Datenschutz im Zahlungsverkehr

Thilo Weichert, Leiter des ULD
Landesbeauftragter für Datenschutz Schleswig-Holstein

Payment World 2010

Management Forum – Handelsverband Deutschland
des Einzelhandels (HDE) - BDOA

Berlin, 26.10.2010

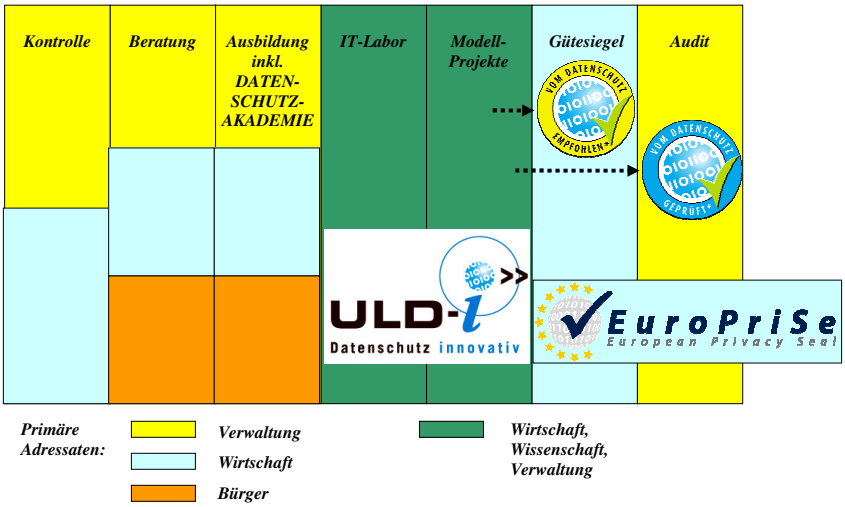
ULD
Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Inhalt

- Unabhängiges Landeszentrum für Datenschutz – ULD
- Rechtsgrundlagen
- Grundprinzipien des Datenschutzes
- Die konkreten Praktiken bei EC-Verfahren
- Zulässigkeit der Datenverarbeitung
  - Einwilligung,
  - Auskunfteitätigkeit
  - Scoring
  - Factoring
- Lösungsmöglichkeiten

ULD www.datenschutzzentrum.de

Unabhängiges Landeszentrum für Datenschutz



ULD www.datenschutzzentrum.de

BVerfG, U.v. 15.12.1983 (1 BvR 09/83 u.a.)

„Unter den Bedingungen der modernen Datenverarbeitung wird der Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten vom **allgemeinen Persönlichkeitsrecht** … umfasst. Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen."

„Einschränkungen dieses **Rechts auf ´informationelle Selbstbestimmung`** sind nur im überwiegenden Allgemeininteresse zulässig."

BVerfG , B.v. 23.10.2003 (1 BvR 2027/02)

„Das allgemeine Persönlichkeitsrecht … entfaltet als Norm des objektiven Rechts seinen Rechtsgehalt **auch im Privatrecht**."

„Ist ersichtlich, dass in einem Vertragsverhältnis ein Partner ein solches Gewicht hat, dass er den **Vertragsinhalt faktisch einseitig bestimmen** kann, ist es Aufgabe des Rechts, auf die Wahrung der Grundrechtspositionen beider Vertragspartner hinzuwirken, um zu verhindern, dass sich für einen Vertragsteil die Selbstbestimmung in eine Fremdbestimmung verkehrt."

