Freie Hansestadt Bremen

Bremische Datenschutzauditverordnung (BremDSAuditV)

Inkrafttreten: 28.12.2009
Zuletzt geändert durch: zuletzt geändert durch Artikel 1 des Gesetzes vom 24.11.2009 (Brem.GBl. S. 535)
Fundstelle: Brem.GBl. 2004, 515
Gliederungsnummer: 206-a-2

Auf Grund des § 7b Abs. 1 Satz 2 des Bremischen Datenschutzgesetzes in der Fassung der Bekanntmachung vom 4. März 2003 (Brem.GBl. S. 85 - 206-a-1) verordnet der Senat:

§ 1
Auditverfahren

(1) Öffentliche Stellen im Sinne des § 1 Abs. 2 des Bremischen Datenschutzgesetzes können Verfahren einschließlich der dazugehörigen technischen Einrichtungen zum Zwecke der Verbesserung des Datenschutzes und der Datensicherheit prüfen und bewerten lassen (Datenschutzaudit).

(2) Ein Verfahren im Sinne von Absatz 1 ist der innerhalb einer festgelegten technisch-organisatorischen Einsatzumgebung auf Wiederholung angelegte, nicht nur untergeordnete Prozess der Verarbeitung personenbezogener Daten. Das Datenschutzaudit kann sich auf alle Verfahren der öffentlichen Stelle oder eines ihrer abgrenzbaren Teilbereiche erstrecken.

(3) Die Prüfung und Bewertung wird durch einen Auditor vorgenommen, der auf Vorschlag der öffentlichen Stelle zur Wahrnehmung dieser Aufgabe vom Landesbeauftragten für den Datenschutz zugelassen wurde. Zugelassen wird nur, wer seine fachliche Eignung, persönliche Zuverlässigkeit und Unabhängigkeit für die Tätigkeit als Auditor nachweist. Diesen Nachweis erbringt in der Regel auch, wer zu einem vergleichbaren Audit im Bund, in einem anderen Land, in einem anderen Mitgliedsstaat der Europäischen Union oder der anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum zugelassen wurde.

§ 2
Ablauf des Datenschutzaudits

(1) Das Datenschutzaudit bedarf einer schriftlichen Vereinbarung der öffentlichen Stelle mit dem Auditor, in der Art und Umfang des zu auditierenden Verfahrens sowie der Ablauf des Auditverfahrens festzulegen sind. Es kann von der öffentlichen Stelle jederzeit beendet werden. Erstreckt sich das zu auditierende Verfahren auf mehrere öffentliche Stellen, ist die Zustimmung aller beteiligten öffentlichen Stellen erforderlich.

(2) Die öffentliche Stelle legt für das zu auditierende Verfahren einen schriftlichen Datenschutzplan vor, in dem sie den bisher erreichten Stand des Datenschutzes und der Datensicherheit darlegt (§ 3), die zu erreichenden Ziele bestimmt (§ 4) und ein Datenschutzmanagementsystem (§ 5) vorsieht. Sie wird hierbei vom Auditor beraten und unterstützt.

§ 3
Stand von Datenschutz und Datensicherheit

Der Stand von Datenschutz und Datensicherheit wird anhand der für eine Verfahrensbeschreibung nach § 8 Abs. 1 des Bremischen Datenschutzgesetzes erforderlichen Feststellungen ermittelt.

§ 4
Ziele und Maßnahmen

(1) Die öffentliche Stelle legt die zu erreichenden Ziele des Datenschutzes und der Datensicherheit fest. Sie hat sich hierbei zu verpflichten, unter Beachtung der Verhältnismäßigkeit von Aufwand und Nutzen den Stand der Technik einzuhalten und die zur Erreichung dieser Ziele erforderlichen konkreten technischen und organisatorischen Maßnahmen vorzusehen; der Zeitrahmen zur Verwirklichung der Ziele und Maßnahmen ist anzugeben. Stand der Technik ist der Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der die praktische Eignung einer Maßnahme zum Datenschutz und zur Datensicherheit gesichert erscheinen lässt.

(2) Die festgelegten Ziele und die zu ihrer Verwirklichung vorgesehenen Maßnahmen müssen in besonderer Weise den Geboten der Datenvermeidung und der Datensparsamkeit Rechnung tragen.

§ 5
Datenschutzmanagementsystem

(1) Die öffentliche Stelle richtet ein Datenschutzmanagementsystem ein, welches die Verwirklichung der Ziele und Maßnahmen gemäß § 4 sicherstellt.

(2) Das Datenschutzmanagementsystem beschreibt die datenschutzrechtliche und datensicherheitstechnische Organisation der Datenverarbeitung einschließlich der Bestimmung von Zuständigkeiten, Arbeitsabläufen und Verhaltensweisen in Bezug auf das auditierte Verfahren. Es legt fest, in welcher Weise die Verwirklichung von Zielen und Maßnahmen gemäß § 4 überwacht und der jeweilige Stand dokumentiert wird.

§ 6
Begutachtung

(1) Der Auditor prüft den Datenschutzplan auf Vollständigkeit und Schlüssigkeit. Er erstellt hierüber ein Gutachten, das eine Bewertung des Datenschutzes und der Datensicherheit des auditierten Verfahrens enthält. Ihm sind Gelegenheit zur Besichtigung des Verfahrens und die für eine Bewertung erforderlichen Auskünfte zu geben.

(2) Werden vom Auditor Mängel festgestellt, die eine Erteilung des Gütesiegels verhindern, so ist der öffentlichen Stelle vor Fertigstellung des Gutachtens Gelegenheit zur Stellungnahme und zur Behebung der Mängel zu geben.

§ 7
Bremisches Datenschutzaudit-Gütesiegel

(1) Bestätigt der Auditor die Vollständigkeit und Schlüssigkeit des Datenschutzplans, so ist die öffentliche Stelle für einen Zeitraum von zwei Jahren berechtigt, das Bremische Datenschutzaudit-Gütesiegel für das auditierte Verfahren zu verwenden. Nach Ablauf dieses Zeitraums ist ein erneutes Audit erforderlich, welches in Umfang und Ausmaß verkürzt werden kann, soweit keine wesentlichen Veränderungen eingetreten sind.

(2) Die Gestaltung des Bremischen Datenschutzaudit-Gütesiegels richtet sich nach der Anlage.

§ 8
Beteiligung des behördlichen Datenschutzbeauftragten

Der behördliche Datenschutzbeauftragte soll in das Datenschutzaudit einbezogen werden.

§ 9
Berichterstattung

Der Senator für Justiz und Verfassung berichtet dem Senat bis zum 31. März 2008 über die Erfahrungen mit dieser Verordnung sowie ihre Auswirkungen in der Praxis.

§ 10
In-Kraft-Treten, Außer-Kraft-Treten

Diese Verordnung tritt am Tage nach ihrer Verkündung in Kraft. Sie tritt mit Ablauf des 31. Dezember 2014 außer Kraft.

Beschlossen, Bremen, den 5. Oktober 2004

Der Senat

Anlage

(zu § 7 Abs. 2)

Bremisches Datenschutzaudit-Gütesiegel