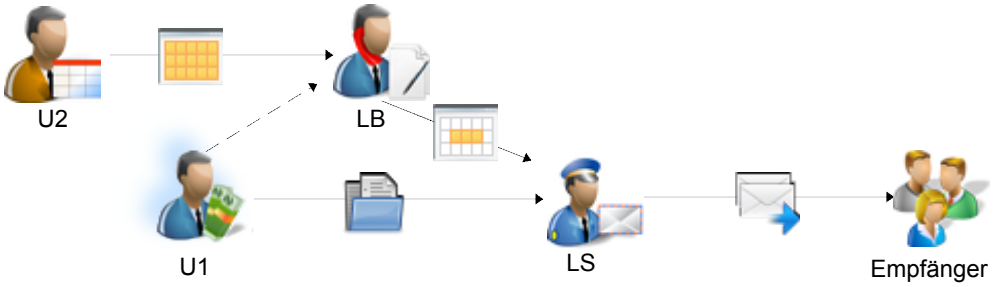
DBSC Infoletter Datenschutz-Praxis ► 2012-04

Lettershops und Listbroker - Werbung für Dritte

Werbung für Dritte kann im Wege des Listbrokings im s.g. Lettershopverfahren erfolgen. Ein Unternehmen, das als Listeigner bezeichnet wird, stellt dabei seine Kundendaten, vermittelt durch einen Adresshändler (Listbroker), für fremde Werbung zur Verfügung. Dabei kommt es nicht zu einer Datenübermittlung an das Unternehmen, für den Ware oder Leistungen geworben wird. Bis zur Kontaktaufnahme durch den (neuen) Kunden bleibt dieser dem werbenden Unternehmen zunächst unbekannt.

Ein drittes Unternehmen, der Lettershop, ein spezialisierter Auftragsdatenverarbeiter für Direktwerbung, bringt nun bereitgestelltes Werbematerial und Adressmaterial zusammen und versendet es. Das Unternehmen, das die Daten für Werbezwecke zur Verfügung gestellt hatte, ist dabei im Werbematerial erkennbar zur machen.

Beispiel:



Unternehmen U1 möchte bei Personen, die nicht zu seinem Kundenkreis gehören, für seine Produkte und Leistungen werben. Dafür wird ein Listbroker eingeschaltet, der seine Daten von Unternehmen U2 erhält und für die Werbeaktion bereitstellt. Unternehmen U1 beauftragt Lettershop LS mit dem Versand von Werbematerial, auf dem erwähnt ist, dass die Daten von U2 stammen.

Dieses Vorgehen ist nach § 28 Abs. 3 Satz 5 BDSG zulässig, so weit dabei sog. Listendaten verwendet werden. Zu solchen Listendaten gehören auch der Name, der Vorname und die Anschrift. Außerdem muss in dem Werbeschreiben die verantwortliche Stelle für die Nutzung der personenbezogenen Daten genannt werden. Dies erfolgt durch den Zusatz „Verantwortliche Stelle im Sinne des Bundesdatenschutzgesetzes ist … (z. B. die U2 GmbH)“. Die verantwortliche Stelle speichert die personenbezogenen Daten der Betroffenen. An diese Stelle können Betroffene jederzeit ihren Widerspruch gegen künftige Werbesendungen richten.

Die Rechtsgrundlage für den geschäftsmäßigen Adresshandel bildet § 29 BDSG. Gesetzlich erlaubt ist nach wie vor der Adresshandel mit Listendaten, d. h. die Übermittlung dieser Daten zu beliebigen Werbezwecken, sofern die Lieferkette nach § 28 Abs. 3 Satz 4 BDSG („Transparente Übermittlung“) dokumentiert ist. Die Übermittlung ist nach §34 Abs. 1a BDSG für die Dauer von 2 Jahren nach der Übermittlung zu speichern und dem Betroffenen ist auf Verlangen Auskunft über die Herkunft die Daten und die Empfänger zu erteilen.

Link: DDV Qualitäts- und Leistungsstandards (QuLS) der Councils DirectMail Services und Listbroker
http://www.deutschepost.de//mlm.nf/dpag/images/download/dokumentation/_download_dokumentation_qualitaets_leistungsstandards.pdf

Videoüberwachung von Privat- und Intimsphäre

Im vergangenen Jahr ist der Einsatz von Videoüberwachungsanlagen durch Unternehmen und andere private Datenverarbeiter weiter stark angestiegen. Das belegt die Vielzahl der Beschwerden von betroffenen Menschen, die den LfDI Berlin erreicht hat. Auffällig ist dabei, dass immer häufiger Videokameras in öffentlich zugänglichen Bereichen installiert wurden, die als sensitiv einzustufen sind. Als sensitiv werden Bereiche bezeichnet, in denen Personen ihre religiösen oder philosophischen Überzeugungen, ihre politische Gesinnung oder ihre Sexualität frei entfalten können.

