

Datenschutz im Internet – am Beispiel des Speicherns von Cookies

Dietmar Jahnel

*Institut für Verfassungs- und Verwaltungsrecht, Universität Salzburg
Kapitelgasse 5-7, A-5020 Salzburg
Dietmar.Jahnel@sbg.ac.at*

Schlagworte: Datenschutzrecht, Internet, Cookies, Datenverwendung, personenbezogene Daten.

Abstract: Bei der Prüfung der datenschutzrechtlichen Zulässigkeit des Speicherns von Cookies auf dem PC des Betroffenen ist zunächst zu untersuchen, ob es sich dabei um personenbezogene Daten iSd DSGVO handelt. Dies ist etwa dann zu bejahen, wenn eine Verknüpfung mit einer Kundendatei erfolgt. Die Speicherung von Cookies ist in diesem Fall solange zulässig, als sie zur Erfüllung einer vertraglichen Verpflichtung zwischen Auftraggeber und Betroffenen erforderlich ist. In Frage kommt dabei vor allem die Abwicklung eines Kaufs über das Internet. Nach Beendigung des Kaufvorgangs wird ein weiteres Speichern des Cookies ohne Zustimmung des Betroffenen allerdings datenschutzrechtlich unzulässig.

1. Anwendbare Rechtsvorschriften

Für den Datenschutz im Internet sind folgende rechtliche Bestimmungen von Bedeutung:

Zunächst das allgemeine Datenschutzrecht im neuen *Datenschutzgesetz 2000* (DSG), das am 1.1.2000 in Kraft getreten ist.¹ Dieses Gesetz, vor allem initiiert durch die Pflicht zur Umsetzung der EG-Datenschutzrichtlinie² in österreichisches Recht, bringt zwar eine weit gehende Liberalisierung des Datentransfers innerhalb der EU, aber kein internationales Datenschutzrecht.

¹ Siehe dazu die Kurzkommentare von *Mayer-Schönberger/Brandl*, Datenschutzgesetz 2000 (Wien 1999), *Duschaneck/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (Wien 2000), *Drobosch/Grosinger*, Das neue österreichische Datenschutzgesetz (Wien 2000) und den Lehrbuchbeitrag von *Jahnel*, Datenschutzrecht, in *Jahnel/Schramm/Staudegger* (Hrsg), Informatikrecht (Wien-New York 2000) 159.

² Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ABI 1995 L 281/31.

Daneben treten besondere Datenschutzbestimmungen, wie etwa im *Telekommunikationsgesetz* für Provider als Betreiber einer Telekommunikationseinrichtung.

Alle genannten datenschutzrechtlichen Regelungen *gelten für jede Art von Datenverarbeitung*, online ebenso wie offline, ja sogar für manuell geführte Karteien. Datenschutzrecht ist daher grundsätzlich auch auf eine Datenverarbeitung im Internet anwendbar. Beim Internet können sich allerdings zusätzliche Schwierigkeiten bei der Rechtsdurchsetzung ergeben, vor allem wenn die Datenverarbeitung ganz oder teilweise im Ausland stattfindet.

1.1. Grundrecht auf Datenschutz³

Zum Schutz der Privatsphäre einer natürlichen oder juristischen Person gewährt das Datenschutzrecht vor allem ein *Recht auf Geheimhaltung* personenbezogener Daten, soweit ein schutzwürdiges Interesse daran besteht. Dieses Recht kann insbesondere mit Zustimmung des Betroffenen oder zur Wahrung überwiegender berechtigter Interessen eines anderen eingeschränkt werden. Daneben treten die weiteren Rechte auf Auskunft, Richtigstellung und Löschung.

1.2. Personenbezogene Daten

Das DSG und damit auch das Grundrecht auf Datenschutz bezieht sich ausschließlich auf die Verarbeitung *personenbezogener Daten*. Das sind nach § 4 Z 1 DSG Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist. Darunter fallen auch „indirekt“ personenbezogene Daten, die der konkrete Verwender mit rechtlich zulässigen Mitteln nicht auf eine Person zurückführen kann (möglicherweise aber jemand anderer). Für die Verwendung nur indirekt personenbezogener Daten durch diesen Verwender gelten erleichterte Bestimmungen. Keine dem DSG unterliegende „Daten“ sind anonymisierte Daten, die niemand auf eine Person zurückführen kann.

Besonders schutzwürdig werden vom Gesetzgeber nach § 4 Z 2 DSG Daten von natürlichen Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben erachtet („sensible Daten“).

³ Vgl dazu *Jahnel*, Datenschutzrecht (FN 1) 166 und *Berka*, Lehrbuch Grundrechte (Wien/New York 2000) RZ 279 ff.

1.3. Zulässigkeit der Datenverwendung

Nach den allgemeinen Grundsätzen des § 6 Abs 1 DSGVO dürfen Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden. Sie müssen für den Zweck der Datenanwendung wesentlich sein und dürfen über diesen Zweck nicht hinausgehen. Sie müssen sachlich richtig sein und dürfen nur so lange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist.

