„Selbstregulierung“ durch Datenschutzaudit

Die Zertifizierung der in einem Unternehmen umgesetzten Datenschutz- und Datensicherheitsmaßnahmen wird inzwischen immer häufiger angeboten. Grundlage der dazu notwendigen Prüfung ist zumeist ein zuvor festgelegtes Verfahren, welches den entsprechend ausgebildeten Gutachtern dazu dient, die im Unternehmen vorhandenen organisatorischen und technischen Maßnahmen auf ihre datenschutzrechtliche und -sicherheitstechnische Wirksamkeit hin zu überprüfen und ggf. Vorgaben zu machen, wie diese zu verbessern sind. Ist ein vorgegebener Standard erreicht, wird ein entsprechendes Zertifikat verliehen, wobei dessen Geltungsdauer auf einen bestimmten Zeitraum begrenzt ist und die Verlängerung zumeist eine erneute Prüfung erfordert. Dabei gibt es inzwischen eine Vielzahl verschiedener Stellen, die nach eigens hierfür festgelegten Standards eine entsprechende Prüfung anbieten. Die Palette reicht dabei u. a. von Berufsverbänden bis hin zu eigens dafür gegründete Gesellschaften, deren Zuständigkeitsbereich sich inzwischen nicht einmal mehr auf den nationalen Raum beschränkt, sondern zum Teil auch den europäischen Markt abdeckt. Doch der Versuch der Verbesserung des Datenschutzes in Unternehmen durch ein Datenschutzaudit ist nicht wirklich neu. Bereits im Jahre 2001 wurde mit § 9a BDSG eine Vorschrift in das Bundesdatenschutzgesetz aufgenommen, durch welche die Möglichkeit eines Datenschutzaudits ausdrücklich vorgesehen ist. Das hierzu durch § 9a S. 2 BDSG eigens zur Regelung des Verfahrens vorgesehene Datenschutzauditgesetz wurde jedoch nie umgesetzt. Die Gründe für das fehlende Gesetz mögen in diesem Zusammenhang sicherlich vielfältig sein und an Diskussionen zum Thema mangelt es in der Literatur ebenfalls nicht. Inwieweit die nunmehr gegründete Stiftung Datenschutz daran etwas ändern kann bzw. zur Umsetzung eines Datenschutzauditgesetzes beiträgt, mögen dann auch schlicht die Zeit bzw. die nächsten Jahre zeigen. Einen gewissen Bedarf durch entsprechende Zertifikate die Einhaltung eines gesetzlich vorgeschriebenen Datenschutzniveaus nachzuweisen, scheint es jedenfalls zu geben, das zumindest zeigen die zahlreichen Anbieter von Datenschutzaudits.

Das vorliegende Schwerpunktheft greift die in diesem Zusammenhang vielfach auftretenden Fragen auf und versucht zumindest anhand einiger der auf dem Markt zu findenden Zertifizierungsverfahren exemplarisch einen Einstieg in die Thematik zu bieten. Dabei wird keinesfalls der Anspruch der vollständigen Darstellung aller angebotenen Datenschutzaudits erhoben. Vielmehr sollen vorliegende Beiträge zur eigenen Recherche anregen und dazu beitragen dieses Thema auch zukünftig, gerade auch im Zusammenhang mit der europarechtlichen Entwicklung, weiter zu diskutieren.

Durch den ersten Beitrag von Jens Eckhardt und Rudi Kramer wird daher zunächst zum besseren Verständnis ein allgemeiner Einstieg in die Thematik geboten und das gerade im Bereich der Auftragsdatenverarbeitung bestehende Problem der Wahl entsprechender Anbieter auf nationaler und europäischer Ebene rechtlich näher erläutert. Im Anschluss daran hat der Leser die Möglichkeit anhand der Beschreibung einiger verschiedener Zertifizierungsmethoden und –angebote selbst zu beurteilen, inwieweit Datenschutzaudits zur Verbesserung des Datenschutzes beitragen. Durch Kai und Dirk von Lewinski wird dann ein aus der Medizin aufgegriffener Ansatz beschrieben und wissenschaftlich näher erläutert. Am Ende findet sich im Gateway außerdem wieder eine kurze Begriffserläuterung zum Schwerpunktthema.

Es bleibt zu hoffen, dass das Aufgreifen dieser Thematik die zukünftige Diskussion weiter anregt und eventuell irgendwann in einer von § 9a S. 2 BDSG bereits angedachten einheitlichen Regelung mündet.

Britta A. Mester