

Neuaufgabe des Leitfadens „Kundendatenschutz“

Die persönliche Ansprache des zielgruppengerechten Konsumenten durch die Anbieter von Waren oder Dienstleistungen gehört zu den effizientesten Mitteln der Kundengewinnung und -bindung. Allerdings: Nicht alles, was technisch möglich ist - und betriebswirtschaftlich vielleicht durchaus interessant erscheint - lässt sich auch einwandfrei realisieren. Der Grund liegt in den engen rechtlichen Grenzen, die zahlreiche Gesetze – zum Beispiel das Gesetz gegen den unlauteren Wettbewerb (UWG) oder das Bundesdatenschutzgesetz (BDSG) - dem Gestaltungs- und Variantenreichtum von Direktmarketingmaßnahmen setzen.

Der von der Gesellschaft für Datenschutz und Datensicherheit e.V. (GDD) gemeinsam mit dem Zentralverband der deutschen Werbewirtschaft e.V. (ZAW) und mit Unterstützung durch den Deutschen Industrie- und Handelskammertag (DIHK) herausgegebene Leitfaden „Kundendatenschutz“ soll zum einen einen praxisorientierten Überblick vermitteln: über rechtmäßige Maßnahmen, aber auch unerlaubte Aktionen, über die Rechtspositionen des umworbenen Kunden als dem sogenannten „Betroffenen“ und über die bestehenden Kontrollmechanismen.

Zum anderen soll er - und das ist das eigentliche Anliegen der beiden Herausgeberorganisationen - denjenigen Unternehmen Hilfestellung bieten, die das Medium der Direktwerbung und Methoden des Customer Relationship Managements in ihre Vertriebsstrukturen integriert haben.

Der Leitfaden beinhaltet die Beschreibung typischer Abläufe, Fallgestaltungen und rechtlicher Probleme

und will damit auch die Möglichkeit einer „Parallelwertung“ anderer vergleichbarer, hier ausdrücklich nicht angesprochener Verfahren eröffnen.

Anlass für die nunmehr dritte Auflage sind die für die Verarbeitung und Nutzung von Kundendaten mit den Novellen I bis III im September 2009 eingefügten Änderungen des BDSG. Berücksichtigt wurden außerdem die auf Grundlage der UWG-Novelle 2008 beziehungsweise des Gesetzes zur Bekämpfung unerlaubter Telefonwerbung und zur Verbesserung des Verbraucherschutzes bei besonderen Vertriebsformen (in Kraft seit: 4. August 2009) erfolgten Neuregelungen.

Die Neuaufgabe wurde außerdem dazu genutzt, Ausführungen der Voraufgabe zu überarbeiten und zu ergänzen. Dadurch hat sich der Umfang des Werks um rund 100 Seiten erhöht. Es hat daher den Charakter eines Handbuchs zum Kundendatenschutz angenommen. Neue Schwerpunkte wurden schließlich im Bereich der Web-Analyse und der Online-Werbung gesetzt.

Der aktuelle Leitfaden kann zum Preis von EUR 34,90 zuzüglich Versandkosten bei der Geschäftsstelle der GDD, Pariser Str. 37, 53117 Bonn, info@gdd.de oder über das Bestellformular unter www.gdd.de/gdd-arbeitshilfen/gdd-ratgeber/ratgeberbestellen bestellt werden. ■

Stichworte: Kundendatenschutz, Leitfaden

Artikel 29-Gruppe: Stellungnahme zur Anwendbarkeit europäischen Datenschutzrechts

Am 16. Dezember 2010 hat die Artikel 29-Gruppe eine Stellungnahme (8/2010) zum anwendbaren Recht angenommen und diese in der ersten Januarwoche 2011 veröffentlicht. Die Stellungnahme bietet viele praktische Anleitungen zum Anwendungsbereich des europäischen Datenschutzrechts und zu den Implikationen von Artikel 4 der Datenschutzrichtlinie 95/46/EG.

Von DR. JÖRG HLADJK, LL.M., Brüssel.*

Ziel der Stellungnahme ist es, den aktuellen Anwendungsbereich des europäischen Datenschutzrechts in Bezug auf die Verarbeitung von personenbezogenen Daten innerhalb und außerhalb des Europäischen Wirtschaftsraums (EWR) klarzustellen. Die Ausführungen der Datenschutzgruppe sind

darauf angelegt, Rechtssicherheit für Verantwortliche der Datenverarbeitung herzustellen, um einen klareren Rechtsrahmen für die Betroffenen und die Interessengruppen zu bieten und um rechtliche Lücken und potentielle Konflikte zwischen sich überschneidenden nationalen Datenschutzgesetzen zu vermeiden.

