten (Selbst-)Kontrolle und Verbesserung (KVP), die darauf abzielt, das unternehmenseigene Level der Datenschutzcompliance zu erhöhen.

Von dieser Definition ausgehend, stellt sich die Frage nach Aufbau und dem Weg der Implementierung des Datenschutzmanagements im Unternehmen.

Ein Lösungsansatz für die beschriebene Problematik wird im Folgenden skizziert.

Lösungsansatz

Der erste Schritt zur Identifizierung des Ansatzes zu Aufbau und Implementierung eines DSMS ist das Verständnis, dass jedes Managementsystem eine für das individuelle Unternehmen maßgeschneiderte Lösung ist. Der zweite Schritt ist das Verständnis, dass der Datenschutz- und damit das Datenschutzmanagement - vergleichbar der Buchhaltung, dem Qualitätsmanagement und der jährlichen Steuererklärung - gekommen ist, um zu bleiben.

Datenschutzmanagement geht daher über die einmalige Anstrengung der Umsetzung der DS-GVO hinaus. Es strebt vielmehr danach, die Datenschutz-Compliance dauerhaft aufrecht zu erhalten.

Der Aufbau eines DSMS sollte mit der Feststellung beginnen, auf welcher Grundlage aufgebaut werden kann, d.h. welche Managementsysteme schon im Hause existieren.

Verfügt das eigene Unternehmen bereits über Managementsysteme, ist der enge Austausch mit den Verantwortlichen unumgänglich. Jedes zusätzliche Managementsystem verursacht Verwaltungsaufwand und damit Kosten. Ziel sollte es daher stets sein, sich an vorhandenen Strukturen zu orientieren, bestenfalls die Prozesse des Datenschutzes in die bereits vorhandenen Schulungs-, Kommunikations-, Audit- und Berichtsabläufe zu integrieren. Besteht bislang kein Managementsystem und ist ein eigener Aufbau des DSMS daher unumgänglich, so empfiehlt sich schon aus Gründen der Rechtsicherheit die Orientierung an einschlägigen Standards wie bspw. den ISO-Normen 19600, 27001 und 27701 oder de IDW PS 980. Nicht nur ist hierdurch sichergestellt, dass

keine relevanten Punkte übersehen wurden, sondern im Fall der externen Überprüfung des DSMS, wird dies stets gegen einschlägige Standards erfolgen. Das Risiko einer Sanktionierung kann daher durch Orientierung an den bekannten Standards deutlich reduziert werden.

Zugleich sollte die Integrationsfähigkeit bei Auswahl des Standards Berücksichtigung finden, d.h. die Möglichkeit einer Erweiterung der Prozesse des eingerichteten Managementsystems um die Prozesse weiterer Managementsysteme. Die Einrichtung eines spezifischen Datenschutzmanagementsystems, das sich später nur mit Mühe in eine Reihe von Managementsystemen fügt, wird erhöhten Verwaltungsaufwand und damit erhöhte Kosten mit sich bringen.

Der jeweilige Datenschutzbeauftragte sollte somit tunlichst diejenige Norm als Grundlage der Umsetzung wählen, die zum Unternehmen, – sofern vorhanden – der Planung weiterer Managementsysteme und dem im Unternehmen vorhandenen Knowhow, passt.

Das nach dieser Maßgabe eingerichtete Datenschutzmanagementsystem sollte hierbei jedenfalls folgende Elemente aufgreifen:

- **Datenschutz-Kultur:** Die Datenschutzkultur ist die Bedeutung, die den Belangen des Datenschutzes seitens der Mitarbeiter beigemessen wird. Als Kernstück des Datenschutzes im Unternehmen entsteht sie insbesondere aus der Grundeinstellung und den Verhaltensweisen des Managements. Denkbare Maßnahmen sind hier bspw. die Aufnahme des Datenschutzes in den Verhaltenskodex und das Vorleben praktizierten Datenschutzes durch das Management. Auch die Festlegung, Kommunikation und aktive Durchsetzung von Konsequenzen, für die Fälle, wenn der Datenschutz untergraben wird, ist für den Aufbau der Datenschutz-Kultur erforderlich. In der Praxis empfiehlt es sich jedoch die Schwere der Konsequenzen nur sukzessive zu steigern um den Widerstand der Mitarbeitenden einem neuen System folgend zu agieren nicht zu erhöhen.

