

Nutzungsdaten im Internet: Was darf der Content-Anbieter speichern ?

Ein aktuelles Urteil des Landgerichts Darmstadt zur Zulässigkeit der Aufbewahrung von personenbezogenen Daten löst Verunsicherung unter Content-Anbietern im Internet aus. Das Urteil wirft die die Frage auf, ob ein Diensteanbieter Daten seiner Kunden, die bei der Nutzung des Dienstes im Internet anfallen, überhaupt speichern darf und, falls er dies darf, wann er diese Daten löschen muss (Urteil vom 25.1.2006, Aktenzeichen: 25 S 118/2005. Das Urteil war zum Zeitpunkt der Erstellung dieses Artikels noch nicht veröffentlicht).

In dem konkreten Fall eines Internet-Access-Providers (t-online), der seinem Kunden eine Flatrate zur Internetnutzung zur Verfügung gestellt hatte, stellte das Gericht fest: Die durch den Provider mitgespeicherten dynamischen IP-Adressen, die dem Nutzerrechner zugeordnet werden, stellen personenbezogene Daten dar, die sofort nach Beendigung der jeweiligen Internetverbindung zu löschen sind. Angaben zu dem vom Provider während der Internet-Verbindung mitgespeicherten und übertragenen Datenvolumen dürfen erst gar nicht erhoben werden.

Drei Arten von personenbezogenen Daten

Das Gericht bezog sich zur Begründung dieser Entscheidung in erster Linie auf Datenschutzvorschriften des Telekommunikationsgesetzes (TKG), die vor allem für solche Anbieter einschlägig sind, die – wie Internet-Access-Provider – eine Datentransportleistung erbringen. Das vorliegende Urteil gibt aber ebenso Content-Providern, die Inhalte wie Wirtschafts- oder Presseinformationen online zum Abruf anbieten, einen Newsletter verschicken, eine Homepage vorhalten, oder sonstige elektronische Informationsangebote unterhalten oder Solche Dritter anbieten, dringend Anlass, ihr Vorgehen bei der Aufbewahrung von Nutzungsdaten zu überdenken. Grund: Die Vorgaben des Teledienstedatenschutzgesetzes (TDDSG) bzw. des Mediendienstestaatsvertrags (MDStV) für die Aufbewahrung von Nutzungsdaten, die für online erbrachtes Content-Providing einschlägig sind, sind inhaltlich mit den TKG-Bestimmungen vergleichbar, die für das Gericht jetzt im Fall von t-online ausschlaggebend waren.

Das Gesetz unterscheidet grundlegend zwischen drei Typen von personenbezogenen Daten: Bestands-, Nutzungs- und Abrechnungsdaten. Zu den Bestandsdaten zählen solche Daten, die für die vertragliche Grundlage zwischen Anbieter und Kunde wichtig sind, d.h. für die Begründung, inhaltliche Ausgestaltung und Änderung des Vertrags über die Nutzung des Dienstes. Man kann sie auch schlicht als Identifikationsdaten bezeichnen. Dies können sein: Der Name einer Person, ihre Anschrift, Bankverbindung, E-Mail-Adresse, Telefon- oder Telefaxnummer und die vom Diensteanbieter dem Kunden zugeteilte User-ID.

Unter Nutzungsdaten sind hingegen solche Daten zu verstehen, die die tatsächliche Inanspruchnahme des Dienstes eines Content-Providers überhaupt erst ermöglichen. Bei einem Datenbankdienst sind dies beispielsweise die personenbezogenen Daten, die bei der Durchführung des online-Datenabrufs durch den Kunden anfallen.

Typischerweise kann es sich dabei um Angaben über Beginn und Ende der Nutzung oder auch um Angaben zur übertragenen Datenmenge handeln. Auch Identifikationsdaten können bei der Nutzung anfallen – insoweit entstehen Überschneidungen zu der Gruppe der Bestandsdaten.

Abrechnungsdaten sind hingegen solche personenbezogenen Daten, die ebenfalls bei der Inanspruchnahme eines Dienstes anfallen, aber nur seiner Abrechnung dienen. Für diese drei Datengruppen sieht das Gesetz unterschiedliche Speichervorschriften vor, die der Diensteanbieter einhalten muss.