Zur Veranschaulichung finden sich durchweg praktische Beispiele, wie beispielsweise im Kontext von zentralisierten HR-Datenbanken, Geolokalisierungsdiensten, Cloud Computing und sozialen Netzwerken. Darüber hinaus beinhaltet die Stellungnahme Vorschläge zur Verbesserung der bestehenden Vorschriften zum anwendbaren Recht, die im Zusammenhang mit der anstehenden Revision der allgemeinen Richtlinie 95/46/EG (im folgenden: „Richtlinie“) zu sehen sind.

Bisherige Kernvorschriften

Die Kernvorschrift der Richtlinie zum anwendbaren Recht ist Artikel 4, nach dem jeder Mitgliedstaat seine eigenen nationalen Rechtsvorschriften anzuwenden hat in Fällen:

“(…) wo die Verarbeitungen im Rahmen der Tätigkeiten einer Niederlassung ausgeführt werden, die der für die Verarbeitung Verantwortliche im Hoheitsgebiet dieses Mitgliedstaats besitzt (Artikel 4 Abs. 1 a), oder

„wenn ein Verantwortlicher, der nicht im Gebiet der Gemeinschaft niedergelassen ist, aber zum Zwecke der Verarbeitung personenbezogener Daten auf automatisierte oder nicht automatisierte Mittel zurückgreift, die im Hoheitsgebiet des betreffenden Mitgliedstaats belegen sind, es sei denn, dass diese Mittel nur zum Zweck der Durchfuhr durch das Gebiet der Europäischen Gemeinschaft verwendet werden (Artikel 4 Abs. 1 c).“

Klarstellungen

Die neue Stellungnahme kann für die Interpretation von Artikel 4 der Richtlinie als Leitfaden angesehen werden. Nach Auffassung der Datenschutzgruppe hat Artikel 4 Abs. 1 a) folgende Bedeutung:

Wenn eine verantwortliche Stelle eine Niederlassung im EWR hat, findet nur ein nationales Recht Anwendung für den EWR, abhängig vom Ort der Niederlassung (mit Ausnahme der Datensicherheitsmaßnahmen, für die möglicherweise die nationalen Gesetze des Staates in dem der Auftragsdatenverarbeiter seinen Sitz hat zur Anwendung kommen); und

Wenn eine verantwortliche Stelle mehrere Nieder-

lassungen im EWR hat, korrespondiert die Anwendung des nationalen Rechts mit den Aktivitäten jeder Niederlassung. Dies bedeutet: Wenn eine verantwortliche Stelle Niederlassungen in mehreren Staaten hat, können mehrere nationale Gesetze auf die Datenverarbeitung Anwendung finden, abhängig vom Grad der Teilnahme der einzelnen Niederlassung an der Datenverarbeitung.

Um festzustellen, welche nationalen Gesetze auf welche Datenverarbeitungen Anwendung finden, beschreibt die Datenschutzgruppe einige wesentliche Konzepte und stellt folgendes klar:

Eine Niederlassung auf dem Gebiet eines Mitgliedstaats impliziert die tatsächliche Ausübung von Aktivitäten durch stabile Einrichtungen, unabhängig davon, ob die Niederlassung eine Rechtspersönlichkeit hat.

Der Begriff „im Kontext von Aktivitäten einer Niederlassung“ bedeutet, dass der Ort, wo sich die Daten befinden oder wo die verantwortliche Stelle ihren Sitz hat, nicht relevant ist für die Entscheidung, welches Recht Anwendung findet. Vielmehr ist es der Ort der Niederlassung, welche die Datenverarbeitungsaktivitäten ausführt, der betrachtet werden soll. Das Maß der Beteiligung dieser Niederlassung an den Verarbeitungsaktivitäten und die Art dieser Aktivitäten sind ebenso wesentlich für die Entscheidung, welches nationale Recht Anwendung findet. Eine solche Analyse basiert auf einem funktionalen Ansatz, der danach fragt, was die wirkliche Rolle jeder beteiligten Niederlassung ist und welche Aktivität im Kontext welcher Niederlassung stattfindet.

Die Datenschutzgruppe äußert sich auch klarstellend zu Artikel 4 Abs. 1 c) bezüglich verantwortlicher Stellen, die ihren Sitz außerhalb des EWR haben und führt dazu folgendes aus:

Artikel 4 Abs. 1 c) findet nur Anwendung, wenn Artikel 4 Abs. 1 a) nicht anwendbar ist (wenn die verantwortliche Stelle also keine Niederlassung hat, die relevant für die fraglichen Aktivitäten im EWR ist). Artikel 4 Abs. 1 c) soll jedoch Anwendung finden, obwohl die verantwortliche Stelle eine Niederlassung im EWR hat, wenn die Datenverarbeitung nicht im Kontext dieser Niederlassung stattfindet (wenn also die Niederlassung im EWR nicht hinreichend in die Datenverarbeitung involviert ist).

Die Datenschutzgruppe versteht den Begriff „Mittel“ dahingehend, dass er unter Umständen technische und manuelle Hilfsmittel (wie beispielsweise Fragebögen) umfasst. Die Datenschutzgruppe ist der Auffassung, dass diese weite Interpretation

manchmal zu unerwünschten Ergebnissen führt und schlägt daher einige Verbesserungen zu diesen Regelungen vor.