Rechtsgrundlagen

- Bundesdatenschutzgesetz (BDSG) seit 1976, letzte Aktualisierung 2009
- Verbraucherrecht, hier v.a. Regelungen zu Allgemeinen Geschäftsbedingungen (§§ 305 ff. BGB)
- Bankgeheimnis ist grds. nicht anwendbar für Dienstleister und für Handelsunternehmen, schützt bei Banken das besondere Vertrauensverhältnis (schutzwürdiges Interesse)

7 Regeln des Datenschutzes

1. Rechtmäßigkeit
2. Einwilligung
3. Zweckbindung
4. Erforderlichkeit und Datensparsamkeit
5. Transparenz und Betroffenenrechte
6. Datensicherheit
7. Kontrolle

Verarbeitung von Zahlungsdaten

- Keine besondere Art von Daten nach § 3 IX BDSG
- Aber Aussagekraft über alle Lebensbereiche (Interessen-, Verhaltens-, Konsum-, Sozial-, Bewegungsprofile, Bonitätsaussagen) Problem: Verbot umfassender Persönlichkeitsprofile (BVerfG)

> Spezialregelung Auskunfteien (§ 28a BDSG)

> Spezialregelung Scoring (§ 28b BDSG)

> Besondere Auskunftsansprüche (§ 34 BDSG)

> Benachrichtigungspflicht bei Datenlecks (§ 42a BDSG)

Hintergründe

- 2005/2006: Prüfung von Telecash durch Aufsichtsbehörde Bade-Württemberg: „...nicht im Widerspruch zum BDSG"
- NDR 06.05.2010: „Umstrittene Einwilligungserklärungen an der Supermarktkasse" – Klage des VZBV wegen Telecash
- NDR 23.09.2010: „Der Datenkrake von Ratingen"
- 12.10.2010: Datenschützer treffen ELV-Forum in Ansbach
- NDR 13.10.2010: „Der Big Brother von Hamburg-Lokstedt"
- Heise 14.10.2010: „Easycash bestreitet Missbrauch von Kundendaten"
- NDR 15.10.2010: Easycash übermittelte 2009 über 2 Monate Zahlungsverkehrsdaten an Tochter Loyalty Solutions - „Strafanzeige durch Datenschützer"

BDSG-Anwendbarkeit und Zuständigkeit I

§ 3 I BDSG: „Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)"

> Bestimmbarkeit bei KontoNr. und BLZ od. EC-Karten-Nr.

§ 38 BDSG: Datenschutzbehörden der Länder = zuständig für Daten verarbeitende Stellen im Land

> Easycash-NRW, Telecash-Hessen, Intercard-Bayern

Handelsunternehmen-Land der Zentrale + der Filiale

§ 3 VII BDSG: „Verantwortliche Stelle ist ... Stelle, die personenbezogene Daten für sich selbst ... verarbeitet ... oder dies durch andere im Auftrag vornehmen lässt."

BDSG-Anwendbarkeit und Zuständigkeit II

§ 11 BDSG: Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Auftrag

> Beschränkung auf Hilfstätigkeiten bei Verarbeitung

> Verantwortlichkeit und Weisungsrecht des Auftraggebers

> Auftragnehmer darf Daten nicht im eigenen Interesse verarbeiten oder von verschiedenen Auftraggebern zusammenführen

§ 3 IV Nr. 3 BDSG: Übermitteln = Bekanntgeben personenbezogener Daten an Dritte

> Dritter wird verantwortliche Stelle

Electronic Cash-Verfahren

- Verantwortliche Stelle = Handelsunternehmen
- EC-Karten-Dienstleister = Auftragsdatenverarbeiter für Handelsunternehmen
- Bank = Datenempfänger u. -übermittler, gibt Zahlungsgarantie
- Online-Identifizierung u. Authentisierung durch Karte und PIN

- Problem: Kosten 0,3% des Umsatzes contra 0,15-0,2% bei Elektronischem Lastschriftverfahren (ELV)
- DS: Absolute Abschottung und Zweckbindung der Daten

ELV-Offline

- Händler erhält evtl. Sperrdatei von Dienstleister (Datenübermittlung durch Auskunftei)
- Offline-Abgleich mit Sperrdatei (nicht bezahlt, Konto erloschen, Widerspruch)
- Einmalige Nutzung nur für Zahlungsvorgang
- Rückmeldung bei Widerspruch an Dienstleister

Spezielle Fragen:

- Ist Sperrdateiübermittlung auf Verdacht (Vorratsdatenübermittlung) zulässig ?
- Ist Rückübermittlung an Dienstleister bei Störung zulässig?

