# eCommerce und Datenschutz

## Wie Sie mit Kundendaten in Webshops umgehen sollten

20.11.2014, München - Best in eCommerce Day

**Dr. Sebastian Kraska** | Rechtsanwalt, Diplom-Kaufmann
Telefon: 089 1891 7360 | Internet: www.iitr.de | E-Mail: email@iitr.de

# Was soll das alles? Warum das Thema Datenschutz für Sie relevant ist.

- Wettbewerber
- Enttäuschte Beschäftigte
- Enttäuschte Kunden
- „IT-Sicherheits-Betrüger“
- Datenschutz-Aufsichtsbehörde

# Verstärkte Prüftätigkeit der Aufsichtsbehörden

- Bislang Audits vor allem nach Ankündigung der Aufsichtsbehörde

- Seit kurzem Wechsel mit stärkerem Focus auf technische Fragestellungen und unangekündigte Vor-Audits (z.B. Test von Mailservern, vgl. vertiefend http://www.iitr.de/140909iitr)

„Zur möglichen Verschlüsselung der Kommunikation zwischen Mailservern ist der Einsatz des Protokolls STARTTLS nach dem **Stand der Technik als erforderlich** zu erachten. Findet im Rahmen der Nachrichtenübermittlung das Verschlüsselungsprotokoll SSL/TLS Einsatz, so ist zudem das Verschlüsselungsverfahren Perfect Forward Secrecy zum erhöhten Schutz der übermittelten Daten notwendig. Darüber hinaus ist eine Verwundbarkeit durch die Heartbleed-Lücke auszuschließen."

Quelle: http://www.lda.bayern.de/onlinepruefung/emailserver.html

## Webanalyse-Tools (1/9)

- „Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat.“
- „Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).“
- Erhebung/Verarbeitung/Nutzung personenbezogener Daten im Rahmen der Webanalyse: Einwilligung erforderlich
- Keine Erhebung/Verarbeitung/Nutzung personenbezogener Daten im Rahmen der Webanalyse: ohne Einwilligung zulässig

# Logfiles und IP-Adressen (2/9)

- Server-Logfiles speichern in der Regel IP-Adressen der Besucher
- IP-Adressen als personenbezogene Daten?
- Sicherungsbedürfnis in der Praxis: Speicherung für maximal 7 Tage

# Werbung per E-Mail (3/9)

- Grundsatz: Einwilligung des Betroffenen erforderlich
  - Freiwilligkeit und bewusste Willensäußerung
  - Transparenz
  - Widerruflichkeit

- Ausnahme: ohne Einwilligung darf Werbung per E-Mail verschickt werden wenn
  - ein Unternehmer im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden dessen elektronische Postadresse erhalten hat
  - der Unternehmer die Adresse zur Direktwerbung für eigene ähnliche Waren oder Dienstleistungen verwendet
  - der Kunde der Verwendung nicht widersprochen hat und
  - der Kunde bei Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen wird, dass er der Verwendung jederzeit widersprechen kann, ohne dass hierfür andere als die Übermittlungskosten nach den Basistarifen entstehen

## Cookies (4/9)

- Häufig (zu Unrecht) Unklarheit bzgl. Regelungslage
- Europäische Richtlinie in Deutschland nicht umgesetzt
- In Deutschland daher keine Veränderung der rechtlichen Situation
- Cookies ohne personenbezogene Daten: keine rechtlichen Besonderheiten
- Cookies mit personenbezogenen Daten: Sperre des Datenschutzrechts

## Technisch/organisatorische Maßnahmen (5/9)

- Externes Hosting: Auftragsdatenverarbeitungsvertrag

- Beachten technischer Mindeststandards
  - Datensicherung
  - Updates von Shop- und Webseitensystemen
  - Einsatz von Monitoringtools
  - Nutzung von Verschlüsselungsmöglichkeiten

# Umgang mit Zahlungsdaten (6/9)

- Empfehlung: Einbindung von externem Zahlungsdiensteanbieter

- Neben regulatorischen Problemen erspart sich der Webshop-Betreiber damit auch so genannte „Informationspflichten im Datenverlustfall“

# Bonitätsprüfungen (7/9)

- Keine verdeckte Bonitätsprüfung

- Prüfung der Bonität nur in Abhängigkeit der gewählten Zahlart

- Erläuterung der Details einer Bonitätsprüfung in AGB und Datenschutzerklärung

# „Social-Plugins“ (8/9)

- Datenschutzrechtliche Besonderheit: Datenübermittlung ohne explizite Handlung des Nutzers

- 2-Klick-Lösung als datenschutzrechtlich vertretbarer Ansatz

- Beschreibung in der Datenschutzerklärung

# Datenschutzerklärung (9/9)

- Reine Informationsseite über Datenverarbeitungsvorgänge auf der Webseite

- Keine Zustimmung zur Datenschutzerklärung erforderlich

- Von jeder Seite des Webportals aufrufbar

# Fragen?

Newsletter: www.iitr.de/news
Kontakt: Dr. Sebastian Kraska

**Institut für IT-Recht IITR GmbH |** Marienplatz 2 | 80331 München
Telefon: 089 1891 7360 | Internet: www.iitr.de | E-Mail: email@iitr.de