Verbesserungsvorschläge

Der wesentliche Vorschlag der Datenschutzgruppe zur Verbesserung von Artikel 4 Abs. 1 a) besteht darin, zum Herkunftslandprinzip zurückzukehren. Dies würde bedeuten, dass nur das nationale Recht desjenigen Mitgliedstaats Anwendung findet, in dem sich die Hauptniederlassung der verantwortlichen Stelle befindet. Entsprechend des aktuellen „verteilten Ansatzes“ können unterschiedliche nationale Gesetze auf verschiedene Niederlassungen der verantwortlichen Stelle im EWR Anwendung finden, abhängig vom Kriterium des „Kontexts der Aktivitäten“. Eine weitere Harmonisierung der nationalen Gesetze, und auch der Datensicherheitsanforderungen wäre notwendig um so genanntes „Forum Shopping“ zu vermeiden.

Für Artikel 4 Abs. 1 c), der Situationen betrifft, wo die verantwortliche Stelle außerhalb des EWR ansässig ist, schlägt die Datenschutzgruppe vor, dass zusätzliche Kriterien entwickelt werden, um sicherzustellen, dass eine hinreichende Verbindung mit dem EWR besteht.

Zunächst schlägt die Datenschutzgruppe die Einführung eines Konzepts „gezielte Ansprache von Kunden“ oder „dienstleistungsorientierten Ansatzes“ vor. Nach diesen Kriterien wären nationale Datenschutzgesetze nur anwendbar, wenn Kunden

im EWR gezielt angesprochen würden. Die Datenschutzgruppe merkt an, dass dieser Ansatz den von der U.S. Federal Trade Commission verwendeten Kriterien im Zusammenhang mit der Durchsetzung des Children's Online Privacy Protection Acts sehr ähnlich wäre. Dieses Gesetz findet unter anderem Anwendung, wenn Kinder in den USA mittels einer Website gezielt angesprochen werden.

Zudem soll das Kriterium „Nutzung von Mitteln“ neu definiert werden. Die aktuelle Anwendung dieses Kriteriums hat zu unerwünschten Ergebnissen geführt, wie beispielsweise die umfassende Anwendung europäischen Datenschutzrechts. Die Datenschutzgruppe rät dazu, dass dieses Kriterium aus einer Grundrechtsperspektive beibehalten werden kann. Nach Auffassung der Datenschutzgruppe sollten in diesen Fällen aber nur wenige Datenschutzgrundsätze Anwendung finden, wie beispielsweise die Grundsätze zur Zulässigkeit der Datenverarbeitung und zur Datensicherheit.

Schließlich verlangt die Datenschutzgruppe eine größere Harmonisierung und Klarstellung hinsichtlich der Anforderung, dass verantwortliche Stellen, die außerhalb des EWR ansässig sind, einen Vertreter innerhalb des EWR bestellen. ■

* Der Autor ist Rechtsanwalt in der europäischen Datenschutzpraxis der Kanzlei Hunton & Williams, Brüssel.

Internet: http://ec.europa.eu/justice/policies/privacy/docs/wp-docs/2010/wp179_en.pdf

Stichworte: Artikel 29-Gruppe, Europäische Datenschutzrichtlinie, anwendbares Recht (Europa)

Weniger Anonymität durch neuen Internet-Standard IPv6

Die Umstellung der IP-Adressen von der Version 4 (IPv4) auf neue IP-Adressen der Version 6 (IPv6) läuft auf vollen Touren. Davon betroffen sind in erster Linie Provider und Netzbetreiber. Endkunden bemerken von der Umstellung fast nichts. Die zweite Hälfte der neuen IPv6-Adressen, der sogenannte Interface Identifier, ist allerdings gerätespezifisch und wird häufig aus Hardware-Kennungen des Systems abgeleitet.

Daher lassen sich Geräte (und damit oft deren Nutzer) über Netzgrenzen verhältnismäßig einfach wiedererkennen – man braucht sich lediglich auf die zweite Hälfte der IPv6-Adresse zu beschränken. Die Folge: Weniger Anonymität.

Abhilfe ist in Form sogenannter „Privacy Extensions“ zwar möglich; viele Smartphones verhindern aber deren Einsatz.

Von DR. THOMAS PROBST, Kiel.

Die Umstellung auf längere IP-Adressen (128 bit) vergrößert den Adressraum ganz enorm – als Beispiel werden die Sandkörner dieser Erde herangezogen, die man theoretisch mit IP-Adressen versorgen könnte. Der Adressraum der IPv4-Adressen umfasst dagegen nur 32 bit (theoretisch etwa 4 Milliarden Adressen) und ist fast vollständig vergeben – nicht zuletzt, weil man zu Beginn der Adressvergabe damit relativ großzügig umging.