

Dr. Jörg Hladjk, LL.M.

EU-Datenschutzrecht und Geolocation-Services

Am 16. Mai 2011 hat die Artikel 29-Gruppe eine Stellungnahme (13/2011) zu Geolocation-Services auf intelligenten mobilen Endgeräten angenommen. Sie beschreibt den Rechtsrahmen sowie die Verpflichtungen im Zusammenhang mit Geolocation-Services (zum Beispiel Ortungs- und Navigationssysteme, Geo-personalisierte Dienste, Geo-Tagging im Internet und Location Based Advertising).

Die Stellungnahme widmet sich einer Reihe von konkreten Datenschutzbedenken, die sich bei der Erbringung von Geolocation-Services durch die Nutzung bestimmter Infrastrukturmodelle ergeben können. Dies betrifft insbesondere GPS-Technologie (Satelliten-gestützte Technologie), GSM-Basisstationen (Antennen-gestützte Technologie) und WLAN-Router. Dabei wird insbesondere Augenmerk auf Dienstleistungen gelegt, die auf WLAN-Zugangspunkte (WiFi Access Points) gestützt werden und über eindeutige Identifikationsmerkmale, wie beispielsweise die sogenannten Medium-Access-Control (MAC)-Adressen, verfügen.

Keine Anwendbarkeit der E-Privacy-Richtlinie

Aus Sicht der Artikel 29-Gruppe ist die EG-Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG („E-Privacy-Richtlinie“) auf Geolocation-Services, die im Zusammenhang mit intelligenten mobilen Endgeräten erbracht werden, nicht anwendbar. Die Artikel 29-Gruppe vertritt die Ansicht, dass die Verarbeitung von Geodaten durch Unternehmen, die Geolocation-Dienste und -Anwendungen im Zusammenhang mit intelligenten mobilen Endgeräten (zum Beispiel Smartphones) erbringen, den Vorschriften der allgemeinen Datenschutzrichtlinie 95/46/EG („Datenschutzrichtlinie“) unterliegt. Gemäß der Artikel 29-Gruppe kann die E-Privacy-Richtlinie nur angewendet werden, wenn die Geodaten durch Betreiber von Telekommunikationsdiensten verarbeitet werden. Andere Unternehmen, die Geolocation-Dienste und -Anwendungen gestützt auf eine Kombination von Basisstationen, GPS und WLAN-Router erbringen, sind als Anbieter von „Diensten der Informationsgesellschaft“ zu qualifizieren und folglich nicht vom Anwendungsbereich der E-Privacy-Richtlinie erfasst.

Geodaten sind personenbezogene Daten

Nach Ansicht der Artikel 29-Gruppe sind Geo-

daten personenbezogene Daten. Insbesondere gelten Geodaten auch dann als personenbezogene Daten, wenn sie aus der Verknüpfung einer eindeutigen MAC-Adresse und des Standortes eines WiFi-Zugangspunktes abgeleitet werden können. Dies wird damit begründet, dass hierdurch Unternehmen, die Geolocation-Services im Zusammenhang mit intelligenten mobilen Endgeräten erbringen, Einzelpersonen indirekt identifizieren können. Diese indirekte Identifizierung reiche aus, um die erlangten Informationen als personenbezogene Daten im Sinne von Artikel 2 a) der Datenschutzrichtlinie zu qualifizieren. Es sei einem Anbieter von Geolocation-Diensten und -Anwendungen möglich, die genaue Lage eines WiFi-Zugangspunktes basierend auf der entsprechenden Signalstärke herauszufinden. Sobald die genaue Lage eines WiFi-Zugangspunktes bekannt ist, könne diese vom Diensteanbieter einem bestimmten Nutzer zugeordnet werden. Beispielsweise könne der Besitzer einer Wohnung oder eines Hauses, wo sich ein bestimmter WiFi-Zugangspunkt befindet, indirekt identifiziert werden.

Anbieter unterschiedlicher Dienstleistungen können verantwortliche Stelle sein

Sowohl Anbieter von Geolocation-Infrastrukturmodellen (zum Beispiel Betreiber von Datenbanken mit WLAN-Zugangspunkten) als auch solche von Geolocation-Diensten und -Anwendungen (zum Beispiel Anwendungen zur Händlersuche oder Wettervorhersage) sowie Entwickler von Betriebssystemen können unter Umständen alle jeweils verantwortliche Stelle für die Datenverarbeitung sein. Daher müssen alle diese Anbieter die Anforderungen der Datenschutzrichtlinie erfüllen.

Einwilligung in vielen Fällen notwendig

Die Artikel 29-Gruppe stellt fest, dass Geodaten in den meisten Fällen nur mit vorheriger Einwilligung der Nutzer verarbeitet werden dürfen. Die

Stichworte

Artikel 29-Gruppe
Geolocation-Services
ortsbasierte Dienste
Europa
E-Privacy-Richtlinie
Europäische Datenschutzrichtlinie



Einwilligung muss konkret, informiert und freiwillig sein und soll jederzeit widerrufen werden können. Die Artikel 29-Gruppe führt weiterhin aus, dass „Opt-out-Mechanismen“ sowie Geolocation-Dienste, die als Voreinstellung standardmäßig aktiviert sind, nicht ausreichen, um diese Anforderungen zu erfüllen.