Für die Frage, ob eine konkrete Datenverwendung zulässig ist, sieht das DSGVO eine *zweistufige Zulässigkeitsprüfung* vor: Zunächst ist der Zweck der Datenverarbeitung anhand der Berechtigung des Auftraggebers zu überprüfen. In einem zweiten Schritt ist zu ermitteln, ob schutzwürdige Geheimhaltungsinteressen verletzt werden, wobei zwischen „sensiblen“ und „nicht-sensiblen“ Daten zu unterscheiden ist.

Bei nicht-sensiblen Daten liegt nach § 8 Abs 1 DSGVO kein schutzwürdiges Geheimhaltungsinteresse vor, wenn

- eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung der Daten besteht
- oder der Betroffene der Verwendung der Daten zugestimmt hat,
- oder lebenswichtige Interessen des Betroffenen die Datenverwendung fordern
- oder überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten die Verwendung erfordern.

2. Speichern von Cookies⁴

Unter „Cookies“ versteht man Informationsstücke, die ein Informationsanbieter im World-Wide-Web (WWW) erstellt und die am Computer des im Internet surfenden Anwenders gespeichert werden, bereit für spätere Zugriffe durch diesen Informationsanbieter. Cookies sind in die Informationen, die zwischen Anwender und Informationsanbieter ausgetauscht werden, so eingebettet, dass der Speichervorgang meist völlig unbemerkt vom Anwender erfolgt. Zwar lassen sich die wichtigsten Internet-Browser so einstellen, dass Cookies gar nicht oder nur mit Zustimmung abgespeichert werden. Wenn man diese Option wählt, wird man

⁴ Vgl dazu *Brandl/Mayer-Schönberger*, CPU-IDs, Cookies und Internet-Datenschutz, *ecolx* 1999, 367.

allerdings so häufig um Zustimmung zum Abspeichern eines Cookies gefragt – selbst dort, wo man es gar nicht erwarten würde, wie etwa bei Abfragen im Rechtsinformationssystem des Bundes (RIS) – dass ein sinnvolles Arbeiten im Internet praktisch unmöglich wird.

Die Gründe für die Verwendung von Cookies sind durchaus unterschiedlich: So wird etwa bei einem Einkauf über das Internet der „Warenkorb“ während des virtuellen Einkaufs in einem Cookie zwischengespeichert, es können persönliche Einstellungen für eine Anwendung gespeichert, oder der letzte Besuch auf einer Site festgehalten werden, etwa um Informationen anzubieten, die sich seither verändert haben. Schließlich ist es sogar möglich, ein Passwort in einem Cookie zu speichern, so dass dieses nicht mehr jedes Mal eingegeben werden muss. Durch den Einsatz von Cookies wird erreicht, dass beim nächsten Besuch der Site die getroffenen Einstellungen oder eine Auswahl (etwa von Waren) wieder hergestellt werden können, wenn der Betrachter zwischenzeitlich etwa auf einen anderen Server wechselt oder seinen Computer ausschaltet.

Die Gefahr, die von den Cookies ausgeht, liegt darin, dass eine Statistik über die letzten Besuche auf Web-Sites geführt werden und daraus auf persönliche Interessen und Vorlieben geschlossen werden kann. Dies kann in weiterer Folge etwa zur Einblendung spezifischer Werbung auf der Site selbst oder zur Zusendung unerwünschter Werbezusendungen führen. Daneben kann die Auswertung dieser Daten aber Kenntnisse von sensiblen Informationen über eine Person bringen. Zu denken ist etwa an den Besuch einer Site mit Informationen über ansteckende Krankheiten, religiöse Sekten, mit rechtsextremen oder pornografischen Inhalten.

Aus datenschutzrechtlicher Sicht stellt sich zunächst die Frage, ob Cookies überhaupt personenbezogene Daten darstellen und damit in den Anwendungsbereich des DSGVO fallen.⁵ Wie sehen diese Cookies in der Realität aus? Zur Demonstration dazu drei Zeilen aus der auf meinem PC gespeicherten Datei „cookies.txt“:

```
www.amazon.de TRUE/ FALSE 969231388 session-id-time 969231600
www.digicenter.at FALSE / FALSE 1031820565 RoxenUserID 0x21
ww.astound.com FALSE / FALSE 1293753600 WEBTRENDS_ID
141.201.51.42-2630877744.29367636.
```

⁵ Vgl dazu *Brandl/Mayer-Schönberger*, CPU-IDs, Cookies und Internet-Datenschutz, *ecolex* 1999, 367, die diese Frage etwas allgemein und undifferenziert bejahen (368).

