Daten & Recht

Datenschutzaudits und -zertifizierungen

Rechtsanwalt Norman Bäuerle

AK IT-Recht | 15.09.2015

Infos & Links zum Vortrag: https://datenundrecht.com/?p=691

Inhaltsübersicht

- Arten von Datenschutzaudits
- Nutzen, Probleme und Regelungsversuche
- Anforderungen an Zertifizierungsdienste
- Datenschutz(güte)siegel
- Datenschutzmanagement
- Datenschutzbestandsaufnahme
- "Kurzaudits"
- RA als Datenschutzgutachter

	Produktaudit	Verfahrensaudit, Systemaudit
Adressatengruppe	Anbieter von Datenverarbeitungs-systemen und -programmen	Datenverarbeitende Stellen
Gegenstandsbereich	Technischen Einrichtungen	• Datenschutzkonzept • Datenschutzmanagementsystem • Einzelne/mehrere Verfahren
Eigenschaften	• Datenvermeidung und Datensparsamkeit • Transparenz • Datensicherheit • Revisionsfähigkeit • Gewährleistung der Betroffenenrechte	• Erfüllung der Anforderungen des Datenschutzrechts und • angestrebter Verbesserungen (Datenschutzziele)
Prüfung	statisch und objektbezogen	struktur- und prozessbezogen
Datenschutzsiegel	• Datenschutz-Gütesiegel beim ULD • European Privacy Seal, EuroPriSe	Datenschutzsiegel basierend auf dem Standard „DS-BvD-GDD-01“

Interne und externe Audits

Unternehmensinterne Audits

- Prüfung der Datenschutzorganisation
- Bestandteil des Risikomanagements oder der Compliance-Strategie
- Adressaten:
  - Geschäftsführung
  - Leitung IT

Zertifizierungsaudits

- Verfahrens- und Produktaudits
- Datenschutzsiegel und -zertifizierungen
- Adressaten:
  - Interne
  - Kunden/Auftraggeber
  - Datenschutzaufsichtsbehörden

Kriterien für Datenschutzaudits

Einhalten gesetzlicher Vorgaben

- Reaktion auf Vollzugsdefizit im Datenschutz
- Maßstab bereits vorhanden und bekannt

Besondere Datenschutzfreundlichkeit

- kontinuierliche und flexible Verbesserung des Datenschutzes durch Förderung von datenschutzfreundlichen Technologien und Best Practices
- Formulierung von Standards, die über die gesetzlichen Vorgaben hinausgehen

Nutzen von Datenschutzaudits

Bisherige Durchsetzung

- ordnungsrechtlicher Ansatz
- nachträgliche Kritik oder die Sanktionierung durch die Datenschutzaufsichtsbehörden
- wenig Datenschutztransparenz
- Defizite in der Einhaltung des geltenden Datenschutzrechts

Datenschutzsiegel und -zertifizierungen

- Selbstregulierung und Wettbewerbs
- präventive Wirkung
- Werbeargument und Wettbewerbsfaktor
- Mobilisierung des legitimen Eigennutzes, um dadurch Beiträge zur Verwirklichung von Gemeinwohlzielen hervorzubringen
- Vermeidung von „Audittourismus“

Probleme

- Kein (besonderes) Vertrauen in die Zertifizierungsdienste und Gutachter
- Keine offenen Prüfstandards (Prüfungsumfang und -tiefe), sodass die erforderliche Transparenz und Vergleichbarkeit der Verfahren und der Prüfkriterien fehlt
  - selbst gewählte Bewertungskriterien
  - selbst bestimmtes Auditverfahren
  - Eigenvornahme der Bewertung

Regelungsversuche

- Programmnorm § 9a BDSG (Novellierung des BDSG 2001)
  - Audit des Datenschutzkonzept und technischen Einrichtungen
  - Erforderliches Ausführungsgesetz – Datenschutzauditgesetz – zuletzt 2009 gescheitert
- Art. 39 DS-GVO Zertifizierung
- § 2 Abs. 1 Satzung der Stiftung Datenschutz
  „Zweck der Stiftung ist es, die Belange des Datenschutzes insbesondere durch die Entwicklung eines Datenschutzaudits sowie eines Datenschutzauditverfahrens [...] zu fördern."

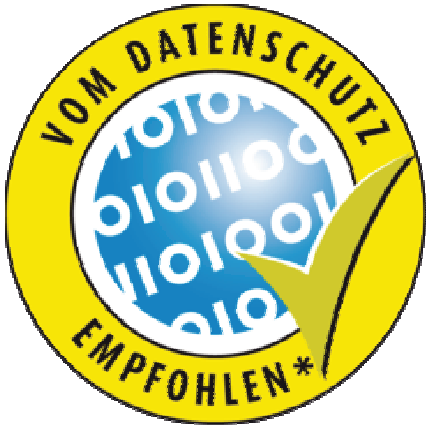
Anforderungen an Zertifizierungsdienste (1)

