Newsletter Datenschutz

Ausgabe 02 | 2024

Navigieren per Smartphone: praktisch oder riskant?

Ihr Datenschutz-Info Blatt

Liebe Leserin, lieber Leser,

wenn es um den Schutz personenbezogener Daten geht, muss man oftmals genauer hinschauen. So könnten Kalender-Apps auf Ihrem Smartphone nicht nur Ihnen einen Terminüberblick geben, sondern ungewollt auch Dritten. Die Navigation mit Ihrem Smartphone könnte ebenfalls ungeahnte Nebenwirkungen haben und zu heimlichen Bewegungsprofilen führen.

Auch die Aufnahmefunktionen Ihres Smartphones für Gesprächsmitschnitte sollten Sie nicht unüberlegt einsetzen. Wie diese neue Ausgabe erklärt, kann dies schwerwiegende rechtliche Konsequenzen haben.

Der Datenschutz kann aber auch überraschende finanzielle Vorteile für Sie bringen, wenn Sie zum Beispiel die Kopie Ihrer Patientenakte von einem Arzt verlangen. Hier gibt es ein neues, spannendes Urteil des Europäischen Gerichtshofs, das Ihnen in dieser Ausgabe erläutert wird.

Ihr Frank Berns, Datenschutzbeauftragter

Heimliche Aufzeichnung von Gesprächen?

Später noch einmal Zugriff auf den genauen Wortlaut eines Gesprächs zu haben – das wäre manchmal schon sehr interessant. Die Aufzeichnung mit dem Handy funktioniert problemlos. Wenn man will, merken die anderen gar nichts davon. Aber ist so etwas zulässig?

Gründe für eine Aufzeichnung scheint es genug zu geben

Gesprochene Worte sind flüchtig. Manches ist nach einem Gespräch schnell vergessen. Anderes interpretieren die Beteiligten im Nachhinein unterschiedlich. Die Idee, ein Gespräch deshalb lieber aufzuzeichnen, liegt nahe. Dann steht fest, was gesagt worden ist. Alle können es dann später noch anhören. Das scheint eine gute Basis, um spätere Meinungsunterschiede oder gar spätere Streitigkeiten zu vermeiden.

Die meisten lehnen eine solche Aufzeichnung allerdings ab

Wenn alle Beteiligten damit einverstanden sind, ist die Aufzeichnung eines Gesprächs rechtlich gesehen kein Problem. Dies setzt voraus, dass alle Beteiligten von der Aufzeichnung wissen. Wer eine

solche Aufzeichnung ins Spiel bringt, wird allerdings rasch merken: Einverstanden mit einer solchen Aufzeichnung sind die wenigsten. Ganz im Gegenteil kann ein solcher Vorschlag dazu führen, dass sich das Gesprächsklima sofort deutlich abkühlt. Nur selten gelingt es, die Zustimmung aller Gesprächspartner zu einer Aufzeichnung zu erreichen.

Einfach heimlich vorzugehen ist keine gute Idee

Schon vom Gefühl her sind heimliche Aufzeichnungen nichts Gutes. Eigentlich. Aber wie sieht es aus, wenn man eine solche Aufzeichnung „nur für sich" macht und sie wirklich an niemanden weitergibt? Als eine Art interne Gedächtnisstütze wird das doch wohl erlaubt sein? Das Gesetz akzeptiert nicht einmal das. Ganz im Gegenteil. Ein Blick in das Strafgesetzbuch zeigt Folgendes: Wer unbefugt das nicht öffentlich gesprochene Wort eines anderen auf einen Tonträger aufnimmt, wird bestraft. Und zwar meist mit einer Geldstrafe, doch ist sogar eine Freiheitsstrafe von bis zu drei Jahren möglich (siehe § 201 Abs. 1 Nr. 1 Strafgesetzbuch).

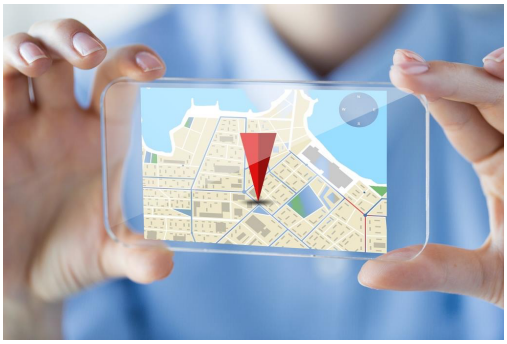
Nahezu alle heimlichen Aufzeichnungen sind unbefugt

Das Gesetz verbietet nur unbefugte Aufzeichnungen. Das legt den Gedanken nahe, dass es auch befugte Aufzeichnungen gibt. Eröffnet das eine Hintertür, die man nur geschickt nutzen muss? Solche Überlegungen führen in die Irre. Weder Konfliktgespräche mit Vorgesetzten noch Verhandlungen mit Geschäftspartnern, die sich später an nichts mehr erinnern wollen, sind Fälle, in denen eine Aufzeichnung befugt wäre. Dass eine Aufzeichnung später noch nützlich sein könnte, gibt für sich allein keine Befugnis für eine Aufzeichnung.