Zu sensitiven Bereichen gehören zum Beispiel:

- Eingangsbereiche zu Kirchen, Partei- und Gewerkschaftsräumen
- Nachtclubs und Bordelle
- HIV-/AIDS-, Suchtberatungsstellen oder Treffpunkte von Homosexuellen
- Umkleidekabinen in Kaufhäusern, Frei- und Hallenbädern
- Behandlungszimmer von Arztpraxen oder sonstigen medizinischen Einrichtungen zumindest dann zu, wenn die Videoaufnahmen Rückschlüsse auf die Krankheit einer bestimmten Person zulassen
- in Freizeit- und Erholungseinrichtungen Dusch-, Umkleide- und Wellness-Bereiche

Einige verantwortliche Stellen geben als Grund für die Installation von Videokameras in ihren Einrichtungen die steigende Anzahl von Diebstählen an. Durch die erhebliche Eingriffsintensität in die Privat- und Intimsphäre der Besucherinnen und Besucher sind jedoch die schutzwürdigen Interessen der Betroffenen höher zu gewichten als die berechtigten Interessen der Verantwortlichen Stelle.

Die Entscheidung, ob eine Videoüberwachung in sensitiven Bereichen zulässig ist, kann nur im Einzelfall getroffen werden. Die für die Videoüberwachungsmaßnahme verantwortliche Stelle hat – ggf. mit ihrem betrieblichen Datenschutzbeauftragten – vorab zu prüfen, ob eine Kamerainstallation zulässig sein kann. Nach § 6b Abs. 1 Nr. 3 BDSG ist die Videoüberwachung nur zulässig, so weit sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Feststellung: In der Regel ist die Videoüberwachung in sensitiven Bereichen unzulässig. In Ausnahmefällen muss ihre datenschutzrechtliche Zulässigkeit nach §§ 6b und 28 BDSG geprüft werden.

Quelle: Tätigkeitsbericht 2011 des Berliner Beauftragten für Datenschutz und Informationsfreiheit

---

Facebook Like Button

Durch die Einbindung des Like Buttons auf einer Website erhält Facebook Kenntnis darüber, dass eine Nutzerin oder ein Nutzer (repräsentiert durch die IP-Adresse) diese Website aufgerufen hat.

In der gegenwärtigen Realisierung erfolgt dies bereits beim Aufruf der Seite, d.h. nicht erst beim Betätigen des Buttons. Damit erhält Facebook auch Informationen über Nicht-Mitglieder. Handelt es sich bei der Nutzerin oder dem Nutzer um ein angemeldetes Facebook-Mitglied, wird diese Information über ein vorhandenes Facebook-Cookie namentlich zugeordnet.

Heise Security: „Für den Like-Button bindet die Web-Seite einen s.g. iFrame ein. Das ist eine kleine Mini-Seite innerhalb der Seite, deren Quelltext von Facebook selber stammt. Ruft man etwa eine Spiegel-Online-Seite auf, bettet diese sofort den Facebook-Frame ein – also bevor der Anwender auf "Gefällt mir" geklickt hat. ... Dabei sendet der Browser an Facebook unter anderem als Referer die URL der gerade geöffneten Spiegel-Seite. Außerdem schickt er dem Facebook-Server auch das von ihm bereits früher gesetzte Cookie. Ist der Anwender gerade in einem anderen Fenster bei Facebook angemeldet, enthält das seine Sitzungs-ID. Damit kann Facebook diesen Aufruf der Spiegel-Seite einer konkreten Person zu ordnen.“ ...

§ 15 Abs. 3 TMG sieht vor, dass über die Inanspruchnahme von Telemedien durch die Nutzerinnen und Nutzer Nutzungsprofile gebildet werden dürfen, dies aber nur in pseudonymisierter Form und in Verbindung mit einer entsprechenden Unterrichtung der Betroffenen. Sie müssen zudem die Möglichkeit haben, der Bildung der Profile zu widersprechen.

Feststellung: In der gegenwärtigen Form trägt der Like Button dem nicht Rechnung. Vor diesem Hintergrund erscheint die Nutzung von Like Buttons durch öffentliche Stellen problematisch. Das s.g. „2-Klick-Verfahren“ entschärft die Problematik. Danach erscheint beim Lenken des Cursors auf einen Button eine Information über die Funktionsweise und die Folgen des Anklickens des eigentlichen Social Plugins, das erst nach dem Anklicken des ersten Buttons erscheint. Das Anliegen, die Betroffenen umfassend über die Verarbeitung ihrer Daten zu informieren, kann allerdings auch auf diese Art nicht erfüllt werden, weil Facebook bislang darüber noch keine verlässlichen und umfassenden Angaben zur Verfügung stellt.

Link: Heise Verlag: http://www.heise.de/ct/artikel/2-Klicks-fuer-mehr-Datenschutz-1333879.html und http://www.heise.de/security/artikel/Das-verraet-Facebooks-Like-Button-1230906.html

Quelle: Landesbeauftragter Datenschutz und Informationsfreiheit, Tätigkeitsbericht 2010/2011