- Beschluss des Düsseldorfer Kreises am 25./26. Februar 2014:
  - Prüffähige Standards, die von den Aufsichtsbehörden befürwortet werden, zu entwickeln, zu veröffentlichen und zur Nutzung für Dritte freizugeben,
  - beim Zertifizierungsprozess zwischen verschiedenen Ebenen zu unterscheiden (Prüfung, Zertifizierung, Akkreditierung),
  - für verschiedene auf Ebenen und/oder in Verfahrensabschnitten anfallende Aufgaben voneinander abzugrenzende Rollen der jeweils Mitwirkenden vorzusehen,
  - Regelungen zur Vermeidung von Interessenkollisionen der an einem Zertifizierungsprozess Beteiligten zu treffen,

Anforderungen an Zertifizierungsdienste (2)

- Beschluss des Düsseldorfer Kreises am 25./26. Februar 2014:
  - Anforderungen an die Eignung als Prüferin und Prüfer festzulegen und diesen Personenkreis für Zertifizierungen zu qualifizieren,
  - den geprüften Sachbereich so zu umschreiben, dass Bürgerinnen und Bürger, Kundinnen und Kunden die Reichweite der Prüfaussage ohne weiteres dem Zertifikat entnehmen können,
  - Bedingungen für Erteilung, Geltungsdauer und Entzug von Zertifikaten zu bestimmen,
  - Zertifikate zusammen mit den wesentlichen Ergebnissen der Prüfberichte zu veröffentlichen.

Datenschutz(güte)siegel



Übersicht der Stiftung Datenschutz mit 35 Anbietern
https://stiftungdatenschutz.org/zertifizierungsubersicht/

Datenschutzmanagementsystem

- … stellt die interne Organisation der datenverarbeitenden Stelle im Hinblick auf die Einhaltung der datenschutzrechtlichen und sicherheitstechnischen Vorgaben dar.
- Es ist die Gesamtheit aus **Zuständigkeiten**, **vorgeschriebenen Verhaltensweisen** und **Abläufen sowie sächlichen Mitteln**, die zur Erreichung der im Datenschutzkonzept festgelegten Datenschutzziele erforderlich sind.
- **Ziel:** Die verantwortliche Stelle soll in der Lage sein, eine systematische Planungs-, Kontroll-, Eingreif- und Unterstützungsfunktion über die eigene Datenschutzkonformität selbst auszuüben.

Datenschutzkonzept

- Zweckbestimmung des Verfahrens
- einzuhaltende Rechtsvorschriften
- zu verarbeitende Datenkategorien
- betroffene Personengruppen
- Phasen der Datenverarbeitung, insbesondere vorgesehene Übermittlungen
- eingesetzte Hard- und Software
- Aufbau der Datenverarbeitungssysteme
- Darstellung der Einhaltung der materiellen Zulässigkeitsvoraussetzungen
- Informationspflichten und der Rechte der Betroffenen

Sicherheitskonzept

- Risikoanalyse
- Schutzzweckbeschreibung
- Beschreibung der Maßnahmen zum technisch-organisatorischen Datenschutz und zur Gewährleistung der informationstechnischen Sicherheit
- Beschreibung und Bewertung der verbleibenden Restrisiken umfasst

Revision

Festlegung von Maßnahmen zur systematischen Überprüfung der Umsetzung der Datenschutzziele (Revision):

- Zuständigkeiten
  - Verantwortlichkeit für die Durchführung der Revision und
  - welcher Stelle ist
  - in welchen Zeitintervallen der erreichte Zustand zu berichten (Eskalation)
- Prüfverfahren
- Dokumentation des durch die Maßnahmen jeweils erreichten Zustandes

Datenschutz Soll-Analyse

Ist-Analyse

Datenschutzdokumentation		
8.	Datenschutzkonzepte • allgemein • anwendungsspezifisch	
9.	Informationssicherheitskonzept, insbesondere • Berechtigungskonzept/Liste der Zugriffsberechtigungen • Sicherungskonzept (Backup) • Passwortrichtlinie • Notfallkonzept	
10.	Verfahrensverzeichnisse	

Tabelle 3: IT-Systeme

1.2.3 Outsourcing

#	Frage	Antwort
1.	Outsourcing einschließlich Shared Services: • Lohn- und Gehaltsabrechnung • Finanzbuchhaltung • Externe Personalagentur	

Bericht

#	Feststellung	Risikobewertung	Empfehlung
1.			
2.			
3.			

„Gesetzestext-Audit“

- §§ 3-11, 28, 32-35,42a BDSG
- §§ 5, 6, 13-15a TMG
- §§ 88, 99 TKG

RA als Datenschutzgutachter

- Aus- und Fortbildung Datenschutz
- Trennung freiberufliche und gewerbliche Tätigkeit
- Vermögensschadens-Haftpflichtversicherung
- Akkreditierung als Gutachter
- Aufbau eines Netzwerks, z. B. technische Experten

Infos & Links zum Vortrag: https://datenundrecht.com/?p=691

Rechtsanwalt Norman Bäuerle

IT-Recht | Compliance | Datenschutz

Schloßstraße 41A

12165 Berlin

baeuerle@datenundrecht.com

+49 30 577055240