Darüber hinaus ist die Artikel 29-Gruppe der Ansicht, dass die Nutzer mindestens einmal im Jahr ihre Zustimmung erneuern sollen. Zudem thematisiert die Stellungnahme die Einwilligung von Arbeitnehmern und Kindern.

Ausreichende Unterrichtung erforderlich

Die verantwortliche Stelle muss die Nutzer über die Datenverarbeitung auf klare, umfassende, verständliche und leicht zugängliche Weise unterrichten. Die Form der Unterrichtung darf das hauptsächliche Ziel, den Nutzern klare Informationen zur Verfügung zu stellen, nicht beeinträchtigen. Die Artikel 29-Gruppe hebt hervor, dass die Gültigkeit der Einwilligung mit der Qualität der Unterrichtung der Nutzer über die Verarbeitung ihrer Daten eng zusammenhängt. Ferner fordert die Artikel 29-Gruppe alle beteiligten Akteure im Bereich der Geolocation-Dienste auf, intensiv zusammenzuarbeiten und „Best Practices“ für die Bereitstellung von entsprechenden Unterrichtungen der Nutzer zu entwickeln.

Geltendmachung der Nutzerrechte

Anbieter von Geolocation-Diensten und -Anwendungen müssen den Nutzern ermöglichen, ihre Rechte auf Auskunft, Berichtigung und Löschung ihrer Daten uneingeschränkt auszuüben. Dies schließt auch das Recht auf Auskunft über Nutzerprofile ein, die mit Hilfe von personenbezogenen Daten erstellt wurden, sowie das Recht, die Berichtigung und Löschung solcher Profile verlangen zu können. Die Artikel 29-Gruppe unterstützt die Einrichtung von Online-Plattformen, die Nutzern einen sicheren Zugang zu ihren Daten ermöglichen.

Schnellstmögliche Löschung

Die verantwortliche Stelle muss Richtlinien zur Aufbewahrung von Geodaten und Nutzerprofilen, die auf solchen Daten basieren, implementieren. Danach sollen Geodaten nur so lange aufbewahrt werden, wie es für die Erfüllung der Zwecke, für die sie erhoben wurden, notwendig ist. Geodaten sind also zu löschen oder zu anonymisieren, sobald sie nicht länger für die Zwecke, für die sie ursprünglich erhoben wurden, erforderlich sind. In diesem Zusammenhang schlägt die Artikel 29-Gruppe vor, dass Unique Identifiers (zum Beispiel MAC-Adressen) nur für 24 Stunden gespeichert werden sollen. Danach sollten diese Daten gelöscht oder anonymisiert werden.

Internet

http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp184_en.pdf

Stichworte

§ 25c KWG
Beschäftigtendatenschutz
Compliance
Korruptionsprävention
Revision
§ 32 BDSG

Dr. Martin Eßer

Der neue § 25c KWG - Aufdeckung von Straftaten in Kreditinstituten

Mitten in der Diskussion um die gesetzliche Neuregelung des Beschäftigtendatenschutzes hat der Gesetzgeber mit Wirkung vom 9. März 2011 eine neue gesetzliche Grundlage im Kreditwesengesetz geschaffen. Sie erlaubt es Kreditinstituten, routinemäßige Kontrollen von Beschäftigtendaten durchzuführen. Unsicherheiten, die diesbezüglich seit der im Jahre 2009 erfolgten Einführung des viel diskutierten § 32 BDSG zur Regelung des Beschäftigtendatenschutzes entstanden waren, sind mit der Neufassung von § 25c des Gesetzes über das Kreditwesen (Kreditwesengesetz - KWG) weitgehend ausgeräumt. Dies gilt allerdings nur für Unternehmen, die in den Anwendungsbereich des KWG fallen.

Kontrolldichte in Kreditinstituten

Kreditinstitute sind regulatorisch dazu verpflichtet, zur Vorbeugung und Verhinderung von Geldwäsche, Terrorismusfinanzierung oder sonstiger strafbarer Handlungen, die zu einer Gefährdung des Vermögens des Instituts führen können, angemessene geschäftsbezogene (und kundenbezogene) Sicherungssysteme zu unterhalten, zu

aktualisieren und Kontrollen durchzuführen. Das regelte § 25c Abs. 1 KWG bereits in alter Fassung. Darüber hinaus gibt es weitere spezialgesetzliche Überwachungs- und Kontrollpflichten, die nicht nur Kreditinstitute treffen. So haben Vorstände von Aktiengesellschaften nach § 91 Abs. 2 Aktiengesetz (AktG) geeignete Maßnahmen zu treffen, um den Fortbestand der Gesellschaft gefährdende

Dr. Martin Eßer ist Datenschutzbeauftragter einer Bundesbehörde.