ELV-Online

- Einlesen und Weitergabe an Dienstleister
- Abgleich mit Sperrdatei (incl. Zusatzinfos aus Banken- und Polizeibereich - KUNO), evtl. Score-Berechnung

unternehmensintern DViA, unternehmensübergreifend DÜ

- Speicherung erfolgreicher Transaktionen (z.B. 30 Tage)
- Rückmeldung incl. Zahlungswegeempfehlung an Händler
- Lastschriftzustimmung incl. Einwilligung zur Datenverarbeitung
- Evtl. Forderungsabtretung
- Transaktionsspeicherung und -auswertung beim Dienstleister, evtl. weitere Nutzung (Kundenkarten-Abgl.)

> sämtliche Transaktionen sind fragwürdig

Zusatzangebote

Transaktionslimits und Frequenzzähler für jeweiligen Händler

Forderungsabtretung (Factoring)

Kundenauswertungen

Adfinder (Adressenauskunft aus Kontoverbindung) d. SCHUFA

Zulässigkeit der Datenverarbeitung

§ 4 I BDSG: „Die … Verarbeitung … ist zulässig, soweit dieses Gesetz … dies erlaubt oder anordnet oder der Betroffene eingewilligt hat."

§ 11 BDSG (DViA): Datenweitergabe unbeschränkt möglich, aber hohe Voraussetzungen und keine Weiternutzung

§ 28 BDSG: Datenverarbeitung für eigene Zwecke

- für Rechtsgeschäft erforderlich
- Abwägung berechtigtes – schutzwürdiges Interesse

§ 29 BDSG: Datenverarbeitung für fremde Zwecke, z.B. Auskunftei, Abwägung bei Speicherung, glaubhaftes überwiegendes berechtigtes Interesse bei Abfrage

Anforderungen Einwilligung (§ 4a BDSG)

Erklärung vor Beginn der Datenverarbeitung
Freiwilligkeit
Information über Daten, verarbeitende Stelle und Zweck
Schriftlichkeit, wenn nicht andere Form angemessen
Besondere Hervorhebung bei mehreren Erklärungen
Widerrufbarkeit

Nachweis der Einwilligung durch Beleg für Betroffenen

Mängel der Einwilligung

- Aushang wird nicht wahrgenommen oder existiert nicht
- Keine Einwilligung durch Hingabe der EC-Karte bzgl. Sperrdateiabgleich und weitere DV
- Bonunterschrift erfolgt nach Datenübermittlung
- Erklärung ist nicht hervorgehoben
- Freiwilligkeit fraglich wg. psychischem Druck an der Kasse
- Transparenz u. Bestimmtheit der konkreten Verarbeitungsschritte und Datenverarbeiter (Wer macht was mit welchen Daten?)
- Oft keine Aushändigung des Belegs

Dienstleister als Auskunftei (§§ 29, 28a)

Bisher:

- DÜ von Positivdaten mit Einwilligung
- DÜ von Negativdaten bei berechtigtem Interesse (§ 28)

Jetzt:

- DÜ nur zur „Wahrung berechtigter Interessen" bei Nichtbegleichung einer Forderung, Fälligkeit, 2x Mahnung, Wartezeit, Hinweis, Nichtbestreiten (§ 28a I Nr. 4)
- Übermittlung von Positivdaten nur durch Kreditinstitute (§ 28a II)

Übermittlung durch Auskunftei bei berechtigtem Interesse nach Abwägung (§ 29 II)

Dienstleister als Auskunftei

Verstöße bzw. Probleme:

Keine Rechtsgrundlage für Anlieferung von Positiv- und Negativdaten

- Keine doppelte Mahnung innerhalb 4 Wochen
- Kein Hinweis auf Speicherung bei Mahnung
- Kein Bankgeschäft (Positivdaten)

Ob Einwilligung noch möglich ist, ist unklar

Berechtigtes Abfrageinteresse zumindest fragwürdig

Keine Berücksichtigung von Betroffeneninteressen

Scoring (§§ 6a, 28b, 34 II)

- Durchführung eines Vertragsverhältnisses
- Berechnung eines Wahrscheinlichkeitswertes
- Wissenschaftlich anerkanntes mathematisch-statisisches Verfahren

Rechtsverstöße:

- Automatisierte Einzelentscheidung
- Datenbasis ist unzulässig
- Berechtigtes Interesse für Abfrage?
- Möglichkeit der Auskunftserteilung?

