EUROFORUM
Quality in Business Information

14. Datenschutz kongress 2013

Internetauftritt von Unternehmen datenschutzkonform gestalten

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

Euroforum, 14. Datenschutzkongress 2013
Berlin 15.05.2013

EUROFORUM
Quality in Business Information

14. Datenschutz kongress 2013

Inhalt

- Rechtsgrundlagen
- Transparenz
- Wahlfreiheit
- Verantwortlichkeit
- Datenarten
- Technisch-organisatorische Maßnahmen

Rechtsgrundlagen

Telemediengesetz (TMG) > Transparenz, Bestands- u. Nutzungs-daten

Bundesdatenschutzgesetz (BDSG) > Grundsätzliches, Inhaltsdat.

Bürgerliches Gesetzbuch (BGB, z. B. AGB-Regelungen, §§ 305 ff.) > Terms of Use, Privacy Policies, Vertragsgrundlagen

Verbraucherrecht (UWG) > Vertragsgestaltung u. -abwicklung

Telekommunikationsgesetz (TKG) > Übertragung von Signalen in Netzen (Router, VoIP, E-Mail, Netzzugang, nicht bei kombinierten Angeboten)

EUROFORUM
Quality in Business Information
14. Datenschutz kongress 2013

Transparenzregelungen I

§ 5 TMG Allgemeine Informationspflichten (Impressum)

- Name, Anschrift, Rechtsform, Vertretungsberechtigung
- Elektronische Kontaktaufnahme
- Evtl. bei Zulassungspflicht Aufsichtsbehörde
- Evtl. bei Register Nummer (HandelsR, VereinsR, GenossenschaftsR)
- Evtl. Berufsbezeichnung und Kammer
- Evtl. Steuer-Nummer

§ 6 Kommerzielle Kommunikation

- Erkennbarkeit des kommerziellen Angebots
- Erkennbarkeit von Zugaben u. Gewinnspielen mit Werbecharakter

Transparenzregelungen II

Art, Umfang u. Zweck der Verarbeitung, Auslandsübermittlung (§ 13 I)

Anzeige der Weitervermittlung (§ 13 V)

Auskunftsanspruch (§ 13 VII, § 34 BDSG): sämtliche Bestands-, Nutzungs- und Inhaltsdaten, auch zu Pseudonym, „Dashboards“ genügen nicht

Information über Profilbildung und Widerspruchsrecht (§ 15 III)

Unberechtigte Kenntniserlangung (Breach Notification, § 15a, § 42a BDSG)

Information bei Einwilligung

- über Stelle, Zweck und Art der Daten (§ 4a BDSG)
- über Widerrufbarkeit (§ 13 III)

EUROFORUM
Quality in Business Information
14. Datenschutz kongress 2013

Transparenzregelungen III

Information über Werbung u. Widerspruchsmögl. (§ 28 IV BDSG)

Verfahrensverzeichnis (§§ 4e, 4gII 2 BDSG)

Evtl. Benachrichtigung bei bes. Übermittlungen (§ 33 BDSG)

Evtl. Automatisierte Entscheidungen (§ 6a BDSG)

Sinnvoll: Erreichbarkeit Beauftragter für Datenschutz (§ 4f BDSG)

Sinnvoll: Wahrnehmung Betroffenenrechte (§§ 6, 34, 35 BDSG)

Einwilligung

§ 13 II: Protokollierung, jederzeitige Abrufbarkeit, künftige Widerrufbarkeit, ebenso Werbeeinwilligung (§ 28 IIIa BDSG)

§ 4a BDSG: Bestimmtheit bzgl. Stellen, Zwecke u. Daten

Freiwilligkeit durch Koppelungsverbot

Privacy by Default

Einwilligung durch Browsereinstellung setzt Standards voraus (W3C-Diskurs, z. B. über DoNotTrack)

EUROFORUM
Quality in Business Information
14. Datenschutz kongress 2013

Gestaltung von Informationen und Optionen

Zwecks Transparenz und Wahlfreiheit (Layered Policy Design):

- Kurzhinweis, evtl. mit Icons
- Zusammengefasster Datenschutzhinweis
- Vollständiger Hinweis
- Evtl. Erläuterungen, Hintergründe und Quellen

Situative Konfrontation

Vgl. WP 100 Art. 29-Datenschutzgruppe vom 25.11.2004:
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2004/wp100_de.pdf

Jederzeitige Abrufbarkeit und Änderbarkeit des Profils

Verantwortlichkeit

§ 3 Abs. 7 BDSG: Datenschutz

eigene DV (Inhalte), AuftragsDV, Nutzung fremder Software
Portale u. Dienste (incl. Cookies; DV außerhalb EU/EWR)

§§ 7-10 TMG (Notice and take down): Zivilrechtliche Haftung
(Schadenersatz, Unterlassung, Beseitigung) Störereigenschaft

