Betrieblicher Datenschutz

Dr. Thilo Weichert
Leiter des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein (ULD)

Kreishandwerkerschaft
Heide, 6. Oktober 2011

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Inhalt

- Unabhängiges Landeszentrum für Datenschutz (ULD)
- Aktuelle Datenschutzthemen
- Schwerpunkte des DS in der Wirtschaft
- Vorgehen bei Eingaben und Kontrollen
- Bundesdatenschutzgesetz und Novellen
- Technische Sicherungsmaßnahmen,
- Datenschutzmanagement
- Verbraucherdatenschutz
- Arbeitnehmerdatenschutz
- Perspektiven

Unabhängiges Landeszentrum für Datenschutz I

- Datenschutzaufsichtsbehörde für den öffentlichen (Behörden) und den nicht-öffentlichen (Wirtschaft) Bereich
- Ordnungswidrigkeitenbehörde nach BDSG
- Beratung von Bürger, Politik, Verwaltung, Wirtschaft
- Aus- und Fortbildung (Datenschutzakademie SH)
- Öffentlichkeitsarbeit, u.a. www.datenschutz.de (virDSB)
- Erstellung von Gutachten (z.B. Scoring, KBS, Kfz-Händer-Netz, RFID, Biometrie, DRM)
- Datenschutz-Audit und -Gütesiegel (SH, EuroPriSe)
- Projekte Forschung und Entwicklung (ID-Management, Sicherheitstechnik, Biobanken, Cloud Computing)

Unabhängiges Landeszentrum für Datenschutz II

Organisation
Ref. 1 Leitung, Service, Personal, Presse, Landtag
Ref. 2 Medizin, Soziales, Informationsfreiheit, Allgemeine Verwaltung, Kommunen, SteuerR, Bildung, Statistik, MeldeR, PersonalR, Umwelt und Planung
Ref. 3 Datensicherheit (technischer Datenschutz) ULD-Systemadministration
Ref. 4 Wirtschaft, Neue Medien
Ref. 5 Justiz, Verfassungsschutz, Polizei
Ref. 6 Projekte – ULD-i
Ref. 7 Datenschutz-Gütesiegel, -Audit

Aktuelle Datenschutzthemen

- Facebook
- Google Street View, Bing Street Side
- Unternehmensdatenverluste, z. B. Sony mit ca. 100 Mio. Datensätzen
- ELENA
- Vorratsdatenspeicherung
- Diskussionen über
  Rotes-Linien-Gesetz (Datenschutz im Internet)
  Gesetz zum Beschäftigtendatenschutz
  „Stiftung Datenschutz“

Schwerpunkte des DS in der Wirtschaft

Videoüberwachung
Banken und Finanzdienstleister (Scoring, SWIFT)
Versicherungen
Internet-Wirtschaft (E-Commerce, Spam, Pranger)
Telemediendienste
Arbeitnehmer-Überwachung
Wohnungswirtschaft
Handel (E-Cash, Kundenbindung, Werbung)
Auskunfteien
Inkasso
Vereine
ambulante und stationäre Medizin (Ref. 2)
  Datensicherheit (Ref. 3)
  Audit – Gütesiegel (Ref. 7)
  Betroffenenrechte (in allen Bereichen)

Vorgehen bei Eingaben

Beschwerde einer Petentin bzw. eines Petenten
Aufforderung der verantwortlichen Stelle um Stellungnahme
- Sachverhaltsdarstellung und präzise Fragen
- Hinweis auf Zuständigkeit und Zeugnisverweigerungrecht
Akteneinsicht in Petition nur nach Zustimmung (Petentengeh.)
evtl. Mahnung mit Fristsetzung und Bußgeldandrohung mit ZU
evtl. Prüfung vor Ort
rechtliche Bewertung des Sachverhaltes > evtl. Beanstandung
Mitteilung des Ergebnisses an Petentin bzw. Petenten
selten: Bußgeldverfahren wegen materiellem Verstoß
sehr selten: Nennung in Presseerklärung oder
Tätigkeitsbericht

Vorgehen bei Kontrollen

regelmäßig Ankündigung
regelmäßig Vieraugenprinzip (rechtlich – technisch)
formelle Prüfung
- betrieblicher Datenschutzbeauftragter (bDSB)
- Verfahrensverzeichnis
- Vorabkontrollen

materiell-rechtliche Prüfung (Schwerpunkt)
- Erhebung, Speicherung, Auswertung, Nutzung, Übermittlung

technische Prüfung (TOM § 9 BDSG)
evtl. Beanstandung
bei Uneinsichtigkeit i.d.R. Bußgeld, evtl. Anordnung (Untersagung, bDSB)
bei „großen Fällen“ öffentliche Bekanntgabe