Es kommt auf das einzelne Geschäftsmodell an

Die richtige Einordnung von Daten in Bestands-, Nutzungs- und Abrechnungsdaten und die korrekte Einhaltung der sich daraus ergebenden unterschiedlichen Vorschriften für die Datenspeicherung sind eine Herausforderung für den Content-Anbieter. Denn es gilt der Grundsatz: Als Bestands-, Nutzungs- oder Abrechnungsdatum überhaupt erhoben und gespeichert werden darf nur, was für den konkreten Zweck unbedingt *erforderlich* ist, also Identifikation, Ermöglichung der Nutzung des Dienstes, Abrechnung. Und: Daten dürfen auch nur solange gespeichert werden, wie sie für den jeweiligen Zweck erforderlich sind. Danach sind sie sofort zu löschen. Sind also einmal gespeicherte Nutzungsdaten für die Ermöglichung des Datenabrufs nicht mehr notwendig und auch für eine Rechnungsstellung nicht mehr erforderlich, müssen sie gelöscht werden.

Wichtig auch: Was erforderlich ist, bestimmt sich nach dem Geschäftsmodell und der technischen Ausgestaltung des Dienstes im Einzelfall. Unterscheidet man daher, sehr vereinfacht, folgende drei Möglichkeiten, Content online zu vertreiben, so ergibt sich folgendes Bild: Für einen Dienst – kostenfrei und ohne Vertragsbindung – ist bereits die Erhebung und Speicherung von Daten wie Name, Adresse u.ä. als "Bestandsdaten" nicht erforderlich und damit unzulässig. Hier besteht nämlich kein Vertrag, für dessen Abwicklung sie erforderlich wären.

Ein Dienst hingegen, der den Informationsabruf nach übertragener Datenmenge abrechnet, wird Identifikationsangaben zum Kunden sowie Angaben zur abgerufenen Datenmenge speichern dürfen. Nicht speichern darf er jedoch Informationen zum Zeitpunkt des Datenabrufs, wie es jetzt das Landgericht Darmstadt im Flatrate-Fall entscheiden hat. Soweit es also keine besonderen technischen Erfordernisse gibt, sind solche Daten weder als Nutzungsdaten für die Bereitstellung des Dienstes, noch als Abrechnungsdaten für die Rechnungsstellung erforderlich. Eine Speicherung ist folglich unzulässig. Dagegen wird die Speicherung von Informationen zur übertragenen Datenmenge dann unzulässig, wenn ein Dienst volumenunabhängig abrechnet.

Prävention statt Reaktion

In der Konsequenz heißt das für Content-Anbieter: Die Einhaltung der vom Gesetzgeber standardmäßig vorgegebenen Datenverarbeitungsvorschriften bezüglich der beim Content-Providing anfallenden personenbezogenen Daten ist nicht ohne Probleme für den Anbieter. Und hinzukommt: Nicht nur die eingangs erwähnten

Gesetze wie TDDSG und MDStV müssen vom Content-Provider beachtet werden. Auch die angebotenen Inhalte selbst enthalten unter Umständen personenbezogene Daten, für die weitere datenschutzrechtliche Vorschriften wie das Bundesdatenschutzgesetz Sonderregelungen vorsehen.

Zusätzliche Fragen, inwieweit IP-Adressen der Kundenrechner vom Content-Anbieter mitprotokolliert werden dürfen – das Landgericht Darmstadt hatte dies für den Access-Provider stark begrenzt – müssen von den Anbietern ebenfalls gelöst werden. Provider sehen sich so gezwungen, die vertragliche und technische Ausgestaltung ihres Dienstes auf das einschlägige Datenschutzrecht anzupassen. Denn die Rechtsfolgen für Verstöße können, neben einem Imageschaden, erheblich sein. Es drohen Unterlassungs- und Schadensersatzansprüche der Betroffenen sowie Bußgelder durch die Aufsichtsbehörde.

Eine solche passive Anpassung des Dienstes auf das Datenschutzrecht kann jedoch nicht im Sinne eines funktionierenden Geschäftsmodells sein. Sinnvoll ist nur der entgegengesetzte, aktive Weg: Diensteanbietern ist, am besten vor ihrem Online-Gang, dringend zu empfehlen, die Grenzen für die Verarbeitung von personenbezogenen Daten auf ihr individuelles Geschäftsmodell hin auszurichten. Hierzu sollten sie auf die ihnen zur Verfügung stehenden rechtlichen Möglichkeiten, wie spezielle Nutzervereinbarungen und die Einholung von datenschutzrechtlichen Einwilligungen, zurückgreifen.

Rechtsanwältin Simona Keßler, Düsseldorf
E-Mail: skessler@kessler-recht.de
Fon: 0211/4976883-0
Fax: 0211/4976883-9