Britta Alexandra Mester

Datenschutzaudit

Gesetzliche Grundlage

Die Möglichkeit eines Datenschutzaudits ist bereits seit 2001 durch das Bundesdatenschutzgesetz (BDSG) vorgesehen.[1] § 9a BDSG regelt hierzu, dass sowohl Anbieter von Datenverarbeitungssystemen und –programmen als auch datenverarbeitende Stellen eine Prüfung ihrer Datenschutzkonzepte und technischen Einrichtungen vornehmen lassen können. Ziel soll die Verbesserung des Datenschutzes und der Datensicherheit sein, weshalb unabhängige und zugelassene Gutachter die Prüfung und Bewertung vornehmen sollen. Doch obwohl die Vorschrift schon seit einigen Jahren im Gesetz verankert und im Zuge der Novellierung zum Jahr 2009 deren Inhalt nochmals diskutiert wurde, fehlt es bisher an dem nach § 9a S. 2 BDSG das Verfahren, die Bewertung sowie die Zulassung näher regelndem Gesetz.

Zertifizierungsstellen

Obwohl es einen entsprechenden Entwurf eines Bundesdatenschutzauditgesetzes (BDSAuditG) gibt[2], handelt es sich also mangels gesetzlicher Grundlage bei den von verschiedener Seite angebotenen Audits, nicht um das nach § 9a BDSG ursprünglich geforderte Datenschutzaudit. Eine von der Bundesregierung u.a. für die Förderung von entsprechenden Maßnahmen zur Umsetzung eines Audits geplante Stiftung Datenschutz[3] ist als öffentlich-rechtliche Einrichtung erst nach mehreren Jahren der Diskussion im Jahr 2013 gegründet worden.[4] Dennoch gibt es inzwischen eine Vielzahl anderer Stellen, die die Möglichkeit der Zertifizierung durch unabhängige Auditoren vorsehen und sich dabei nicht zuletzt am Entwurf des Datenschutzauditgesetzes orientieren. So bieten sowohl Berufsverbände[5] als auch diverse andere Einrichtungen[6] eigene Prüfverfahren und Zertifikate an.[7] Selbst auf europäischer Ebene sind Bestrebungen zur Vereinheitlichung entsprechender Verfahren zu verzeichnen und nehmen teilweise bereits konkret Gestalt an.[8]

Verfahren und Siegel

Gemeinsam ist allen Prüfverfahren, dass anhand vorformulierter Prüfungsschritte durch zuvor geschulte und ausgebildete Auditoren die bei den geprüften Unternehmen vorhandenen datenschutzrechtlichen und sicherheitstechnischen Voraussetzungen begutachtet und dann bei Erfüllen der verlangten und geprüften Kriterien ein entsprechendes Siegel verliehen wird, wobei die Zeiten für die Gültigkeit des Zertifikats wiederum variieren können. Außenstehenden (potentiellen Kunden oder Vertragsparteien, insbesondere Auftraggebern) soll damit die Prüfung der Einhaltung datenschutzrechtlicher Vorgaben vereinfacht und den zertifizierten Unternehmen die Außendarstellung der Einhaltung datenschutzrechtlicher Vorgaben erleichtert werden. Zur Nachvollziehbarkeit der angesetzten Kriterien finden sich die Prüfkataloge zumeist im Internet veröffentlicht. Insbesondere im Bereich der Auftragsdatenverarbeitung nach § 11 BDSG soll damit sowohl dem Auftragnehmer als auch dem Auftraggeber eine Entscheidungshilfe geboten und die Prüfung der Einhaltung vorgegebener Datenschutzpflichten vereinfacht werden. Inwieweit damit wirklich ein Wettbewerbsvorteil, so aber schon Ziel des § 9a BDSG, und eine Werbewirksamkeit nach Außen erreicht werden, muss dann allerdings das jeweilige Unternehmen selbst entscheiden.[9]

Internationale Ansätze

Während die EG-Datenschutzrichtlinie[10] ein entsprechendes Verfahren noch nicht vorsieht, findet sich im Entwurf der EU-Datenschutzgrundverordnung[11] bereits eine Verpflichtung, entsprechende Verfahren sicherzustellen, wobei konkrete Regelungen noch ausstehen (vgl. Art. 22 Abs. 4 EU-DS-GVO).[12] Darüber hinaus kennen auch andere Länder Möglichkeiten der Auditierung, so zum Beispiel die USA.[13]

1 Vgl. dazu aber auch schon *Bachmeier*, DuD 1996, S. 680.

2 Siehe zu den Regelungsinhalten bei *Schultze-Melling*, in: Taeger/Gabel, BDSG, 2. Aufl., Frankfurt a.M. 2013, § 9a Rn. 11 ff.

3 Vgl. http://stiftungdatenschutz.org (letzter Abruf: 16.1.2014).

4 Zur Diskussion s. *Schultze-Melling*, in: Taeger/Gabel, BDSG, 2. Aufl., Frankfurt a.M. 2013, § 9a Rn. 10; zur Kritik vgl. u.a. unter http://www.bundestag.de/dokumente/textarchiv/2013/43341654_kw12_pa_neue_medien/ (letzter Abruf: 16.1.2014).

5 Zum Beispiel der BvD und die GDD (DS-BvD-GDD-01), dazu *Staub* in diesem Heft 3/2014.

6 Siehe bspw. unter http://www.tuev-sued.de/unser_pruefzeichenkatalog (letzter Abruf: 16.1.2014).

7 Bspw. schon seit einigen Jahren eine öffentlich-rechtliche Zertifizierung auf Basis von Privatgutachten bietet das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD), dazu näher unter www.datenschutzzentrum.de/gütesiegel/index.htm (letzter Abruf: 16.1.2014).

8 Bspw. in Form des „European Privacy Seal" (EuroPriSe), hierzu weitere Informationen unter www.european-privacy-seal.eu/ (letzter Abruf: 16.1.2014) oder bei *Meissner*, DuD 2008, S. 525 und in diesem Heft 3/2014.

9 Kritisch mit w.Nw. siehe *Schultze-Melling*, in: Taeger/Gabel, BDSG, 2. Aufl., Frankfurt a.M. 2013, § 9a Rn. 6.

10 Richtlinie 95/46/EG (Datenschutzrichtlinie), abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:de:html (letzter Abruf: 29.1.2014).

11 Entwurf abrufbar unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:DE:HTML (letzter Abruf: 29.1.2014).

12 Zur rechtlichen Unterscheidung vgl. auch *Mester*, DuD 2012, S. 603; *Mester*, DuD 2013, S. 250; zur Kritik *Eckhardt/Kramer/Mester*, DuD 2012, S. 623 ff.

13 Dazu und auch zur Kritik vgl. bei *Grimm/Roßnagel*, DuD 2000, S. 446 (449).