

Techniken der Ausspähung – bedrohte Privatheit

„Der gläserne Mensch“ – was wir von uns preisgeben?

Christian Goltz, Wirtschaftsabteilung bei der StA Chemnitz

Saarbrücken, 18.09.2008

© 2008 Christian Goltz

EDV-Gerichtstag 2008, Saarbrücken

Techniken der Ausspähung – bedrohte Privatheit

Ausblicke für Datenverarbeitung in der Zukunft

Heute: Computer (PC/Großrechner)
Morgen: Eine Vielzahl von (Klein-)geräten wie z.B.
Chips auf Skipässen, Ausweisen,
Navigationsgeräten, Fahrzeugassistenten,
.....

➔ Begriff des „Pervasive Computing“ (Allgegenwärtige
Datenverarbeitung)

© 2008 Christian Goltz

EDV-Gerichtstag 2008, Saarbrücken

Techniken der Ausspähung – bedrohte Privatheit

Daten in der Öffentlichen Verwaltung

- Erforderlich für :
- Meldewesen
 - Steuern
 - Verkehrsinfrastruktur

Techniken der Ausspähung – bedrohte Privatheit

Daten in der Privatwirtschaft I

Erforderliche Daten, z. B. für Buchhaltung (Abrechnung),
Garantieleistungen oder andere vertragliche Leistungen

Problem: Datensammlung führt dazu, dass Produkte **nicht** mehr
verkauft werden (Scoring)

Techniken der Ausspähung – bedrohte Privatheit

Daten in der Privatwirtschaft II

Freiwillig überlassene Daten aus Umfragen,
Kundenbindungssystemen, Internet (z.B. Payback, Schufa)

Erhebung von Daten nur zulässig, sofern Kunde wirksam
eingewilligt hat

Techniken der Ausspähung – bedrohte Privatheit

§ 4a BDSG

Die Einwilligung ist nur wirksam, wenn sie auf der **freien Entscheidung** des Betroffenen beruht. Er ist auf den vorgesehenen **Zweck der Erhebung, Verarbeitung oder Nutzung** sowie, soweit nach den Umständen des Einzelfalles erforderlich oder auf Verlangen, auf die Folgen der Verweigerung der Einwilligung **hinzuweisen**. Die Einwilligung bedarf der **Schriftform**, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soll die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt werden, ist sie **besonders hervorzuheben**.

Techniken der Ausspähung – bedrohte Privatheit

Einwilligungserklärung Payback (Stand: 15.09.2008)

Einwilligungserklärung: Ich bin damit einverstanden, dass die von mir angegebenen Daten sowie die Rabattdaten (Waren/Dienstleistungen, Preis, Rabattbetrag, Ort und Datum des Vorgangs) für an mich gerichtete **Werbung** (z.B. Informationen über Sonderangebote, Rabattaktionen) per Post sowie zu Zwecken der **Marktforschung** ausschließlich von der Loyalty Partner GmbH und den Partnerunternehmen gemäß **Ziffer 2 der Hinweise zum Datenschutz** gespeichert und genutzt werden. Außerdem darf die Loyalty Partner GmbH diese Daten gleichermaßen für an mich gerichtete Werbung nutzen, während ich beim PAYBACK Service Center anrufe, die Internet-Seite www.payback.de besuche, ein PAYBACK Kundenterminal benutze, und in weiteren von mir bestellten PAYBACK Services (z.B. E-Mail Newsletter).

Techniken der Ausspähung – bedrohte Privatheit

Hinweise zum Datenschutz Payback (Stand 15.09.2008)

1. Daten

Wenn Sie am PAYBACK Programm teilnehmen, wird Ihr voller Name, Ihr Geburtsdatum und Ihre vollständige Anschrift benötigt (Basisdaten). Die über das Anmeldeformular insgesamt mitgeteilten Daten werden durch die PAYBACK Betreibergesellschaft PAYBACK GmbH, Postfach 232103, 85330 München-Flughafen, zur Abwicklung des PAYBACK Programms erhoben, gespeichert und genutzt. Die Basisdaten, freiwilligen Angaben und ggf. deren Änderungen, übermittelt PAYBACK an das Partnerunternehmen, über welches Sie Ihre PAYBACK Karte erhalten haben. Sollten Sie Ihre PAYBACK Karte direkt von PAYBACK oder von einer Apotheke erhalten haben, erfolgt eine solche Übermittlung nicht. Eine Übermittlung an die übrigen Partnerunternehmen oder außerhalb des Programms stehende Dritte ist in jedem Fall ausgeschlossen.

