
HOFFMANN
LIEBS
FRITSCH
& PARTNER
Rechtsberatung
für Unternehmen
www.hlfp.de

Durchbruch für das Datenschutzaudit?

Vortrag anlässlich der Konferenz Sicherheit 2008 der Gesellschaft für Informatik e.V. in Saarbrücken am 3. April 2008

§ 9a Datenschutzaudit

Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutz-konzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt.

Gesetzentwurf der Bundesregierung für ein Bundesdatenschutzauditgesetz

§ 1 Datenschutzaudit

(1) Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen können auf Antrag ihr Datenschutzkonzept sowie ihre technischen Einrichtungen auf Vereinbarkeit mit den Vorschriften über den Datenschutz prüfen und bewerten lassen (Datenschutzaudit).

Gesetzentwurf der Bundesregierung für ein Bundesdatenschutzauditgesetz

(2) Vorschriften über den Datenschutz im Sinne dieses Gesetzes sind solche, die die automatisierte Verarbeitung personenbezogener Daten oder die Verarbeitung oder Nutzung personenbezogener Daten in oder aus nicht automatisierten Daten regeln, einschließlich des Rechts der Mitgliederstaaten der Europäischen Union in den Fällen des § 1 Abs. 4 Bundesdatenschutzgesetzes.

(3) Die Bewertung nach Absatz 1 erstreckt sich nicht auf die Sicherheit informationstechnischer Systeme und informationstechnischer Komponenten.

Gesetzentwurf der Bundesregierung für ein Bundesdatenschutzauditgesetz

§ 2 Sachverständige

(1) Das Datenschutzaudit wird durch Sachverständige durchgeführt, die von der Datenschutzaufsichtsbehörde des Landes öffentlich bestellt sind, in dem sie eine Haupt- oder Zweigniederlassung haben. Die Bestellung eines Sachverständigen in mehreren Ländern ist zulässig.

(2) Der Antrag auf Durchführung eines Datenschutzaudits kann bei jedem Sachverständigen gestellt werden, der von der Datenschutzaufsichtsbehörde des Landes bestellt ist, in dem der Antragsteller eine Niederlassung hat. Ausländische Antragsteller können den Antrag bei jedem Sachverständigen stellen.

Gesetzentwurf der Bundesregierung für ein Bundesdatenschutzauditgesetz

§ 3 Zertifikat, Datenschutzauditsiegel

(1) Über die Vereinbarkeit eines Datenschutzkonzepts oder einer technischen Einrichtung mit den Vorschriften über den Datenschutz stellt der Sachverständige ein Zertifikat aus.

(2) Zertifizierte Datenschutzkonzepte und zertifizierte technische Einrichtungen dürfen mit einem Datenschutzauditsiegel so lange gekennzeichnet werden, wie sie gegenüber der zertifizierten Version unverändert sind, längstens jedoch zwei Jahre. Der Antragsteller ist verpflichtet, dem Bundesbeauftragten für den Datenschutz und der Informationsfreiheit Veränderungen der zertifizierten Version anzuzeigen. Der Sachverständige weist ihn darauf in dem Zertifikat hin.

Gesetzentwurf der Bundesregierung für ein Bundesdatenschutzauditgesetz

(3) Der Sachverständige unterrichtet den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit über ausgestellte Zertifikate und bezeichnet dabei das zertifizierte Datenschutzkonzept oder die zertifizierte technische Einrichtung, den Namen und die Anschrift des Antragstellers, sowie die Dauer, für die Kennzeichnung mit dem Datenschutzauditsiegel längstens zulässig ist.

(4) Ist die Zertifizierung bestandskräftig abgelehnt worden, weil das Datenschutzkonzept oder die technische Einrichtung mit den Vorschriften über den Datenschutz unvereinbar ist, kann ein erneuter Antrag erst gestellt werden, wenn das Datenschutzkonzept oder die technische Einrichtung gegenüber der auditierten Version verändert ist.

Welche Fragen sind für die praktische Durchführung eines Datenschutzaudits aus Sicht eines Unternehmens zu beantworten:

1. Wer darf ein solches Datenschutzaudit bei sich durchführen lassen? Wer also sind die Anbieter von DV-Systemen und DV-Programmen sowie datenverarbeitende Stellen?

2. Welche Kriterien werden geprüft und welches Unternehmen muss welche Kriterien erfüllen?

3. Keine Prüfung der Sicherheit informationstechnischer Systeme und informationstechnischer Komponenten?

Verfügbarkeitskontrolle nach § 9 Satz 1 Nr. 7 BDSG:

Öffentliche und nicht-öffentliche Stellen haben die Pflicht zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung und Verlust geschützt sind.

4. Wer sind die Sachverständigen, die das Datenschutzaudit durchführen, und welche fachlichen und sachlichen Qualifikationen besitzen sie bzw. müssen sie aufweisen?

Diese Fragen werden mit dem Gesetzentwurf **nicht** beantwortet.

Zur Erinnerung:

„Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt.“ (§ 9a Satz 2 BDSG)

Vielen Dank für Ihre Aufmerksamkeit!


HOFFMANN
LIEBS
FRITSCH
& PARTNER
Rechtsberatung
für Unternehmen
www.hlfp.de