Auf den ersten Blick handelt es sich um kryptische Zahlenkombinationen, die keinerlei Personenbezug erkennen lassen. Tatsächlich können Cookies für den Informationsanbieter, der auf sie zugreift, zunächst nur einen Maschinenbezug herstellen. Damit es sich nach § 4 Z 1 DSGVO um personenbezogene Daten handelt, muss aber die Identität des Betroffenen bestimmt oder bestimmbar sein. Es kommt also darauf an, ob es im konkreten Fall für denjenigen, der das Cookie verwendet, über diesen Maschinenbezug hinaus möglich ist, einen Bezug zu einer konkreten Person herzustellen. Dies kann etwa über eine Verknüpfung mit User- und Passworteingaben (etwa nach einer Bestellung) oder mit E-Mail-Adressen erfolgen. In diesem Fall sind Cookies jedenfalls personenbezogene Daten.

Ein Beispiel für diese Verknüpfung bildet etwa ein Einkauf beim Internetanbieter „Amazon“. Hier wird man nach dem ersten Einkauf beim nächsten Besuch der Site mit dem eigenen Namen freundlich begrüßt. Hier erfolgt also ein Personenbezug durch Verknüpfung zwischen dem auf der Festplatte gespeicherten Cookie und der Kundendatei.

Cookies können aber auch „indirekt personenbezogene Daten“ enthalten, nämlich dann, wenn zwar nicht der Informationsanbieter selbst, sondern jemand anderer die Identität des Betroffenen bestimmen kann. Ist dieser Bezug für niemanden herstellbar, enthält das Cookie keine personenbezogene Daten.

Wie sieht es nun mit der Zulässigkeit des Abspeicherns von Cookies durch den Informationsanbieter, der Auftraggeber im Sinne des § 4 Z 4 DSGVO ist, auf der lokalen Festplatte des Anwenders (Betroffener iSd § 4 Z 3 DSGVO) aus? Dabei ist zwischen personenbezogenen und nur indirekt personenbezogenen Daten zu unterscheiden. Cookies ohne Personenbezug fallen ohnehin nicht unter das DSGVO. Zunächst ist zu prüfen, ob Zweck und Inhalt der Cookies von der gesetzlichen Zuständigkeit oder den rechtlichen Befugnissen des Auftraggebers gedeckt sind. Diese Voraussetzung ist etwa beim Warenkorb-Cookie eines gewerblichen Internetanbieters erfüllt. Die zweite Voraussetzung für die Zulässigkeit ist, dass keine schutzwürdigen Geheimhaltungsinteressen des Betroffenen verletzt werden. Diesbezüglich ist zwischen personenbezogenen und indirekt personenbezogenen Daten zu unterscheiden. Nach § 8 Abs 2 DSGVO gelten bei der Verwendung von nur indirekt personenbezogenen Daten schutzwürdige Geheimhaltungsinteressen als nicht verletzt.

Anders sieht die Beurteilung aus, wenn ein Cookie (nicht nur indirekt) personenbezogene Daten enthält. Die Zulässigkeitsvoraussetzung einer ausdrücklichen gesetzlichen Ermächtigung oder Verpflichtung zur Datenverwendung scheidet in der Regel ebenso aus wie das Vorliegen von le-

benswichtigen Interessen des Betroffenen. In Frage käme allenfalls die Zustimmung des Betroffenen zur Datenverwendung als Internet-Anwender. Unter "Zustimmung" versteht § 4 Z 14 DSGVO die gültige, insbesondere ohne Zwang abgegebene Willenserklärung des Betroffenen, dass er in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten einwilligt. In den Fällen, in denen der Betroffene von der Speicherung der Cookies gar nichts weiß, weil der Browser in der standardmäßigen Einstellung Cookies ohne Warnung akzeptiert, liegt keine derartige Einwilligung vor. Selbst wenn man sich die Warnung vor den Speichern anzeigen lässt, sind die Informationen, die man dabei erhält derartig kryptisch, dass nicht von „Kenntnis der Sachlage“ gesprochen werden kann. Selbst bei einem Einblick in die tatsächlich gespeicherten Daten werden – wie das oben abgedruckte Beispiel zeigt – Inhalt und Konsequenz der gespeicherten Daten keineswegs deutlich.

Bleibt also nur noch die Generalklausel des § 8 Abs 1 Z 4 DSGVO, wonach überwiegende berechnigte Interessen des Auftraggebers oder eines Dritten die Verwendung erfordern müssen. Aus den dazu in § 8 Abs 3 DSGVO genannten Beispielen könnte am ehesten noch die Z 4 herangezogen werden, wonach die Datenverwendung zur Erfüllung einer vertraglichen Verpflichtung zwischen Auftraggeber und Betroffenen erforderlich sein muss. Das Speichern des (personalisierten) „Warenkorbes“ auf der Festplatte des Anwenders etwa wird danach bis zur Absendung der Bestellung zulässig sein. Nach Absenden der Bestellung ist ein weiteres Speichern für die Abwicklung der vertraglichen Beziehung aber nicht mehr erforderlich und die Daten sind daher zu löschen, was in der Praxis häufig nicht geschieht.