Eine wichtige Ausnahme gibt es aber doch

Manchmal sind Worte ein Instrument, um Straftaten zu begehen. Ein Gesprächspartner droht im Gespräch unter vier Augen mit unliebsamen Enthüllungen, wenn er kein Schweigegeld bekommt. Oder ein Gesprächspartner fängt bei Verhandlungen mittels Telefons an, den anderen grob zu beleidigen. Das sind dann Situationen, in denen Sie absolut befugt sind, eine heimliche Aufzeichnung zu beginnen. Denn wie sonst sollten Sie das strafbare Verhalten des anderen nachweisen können?

Navigieren per Smartphone: praktisch oder riskant?



Das Smartphone hat die klassischen Navigationsgeräte nahezu verdrängt. Egal ob man beruflich oder privat unterwegs ist – das Smartphone zeigt den Weg. Die Frage ist allerdings, wer alles diesen Weg nachverfolgen kann.

Smartphones sind Multifunktionsgeräte

Smartphones sind zu Geräten für alle Lebenslagen geworden. Andere Geräte, wie etwa Navigationsgeräte und digitale Kompaktkameras, sind dadurch für viele Nutzerinnen und Nutzer überflüssig geworden.
Möglich geworden ist dies zum einen durch die leistungsstarke Hardware der Smartphones, die in aller Regel auch über GPS-Sensoren verfügen, die früher Navigationsgeräten vorbehalten waren.

Zum anderen sind es die Apps, die Smartphones so vielseitig machen. Apps zur Navigation werden nicht nur bei Wanderungen oder zu Fuß in der Innenstadt genutzt. Während der privaten oder beruflichen Autofahrt sind diese Anwendungen ebenfalls vielfach im Einsatz. Navigations-Apps gehören inzwischen zu den beliebtesten Applikationen für Smartphones, denn sie erscheinen wirklich hilfreich. Und in den meisten Fällen sind sie das auch.

Navi-Apps sind nicht nur bei Nutzerinnen und Nutzern beliebt

Die hohe Verbreitung von Navigations-Apps hat aber auch Schattenseiten. Damit ist nicht nur gemeint, dass so manches Werbeunternehmen nur zu gern die Standortdaten der App-Nutzenden haben möchte, um die Online-Werbung passender und relevanter zu machen. Zweifellos hat die Werbung für ein Restaurant mehr Aussicht auf Erfolg, wenn man sich in der Nähe befindet.

Doch neben der Werbeindustrie sind auch die Datendiebe an den Navigations-Anwendungen auf Smartphones interessiert. Dabei versuchen sie nicht nur, an die Daten legitimer Navigations-Apps zu gelangen. Sie bringen auch eigene Navi-Apps in Umlauf, leider mit großem Erfolg.

Online-Betrug und Datendiebstahl per Navi-App

IT-Sicherheitsprovider warnen regelmäßig vor Betrugsmaschen mit Fake-Apps. So wurden schon mehrfach kostenpflichtige gefälschte Navi-Apps im Google Play Store entdeckt. Statt des versprochenen Zusatznutzens boten diese Apps lediglich die Funktionen von Google Maps und zogen dem Anwender dafür Geld aus der Tasche. Viele Nutzerinnen und Nutzer im Play Store fallen auf die überwiegend guten Bewertungen herein, doch auch diese Bewertungen können gefälscht sein.

Der Zweck der vermeintlichen Navi-Apps war nicht nur, Geld zu generieren. Die Anwendenden zahlten gleich doppelt: mit ihren Nutzungsdaten und dem Kaufpreis für eine App, deren Funktionen es bei Google Maps völlig kostenfrei gibt. Ein Teil dieser Apps verlangt vom Anwendenden zum Beispiel Zugriffsrechte auf die Kontakte und das Telefonbuch – ein deutlicher Hinweis auf Datenschutz-Probleme.

Für berufliche wie auch private Smartphone-Nutzer und -Nutzerinnen bedeutet das: Auch kostenpflichtige Apps können zusätzlich Nutzungsdaten stehlen. Ohne Schutzsoftware auf dem Smartphone sollte man also gar nichts installieren.