Bundesdatenschutzgesetz

Zulässigkeit der Datenverarbeitung

- Durchführung eines Vertrages (§ 28 I Nr. 1)
- Einwilligung des Betroffenen (freiwillig, schriftlich) (§ 4a)
- Spezialgesetzliche Regelungen (AO, HGB, SGB V (Kranken), SGB VI (Renten), SGB VII (Unfall)
- Allgemeine Verarbeitungsbefugnis (§ 28 I Nr. 2: Abwägung berechtigtes Interesse – schutzwürdiges Interesse)
- Spezialproblem: Übermittlung ins Ausland (§§ 4b, 4c)

Allgemeine Grundsätze

- Erforderlichkeitsgrundsatz
- Datensparsamkeit (Pseudonymisierung-Anonymisierung)
- Zweckbindung

BDSG-Novellen 2009

- Mehr Transparenz bei Scoring und Bonitätsprüfung
- Neuregelung des Adresshandels und des Direktmarketing (keine Abschaffung des „Listenprivilegs“)
- (beschränktes) Koppelungsverbot
- Benachrichtigungspflicht bei DS-Verstößen
- Outsourcing, Datenkennzeichnung und Protokollierung
- Datenschutzauditgesetz (gescheitert)

Technische Sicherungsmaßnahmen

Technisch-organisatorische Maßnahmen der Datensicherheit intern und im offenen Netz (§ 9)

- Vertraulichkeit (z.B. Verschlüsselung)
- Integrität (Backup)
- Verfügbarkeit (ausfallsichere Stromversorgung, Datenmanagement)
- Authentizität (Aktenführung, digitale Signatur)
- Revisionsfähigkeit, Transparenz (Protokollierung, Kontrolle der SysAdmin, Dokumentation, Anwenderhandbücher, Information bei Erhebung, Benachrichtigung bei Bearbeitung)

Datenschutzmanagement

verpflichtend

- Betrieblicher Datenschutzbeauftragter (§§ 4f, 4g: ab 9 Personen in ADV, sonst ab 20 Personen)
- Vorabkontrolle (§ 4d V)
- Verfahrensverzeichnis (§§ 4d, 4e)
- Verpflichtung auf das Datengeheimnis (§ 5)

zu empfehlen

- Datenschutzkonzept
- IT-Sicherheitskonzept
- Konzept bei IT-Einführungen (incl. Betriebsrat)
- Ausbildungskonzept
- Beschwerdemanagement (Betroffeneneingaben)
- Durchführung von Audits

Verbraucherdatenschutz

Kooperation ULD mit VZ SH und vzbv

rechtlicher Schutz

- Betroffenenrechte (incl. Auskunft, Widerspruch)
- materielle Zulässigkeit
- Datensparsamkeit (Anonymisierung, Pseudonymisieurng)
- Koppelungsverbot
- Formular- u. AGB-Kontrolle

technischer Schutz

- Virenschutz
- Firewall
- Verschlüsselung
- Spam-Abwehr
- Anonymisierungsdienste

Arbeitnehmerdatenschutz

- Einstellung
- Personalaktenführung
- Gesundheitskontrolle
- Arbeitskontrolle

- Zugangskontrolle (Ausweise, Biometrie)
- E-Mail- und Internetüberwachung am Büroarbeitsplatz
- Technische Überwachung in Produktion und Service (RFID, Fraud-Prevention)
- Videoüberwachung
- Lokalisierungsdienste

Perspektiven

- Verabschiedung eines Gesetzes zum Beschäftigtendatenschutz
- Einrichtung einer „Stiftung Datenschutz“
- Neuregelung des Internet-Datenschutzes (u.a. Umsetzung Einwilligung zu Cookies)
- Kündigung des Safe-Harbor-Abkommens zwischen EU und USA
- Diskussionen über einheitlichen europäischen Datenschutz (Europäische Datenschutzverordnung?)
- Globale Festlegung von Datenschutzstandards

Betrieblicher Datenschutz

Dr. Thilo Weichert
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)
Independent Center for Privacy Protection Schleswig-Holstein (ICPP)
Holstenstr. 98, D- 24103 Kiel
mail@datenschutzzentrum.de
https://www.datenschutzzentrum.de