§§ 13 ff. StGB: Strafrecht (ähnlich: OWi-Verfahren)

EUROFORUM
Quality in Business Information
14. Datenschutz kongress 2013

Auftragsdatenverarbeitung

§ 11 BDSG, wenn rechtliche Voraussetzungen fehlen
Funktionsübertragung, evtl. gemeinsame Verantwortlichkeit
gilt auch für Cloud-Anwendungen

Vertragliche Festlegung (schriftlich) und praktische Umsetzung

- Gegenstand und Dauer
- Technisch-organisatorische Maßnahmen
- Berichtigung, Löschung, Sperrung – auch nach Vertragsende
- Weisungen und Kontrollen – Pflichten von AG u. AN
- Transparenz u. Internventionsmöglichkeit für AG
- Unterauftragsverhältnisse

Bestandsdaten

§ 14: nur soweit für Vertrag erforderlich

- Adresse, Telefonnummer, Bankdaten, Pseudonym, Passwort
- Angabe, welche Daten obligatorisch, welche fakultativ

§ 13 VI: Anonyme/Pseudonyme Nutzung, „soweit dies technisch möglich und zumutbar“

> Abrufdienste immer anonym

Differenzierung Anonymität im Netz, Identifizierkeit f. Anbieter

EUROFORUM
Quality in Business Information
14. Datenschutz kongress 2013

Nutzungsdaten

§ 15: Erforderlichkeit für Inanspruchnahme (incl. kurzfristige Sicherheitskontrolle) und Abrechnung

- Identifikation, Nutzungsdauer, Art des Dienstes
- Profilbildung für Zwecke der Werbung, Marktforschung und Dienstgestaltung (auch Nutzungsanalyse), keine Reidentifizierung erlaubt

Art. 5 III E-Privacy-Directive: Einwilligung bei Cookies, die für Diensterbringung nicht erforderlich sind

Zahlungsdaten

Wahlmöglichkeiten der Zahlungsart

- Anonyme/pseudonyme Zahlung: Prepaid, Vorauskasse, Bitcoin, (Nachnahme)
- Identifizierende Zahlung: Überweisung, Lastschrift, EC-Cash, Kreditkarte, sofortüberweisung.de, PayPal

Transparenz bzgl. Zahlungsvorgang, Beteiligte, Ablauf

Sichere Authentisierung (evtl. 2 Wege)

Abschottung, strenge Zweckbindung

Bonitätsbewertung nur bei kreditor. Risiko (Auskunftei, Scoring)

Negativinformationen an Auskunftei (§ 28b BDSG)

Einschaltung von Inkasso

EUROFORUM
Quality in Business Information
14. Datenschutz kongress 2013

Technische Sicherungen

Vermeidung von Identifizierung durch Identifikatoren (IP-Adresse, Cookies, Browser-Fingerprint)

Privacy by Default (DS-freundliche Grundeinstellungen)

Protokollierung nach Erforderlichkeitsgrundsatz und Relevanz: Speicherung, Änderung, Löschung

Sichere Authentisierung bei Kunden-Logins (nPA, Besitz u. Wissen, Biometrie)

Verschlüsselung der Kommunikation Nutzer-Server: https

Absicherung vor Drittzugriff

Sichere Update-Verfahren

Evtl. Ausschluss von Suchmaschinen (robot.txt)

Einsatz neuer Personalausweis (nPA)

Zertifizierung durch Vergabestelle (VfB)

- Identifizierungsfunktion
- Altersverifikation
- Pseudonym-Funktion
- Wohnortverifikation
- Eintrittskarte/Wiedererkennung

Zertifizierung > Nachweise in Datenschutz und Datensicherheit

EUROFORUM
Quality in Business Information
14. Datenschutz kongress 2013

Datenschutzmanagement

Beauftragter für Datenschutz (bDSB, §§ 4f, 4g BDSG)

Einrichtung eines Beschwerdemanagements

Systemdokumentation

Ablaufplanung bzgl. typischer Prozesse (Verfahrensänderungen, Test+Freigabe, Updates, Schulung, Mitarbeiterkontrolle)

Evtl. Einbeziehung des Betriebsrats (bei Mitarbeiterkontrollierbarkeit)

Schlussfolgerungen

E-Commerce-Angebote zertifiziert durch D21-Gütesiegel-Mitglieder

Datenschutz-Zertifizierung durch ULD (Gütesiegel SH, European Privacy Seal)

Standardisierung dringend geboten

Verhaltensregeln wünschenswert (§ 38a BDSG)

Datenschutzfreundliche Webangebote als Marktvorteil

> Datenschutz ist möglich

EUROFORUM
Quality in Business Information
14. Datenschutz kongress 2013

Internetauftritt von Unternehmen datenschutzkonform gestalten

Dr. Thilo Weichert

Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein (ULD)

Holstenstr. 98, D- 24103 Kiel

mail@datenschutzzentrum.de

https://www.datenschutzzentrum.de