Nicht nur Navi-Apps nutzen die Ortung

Betrügerische Navi-Apps nutzen auch die Standortdaten mehrfach. Zum einen für den angeblichen Navigationsdienst, der in Wirklichkeit von Google Maps erbracht wird. Zum anderen aber können sie die Standortdaten auch an Datendiebe liefern, die so Bewegungsprofile der ahnungslosen Nutzerinnen und Nutzern erhalten.

Diese Bewegungsprofile werden verkauft und zu weiteren kriminellen Aktivitäten missbraucht. Polizeibehörden haben bereits berichtet, dass solche Bewegungsprofile bei Entführungen genutzt wurden.

Nicht nur kriminelle Navigations-Apps sammeln heimlich und unerlaubt Standortdaten, auch andere Apps versuchen, Berechtigungen für Standortdaten zu erhalten, ohne diese für den gewünschten Zweck zu benötigen. Hier ist große Vorsicht angesagt, Datenminimierung und minimale Berechtigungen sind Trumpf.

Terminkalender-Apps: Fast wie ein Schwarzes Brett

Geht es um eine Terminabstimmung, greifen viele inzwischen zu ihrem Smartphone. Einige Kalender-Apps sind aber keine einfachen Terminkalender, sondern kleine Plaudertaschen.

Der offene Terminkalender

Ging es früher darum, einen freien Termin zu suchen, griff man in die Hand- oder in die Jackentasche und brachte ein kleines Büchlein zum Vorschein, den Terminkalender. Nur unter Freunden konnte es passieren, dass man seinen Terminkalender offen auf den Tisch legte, sodass auch das Gegenüber einen Blick auf die Terminlücken werfen konnte. Den Kalender einem Dritten hinüberzureichen, wäre undenkbar gewesen.

Heute ist das anders: So mancher hat einen offenen Terminkalender, in den Dritte schauen können. Allerdings geschieht das nicht bewusst, sondern ungewollt.

Smartphones ersetzen klassische Kalender

Besondere Vorsicht ist angezeigt, wenn das Smartphone, genauer gesagt eine Terminkalender-App, den Papier-Kalender ersetzt. Viele Smartphone-Nutzende verwenden mittlerweile ihr mobiles Gerät als Kalender oder Terminplaner. Die meisten Smartphones nutzen gegenwärtig das Android-Betriebssystem, und dort gibt es als führende Kalender-App den Google-Kalender.

Die Google-Kalender-App hat viele auf den ersten Blick praktische Funktionen, die aber auf den zweiten Blick zeigen, wie stark die Daten im Terminkalender ausgewertet werden und wie leicht andere Personen Zugang zu ihnen bekommen könnten.

Nicht nur Google Assistant könnte mitlesen

Google beschreibt die Funktionen seiner Kalender-App unter anderem so: Flüge, Hotelbuchungen, Konzerte, Tischreservierungen und andere Termine aus dem E-Mail-Dienst Gmail werden auf Wunsch automatisch zum Kalender hinzugefügt. Mithilfe von intelligenten Vorschlägen für Termintitel, Orte und Personen lassen sich neue Termine schnell erstellen. Man fügt Kolleginnen und Kollegen als Gäste hinzu, und der Google-Kalender hilft dabei, die besten Besprechungszeiten zu suchen.

Virtuelle Assistenten wie Google Assistant durchsuchen den Kalender und geben Hinweise, wann man aufbrechen muss, um rechtzeitig anzukommen. Gibt man an, an welchem Ort ein Termin stattfindet, bekommt man nicht nur passende Stadtpläne und Bilder des Ortes angezeigt, auch die Werbung passt zu den Terminen.

Die mit KI (Künstlicher Intelligenz) versehenen Dienste wie Google Assistant können auf Wunsch automatisch Termine auf den Kalender zu setzen, eine Übersicht über die Termine geben oder Termine passend verschieben. Bei den Geräten mit integriertem Assistant können Nutzende per Sprachbefehl Termine hinzufügen oder Fragen zu Terminen stellen. Dazu müssen die Termine aber auf den Google-Servern liegen, sie sind also nicht mehr im „geschlossenen Terminbüchlein".

Diese Beispiele zeigen: Mit unbedachten Klicks und Einstellungen könnten Kolleginnen, Kollegen, Kunden und andere Personen, die man trifft, ungewollt Einsicht in Termine bekommen. Anders als beim Termin-Büchlein befinden sich die Termindaten auf den Servern des Betreibers wie Google.