Factoring

Datenschutzanforderungen an systematische Forderungs-abtretung (Factoring) sind unabhängig von zivilrechtlichen Voraussetzungen

Rechtsgrundlagen:

§ 28 I Nr. 1 BDSG: Expliziter Gegenstand des Vertrages, evtl. Integration in AGB, aber Problem der Überraschungsklausel, > i.d.R. kein Vertragsbestandteil

§ 28 I Nr. 2 BDSG: Berechtigtes Interesse des Händlers (+), aber entgegen stehendes schutzwürdiges Betroffeneninteresse (Gefahr der Auswertung, unbekannter Vertragspartner) > (-)

Auswertungen für Kundenbindung ?

Absolutes „No Go" –
gilt auch für Händler selbst oder im Form der DViA

- Keine Transparenz bei Datenerhebung
- Kein Bestandteil der Einwilligung
- Unzulässige Übermittlung
- Verstoß gegen Zweckbindung
- Verstoß gegen Verbot der Bildung von Persönlichkeitsprofilen

Betroffenenrechte

- Informationspflichten bei vertraglicher Datenerhebung (§ 4 III BDSG) und Einwilligung (§ 4a BDSG)
- Auskunftsanspruch über eigene Daten (§ 34 BDSG)
- Benachrichtigungspflicht bei erstmaliger DV (§ 33 BDSG)
- Anspruch auf Sperrung und Berichtigung bei bestrittenen und falschen Daten (§ 35 I, III, IV BDSG)
- Anspruch auf Löschung bei unzulässiger Speicherung (§ 35 II BDSG)
- Anspruch auf Schadenersatz (§ 7 BDSG, §§ 823 ff. BGB)
- Anrufungsrecht an Aufsichtsbehörde (§ 38 BDSG, Art. 17 GG)

Sanktionen

- Beanstandung durch Aufsichtsbehörde (§ 38 I BDSG)
- Veröffentlichung eines Verstoßes
- Anordnungsverfahren (§ 38 V BDSG)
- Bußgeldverfahren (§ 43 BDSG)
- Strafverfahren bei Schädigungs- und Bereicherungsabsicht (§ 44 BDSG), Entgeltlichkeit genügt
- Verbraucherrechtliche Sanktionen durch Verbraucherzentralen (UKlaG)

Branchen-Verhaltensregeln

§ 38a BDSG

(1) Berufsverbände und andere Vereinigungen, die bestimmte Gruppen von verantwortlichen Stellen vertreten, können Entwürfe für Verhaltensregeln zur Förderung der Durchführung von datenschutzrechtlichen Regelungen der zuständigen Aufsichtsbehörde unterbreiten.

(2) Die Aufsichtsbehörde überprüft die Vereinbarkeit der ihr unterbreiteten Entwürfe mit dem geltenden Datenschutzrecht.

Lösungsmöglichkeiten

- Gestaltung des gesamten ELV als DViA für Händler
- Verzicht auf händlerübergreifende Auswertungen
- Information der Kundenschaft, z.B. über Internet/Aushändigungen auf Anfrage
- Bei weitergehender DV Einwilligung durch ELV-Zulassung durch Kunden vor Beginn der Kaufvorgänge mit umfassender Information – Aushändigung der Erklärung
- Auskunftserteilung an Betroffene nach hinreichender Identifizierung (Kopie Ausweis u. EC-Karte; Bankenbestätigung)
- Systemänderung nicht ohne DS-Audit

Datenschutz im Zahlungsverkehr

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