Techniken der Ausspähung – bedrohte Privatheit

...

Setzen Sie Ihre PAYBACK Karte bei einem Partnerunternehmen ein, so meldet dieses die Rabattdaten (Waren/Dienstleistungen, Preis, Rabattbetrag, Ort und Datum des Vorgangs) an PAYBACK zur Gutschrift, Abrechnung gegenüber den Partner- unternehmen, Verwaltung und Auszahlung der Rabatte. Apotheken melden Waren/Dienstleistungen nicht. Eine Übermittlung von Rabattdaten an die übrigen Partnerunternehmen sowie an außerhalb des Programms stehende Dritte ist ausgeschlossen.

Haben Sie zur Auszahlung der Rabatte Ihre Bankverbindung angegeben, so wird diese nur durch PAYBACK erhoben, gespeichert und zur Auszahlung genutzt.

Auf Anforderung teilt Ihnen PAYBACK gerne mit, ob und welche persönlichen Daten über Sie gespeichert sind.

Techniken der Ausspähung – bedrohte Privatheit

2. Werbung und Marktforschung

Wenn Sie bei der Anmeldung Ihre diesbezügliche Einwilligung erteilt haben, nutzt PAYBACK die Basisdaten, eventuelle freiwillige Angaben und die gemeldeten Rabattdaten sowie etwaige Änderungen hiervon zu Zwecken der Marktforschung sowie zur individuellen Erstellung und Versendung ausgewählter Informationen (Werbung) per Post.

Wenn Sie ein PAYBACK Kunden-Terminal bei einem Partnerunternehmen nutzen, das PAYBACK Service Center anrufen oder die Internet-Seite www.payback.de besuchen, kann Ihnen PAYBACK auch bei dieser Gelegenheit individuelle Angebote auf Grundlage Ihrer oben genannten Daten unterbreiten. Daneben kann das Partnerunternehmen, von dem Sie Ihre PAYBACK Karte erhalten haben, Ihre Basis- und dort anfallenden Rabattdaten, Ihre Angaben zum Familienstand, zur Berufstätigkeit und zum monatlichen Haushaltsnettoeinkommen sowie eventuelle freiwillige Angaben zu eigenen Zwecken der Marktforschung und der Versendung von Informationen per Post nutzen. Apotheken können dieses nicht.

Ihre diesbezügliche Einwilligung können Sie jederzeit gegenüber dem PAYBACK Service Center, Postfach 23 21 02, 85330 München-Flughafen, oder der PAYBACK GmbH, Postfach 23 21 03, 85330 München-Flughafen, widerrufen. Das ggf. betroffene Partnerunternehmen wird von PAYBACK über Ihren Widerruf informiert. Haben Sie Ihre Einwilligung nicht erklärt oder widerrufen Sie diese, findet eine Datennutzung nach vorstehendem Absatz nicht statt. Selbstverständlich können Sie aber am PAYBACK Programm teilnehmen bzw. weiterhin teilnehmen. Sie erhalten dann lediglich die zur Abwicklung des Programms notwendigen Informationen (z.B. Mitteilungen zu Ihrem Punktestand).

Zur Versendung von Informationen per Post werden die notwendigen Basisdaten fallweise durch beauftragte Dienstleistungsunternehmen verarbeitet (Auftragsdatenverarbeiter). Unmittelbar nach Durchführung der Aktion werden Ihre Daten dort gelöscht. Jede Möglichkeit einer Identifizierung Ihrer Person durch Partnerunternehmen oder Dritte ist ausgeschlossen.