Datenschutz-Einstellungen und eine genaue Durchsicht der Datenschutzerklärung und der Berechtigungen für die App sind bei einem Smartphone-Kalender absolute Pflicht. Sonst könnte der eigene Kalender zum Schwarzen Brett im Internet werden.

Kostenlose Kopien von Behandlungsunterlagen

Manchmal braucht ein Patient eine Kopie von Behandlungsunterlagen, etwa wegen Schadensersatzansprüchen nach einem Behandlungsfehler. Die Kosten von Kopien können erheblich sein. Ein Streit darüber kam bis zum Europäischen Gerichtshof (EuGH). Dabei ging es aber noch um einiges mehr als „nur" um Geld.

Ausgangspunkt war ein Besuch beim Zahnarzt

Ein Patient war mit seiner Zahnärztin nicht zufrieden. Er hatte den Verdacht, ihre Behandlung sei fehlerhaft gewesen. Deshalb forderte er von ihr eine Kopie seiner Patientenakte. Zu einer solchen Kopie war die Zahnärztin bereit. Allerdings verlangte sie vom Patienten die Erstattung der Kosten dafür. Das sah der Patient nicht ein. Nach seiner Auffassung gibt ihm die DSGVO das Recht auf eine kostenlose Kopie.

Das deutsche Recht ist hinsichtlich Kosten für Kopien eher ärztefreundlich

Die Zahnärztin sah dies völlig anders. Sie verwies auf eine Regelung des BGB. Nach ihr hat ein Patient zwar einen Anspruch auf eine Kopie seiner Behandlungsunterlagen. Allerdings muss er die Kosten tragen, die dem Arzt oder Krankenhaus entstehen (siehe § 630g Abs. 1 BGB).

Das weicht von den Vorgaben der DSGVO ab

Diese Regelung beißt sich ersichtlich mit den Vorgaben der DSGVO. Danach gilt die Grundregel, dass betroffene Personen ein Recht auf „Gratis-Auskunft" über ihre Daten haben (siehe Art. 12 Abs. 5 Satz 1 DSGVO). Für Kopien von Daten ist geregelt, dass nur für „weitere Kopien" ein Entgelt verlangt werden kann. Daraus folgt, dass die „erste Kopie" kostenlos sein muss (Art. 15 Abs. 3 Satz 2 DSGVO.

Strittig war, ob sich das mit der DSGVO vereinbaren lässt

Dass die DSGVO als EU-Recht den Vorrang vor dem BGB als deutsches Recht hat, ist ein fester Grundsatz. Deshalb kann es auf den ersten Blick verwundern, dass ein Streit über Kosten von Kopien überhaupt bis zum Europäischen Gerichtshof (EuGH) kommen konnte. Unter bestimmten Voraussetzungen erlaubt die DSGVO jedoch, dass die Mitgliedstaaten das Auskunftsrecht beschränken.

Dreh- und Angelpunkt ist die Berücksichtigung wirtschaftlicher Interessen

Deshalb stellte sich die Frage: Sind die wirtschaftlichen Interessen von Ärzten und Kliniken als „Rechte und Freiheiten anderer Personen" anzusehen, die eine Abweichung von den Vorgaben der DSGVO

erlauben? Falls ja, läge in der Regelung des BGB für Kosten von Kopien eine zulässige Abweichung von der DSGVO. Denn Art. 23 Abs. 1 Buchst. i DSGVO erlaubt es, das Auskunftsrecht der DSGVO zugunsten der Rechte und Freiheiten anderer Personen einzuschränken.

Der EuGH setzt dafür klare Grenzen

Den EuGH schienen solche Überlegungen fast schon etwas zu verwundern. Für ihn steht fest: Die erste Kopie, die ein Patient von seinen Daten fordert, muss kostenlos sein. Er verweist dazu auf den Wortlaut der DSGVO. Er erlaubt lediglich, für jede „weitere Kopie" Kosten zu erheben. Dann muss aber die erste Kopie logischerweise kostenlos sein.

Neben der DSGVO ist kein Platz für andere Kostenregelungen

Ferner argumentiert der EuGH, dass die DSGVO in Sonderfällen durchaus die Erhebung von Kosten erlaubt. Beispiele dafür sind offenkundig unbegründete oder häufig wiederholte Anträge (siehe Art. 12 Abs. 5 Satz 1 DSGVO). Damit berücksichtigt die DSGVO selbst die wirtschaftlichen Interessen der Stellen, die zur Auskunft verpflichtet sind. Deshalb besteht kein Spielraum mehr dafür, dass der deutsche Gesetzgeber durch eine Regelung im BGB solche wirtschaftlichen Interessen noch ein zweites Mal berücksichtigt. Die Kostenregelung des BGB darf deshalb neben der DSGVO nicht angewandt werden.