- **Datenschutz-Ziele:** Das Management des Unternehmens legt die Ziele fest, die mit dem DSMS erreicht werden sollen. Wenn bspw. die vertrauensvolle Beziehung zu Kunden im Mittelpunkt des unternehmerischen Handelns steht, könnte das Ziel des DSMS darin bestehen, den Datenschutz als Werbefaktor einsetzen zu können, um damit im Wettbewerb einen Vorteil zu erlangen. Das Angebot leistungsfähiger, rechtlich und technisch sicherer Lösungen könnte ein mögliches Ziel eines Hosting Anbieters sein. Diese allgemeinen Ziele sollten im nächsten Schritt mit „Leben“, heißt mit konkreten Einzelzielen für einzelne Bereiche, befüllt werden.

- **Datenschutz-Risiken:** Auf Grundlage der Datenschutzziele werden systematisch diejenigen Risiken ermittelt und hinsichtlich ihrer Eintrittswahrscheinlichkeit und Folgen analysiert, die zur Verfehlung der Ziele führen könnten. Besonders wichtig ist es an dieser Stelle, den Kontext der Organisation einzuordnen. Mögliches Risiko eines Hosting Anbieters wäre etwa der Wegfall des US-Privacy-Shields und die sich daraus ergebende Problematik von Datenübermittlungen an (Unter-) Auftragsverarbeiter in den USA.

- **Datenschutz-Programm:** Das Datenschutzprogramm ist die Beschreibung der Grundsätze und Maßnahmen (u.a. Richtlinien, Schulungen, Kommunikation) die der Begrenzung des Risikos und der Verhinderung (künftiger) Verstöße gegen datenschutzrechtliche Vorschriften dienen. Das Datenschutzprogramm eines Hosting Anbieters könnte bspw. die Richtlinien zur Auswahl und zum Einsatz von Auftragsverarbeitern, Schwerpunktschulungen der Mitarbeiter zur Informationssicherheit sowie regelmäßige IT-Schwachstellenanalysen vorsehen.

- **Datenschutz-Organisation:** Die Datenschutzorganisation ist die Festlegung der Aufbau- und Ablauforganisation im DSMS und umfasst die Freigabe der Ressourcen (Zeit, Geld, Personal), die zur Durchführung des Datenschutzprogramms erforderlich sind.

- **Datenschutz-Kommunikation:** Weder Datenschutzziele noch Datenschutzkultur sind ohne Kommunikation über Belange des Datenschutzes im Unternehmen erreichbar. Hier ist die Erstellung eines Kommunikationsplans sinnvoll, der festlegt wie „Update-Kommunikation“ betreffend bspw. neue Richtlinien, Änderungen der Rechtsprechung und aufsichtsbehördliche Auffassungen, „Awareness-Kommunikation“, die darauf abzielt, Akzeptanz und Verständnis der Mitarbeiter für Belange des Datenschutzes zu verbessern, „Reporting-Kommunikation“, und „Ad-hoc-Kommunikation“, d.h. Kommunikation im Fall einer Datenpanne erfolgen sollen.

- **Datenschutz-Überwachung und Verbesserung:** Ohne regelmäßige Überprüfung der Wirksamkeit des implementierten DSMS bleibt dieses zwingend ein Papiertiger. Der Stand des Datenschutzes im Unternehmen muss daher regelmäßig geprüft und im Rahmen der Überprüfung festgestellte Mängel beseitigt werden. Denkbar sind hier etwa jährliche anlasslose sowie quartalsweise Überprüfungen von Risikoschwerpunkten. Auch können Schulungen mit anschließenden Tests auf die Wirksamkeit hin überprüft werden. Stets zu bedenken ist hierbei die Dokumentation der Überprüfung und die Beseitigung ermittelter Mängel.

Kontakt

Jannik Wallbaum

Senior Legal Consultant Datenschutz

Fon: 05221 87292-09 | Fax: 05221 87292-49
E-Mail: j.wallbaum@audatis.de

audatis CONSULTING GmbH

Luisenstraße 1 | 32052 Herford
Fon: 05221 87292-0 | Fax: 05221 87292-49
E-Mail: info@audatis.de
www.audatis.de