Google Chrome

Google Chrome - Anmerkung zum Datenschutz

2. September 2008

In den [Datenschutzbestimmungen von Google](#) wird beschrieben, wie persönliche Informationen behandelt werden, wenn Sie Produkte und Dienste von Google verwenden. Dazu zählen auch bei der Verwendung von Google Chrome bereitgestellte Informationen. Zudem werden im Folgenden unsere spezifischen Datenschutzmaßnahmen für Google Chrome erläutert. Google benachrichtigt Sie über alle erheblichen Änderungen an diesen Bestimmungen und Sie haben immer die Möglichkeit, das Senden von persönlichen Informationen an Google durch entsprechende Browsereinstellungen zu verhindern oder die Verwendung einzustellen.

n Bei der Verwendung von Google Chrome an Google gesendete Informationen

Zum Verwenden und Herunterladen von Google Chrome müssen keine persönlichen Informationen angegeben werden. Falls Sie Google Chrome herunterladen oder zum Herstellen einer Verbindung mit den Servern von Google verwenden, empfängt Google nur [standardmäßige Protokollinformationen](#) wie die IP-Adresse Ihres Computers und einige [Cookies](#). Sie können Google Chrome wie [hier](#) erläutert so konfigurieren, dass keine Cookies an Google oder andere Websites gesendet werden.

Darüber hinaus werden von einigen Funktionen von Google Chrome begrenzte weitere Informationen an Google gesendet:

- In die Adressleiste eingegebene URLs oder Suchanfragen werden an Google gesendet, damit von der Vorschlagsfunktion automatisch gesuchte Begriffe oder URLs empfohlen werden können. Falls Sie Nutzerstatistiken an Google senden möchten und Sie eine vorgeschlagene Suchanfrage oder URL akzeptieren, sendet Google Chrome diese Information ebenfalls an Google. Sie können diese Funktion wie [hier](#) erläutert deaktivieren.
- Von Ihnen aufgerufene nicht vorhandene URLs werden möglicherweise an Google gesendet, damit wir Ihnen bei der Suche nach der gewünschten URL helfen können. Sie können diese Funktion wie [hier](#) erläutert deaktivieren.
- Die Funktion "Sicheres Durchsuchen" stellt regelmäßig eine Verbindung zu den Servern von Google her, um die aktuellste Liste bekannter Phishing- und Malware-Websites herunterzuladen. Zusätzlich wird, wenn Sie eine Website besuchen, die eine Phishing- oder Malware-Website sein könnte, von Ihrem Browser eine verschlüsselte Kopie eines Teils der URL dieser Website an Google gesendet, so dass wir weitere Informationen über diese potentiell gefährliche URL senden können. Google kann die reale URL, die Sie besuchen, aus diesen Informationen nicht bestimmen. Weitere Informationen erhalten Sie [hier](#).
- Ihre Kopie von Google Chrome enthält mindestens eine eindeutige Anwendungsnummer. Diese Nummern und Informationen zur Installation des Browsers (z. B. Versionsnummer, Sprache) werden bei der erstmaligen Installation und Verwendung der Anwendung und bei der automatischen Update-Prüfung von Google Chrome an Google gesendet. Falls Sie [Nutzungsstatistiken und](#)

Techniken der Ausspähung – bedrohte Privatheit

Datenverarbeitung im Ausland

Datenübertragung ins Ausland im Einzelfall sicher zulässig, aber:
Unzulässige Zusammenführung einzelner Daten und nach deutschen Gesetzen unzulässige Datenverarbeitung im Ausland ist mit deutschen Gesetzen nicht greifbar.

Techniken der Ausspähung – bedrohte Privatheit

Feststellungen aus der Praxis:

Nur in ca. 50 % aller Fälle wird Position eines
Datenschutzbeauftragten eingerichtet

Verfahrensverzeichnisse fehlen völlig

Tatsächlicher Umfang der Datenverarbeitung selbst im Wege
von Durchsuchungen nur sehr schwer aufklärbar

Techniken der Ausspähung – bedrohte Privatheit

Fazit:

- Datenschutzgesetze nach geltender Regelung bieten gewissen, aber keinesfalls ausreichenden Schutz bei einer „allgegenwärtigen Datenverarbeitung“.
- Grundrecht auf informationelle Selbstbestimmung erheblich gefährdet
- Datenschutz kein Hemmschuh, sondern **Freiheitsrecht**

Techniken der Ausspähung – bedrohte Privatheit

*Unter den Bedingungen der elektronischen
Datenverarbeitung
gibt es kein belangloses personenbezogenes
Datum mehr.
(Burkhard Schröder)*