Dem Patienten ging es um „datenschutzfremde Zwecke"

Zahnärztin und Patient waren sich jedoch auch noch in einer anderen Frage nicht einig. Der Patient hatte offen gesagt, dass er die Kopie seiner Behandlungsunterlagen für einen möglichen Haftungsprozess gegen die Zahnärztin benötigt. Damit verfolgte er ein völlig anderes Ziel als die Überprüfung des Datenschutzes. Das sah die Zahnärztin nicht ein. Dafür sei der Auskunftsanspruch nach der DSGVO nicht da.

Nach Auffassung des EuGH geht das jedoch in Ordnung

Der EuGH stört sich schon daran, dass ein Verantwortlicher überhaupt fragt, warum jemand Auskunft über seine personenbezogenen Daten verlangt. Die DSGVO lege nirgends fest, dass eine betroffene Person ihren Antrag auf Auskunft begründen muss. Deshalb dürfe sie auch nicht danach gefragt werden, worum es ihr bei der Auskunft geht. Sollte eine betroffene Person dazu von sich aus etwas sagen, ändert das nichts am Ergebnis. Auch dann hat sie Anspruch auf Auskunft über ihre Daten.

Die Entscheidung hat große praktische Bedeutung

Für das gesamte Gesundheitswesen ist nunmehr klar, dass Patienten eine Kopie (nicht: mehrere Kopien) der Behandlungsunterlagen kostenlos bekommen müssen. Nicht nur dort, sondern generell gilt außerdem: Betroffene Personen haben auch dann ein Auskunftsrecht, wenn sie die Auskunft für Rechtsstreitigkeiten in Gerichtsverfahren verwenden wollen.

Hier finden Sie die vollständige Entscheidung

Wer das Aktenzeichen C-307/22 in eine Suchmaschine eingibt, findet die Entscheidung des EuGH vom 26. Oktober 2023 weit oben in der Ergebnisliste.

Schützen Sie sich vor heimlicher Ortung? Machen Sie den Test!

Frage: Smartphone-Apps nutzen Standortdaten nur zur Navigation. Stimmt das?

1. Nein, viele Apps versuchen, Zugriff auf die Daten zum Standort zu erlangen, auch wenn sie diese Daten für ihren Zweck nicht benötigen.
2. Ja, nur die Apps, die eine Navigation ermöglichen, verlangen nach den Standortdaten.

Lösung: Die Antwort 1. ist richtig. Nicht nur die Apps, die Standortdaten zur Navigation benötigen, verlangen Zugriff auf die Daten zum Standort. Selbst scheinbar nützliche Apps, die zum Beispiel ein Smartphone in eine Taschenlampe wandeln, wollen oftmals Berechtigungen für Standortdaten, die offensichtlich nicht erforderlich sind. Deshalb sollten Sie bei jeder App die Berechtigungen prüfen, die diese bereits hat oder aber haben möchte. Bei Android-Smartphones tippen Sie auf die App, deren Berechtigungen Sie prüfen möchten. Tippen Sie dann auf Berechtigungen. Wenn Sie die Einstellung für eine Berechtigung ändern möchten, tippen Sie auf diese und wählen Sie Zulassen oder Ablehnen aus.

Frage: Kostenpflichtige Apps sammeln nicht zusätzlich heimlich Daten der Nutzenden. Stimmt das?

1. Ja, bezahlt man für eine App, finden keine heimlichen Datenauswertungen statt.
2. Nein, selbst Apps, die Geld kosten, können versuchen, zusätzlich Nutzungsdaten zu sammeln, um weiteren Gewinn zu machen.

Lösung: Die Antwort 2. ist richtig. Selbst Apps, die Geld kosten, könnten versuchen, zusätzlich Nutzungsdaten zu sammeln, um weiteren Gewinn zu machen. Besonders raffiniert sind Fake-Apps, die einen scheinbaren Nutzen versprechen, dafür Geld kosten und zusätzlich ohne informierte Einwilligung Daten sammeln, die für den gewünschten und bezahlten Zweck gar nicht erforderlich sind. Auch bei Bezahl-Apps sollten Sie also die Berechtigungen prüfen, die die App hat oder anfordert.

Impressum

Redaktion:
Frank Berns, Datenschutzbeauftragter, Geschäftsführer

Anschrift:
Konzept 17 GmbH
Westring 3
24850 Schuby
Amtsgericht Flensburg: HRB 12329
Telefon: 0049 4621 5 30 40 50
E-Mail: mail@konzept17.de