App-Überwachung

In zunehmendem Umfang erheben und verarbeiten Apps auf Smartphones personenbezogene Daten, die an den App-Anbieter oder den von der App genutzten Dienstanbieter übermittelt werden. Dazu zählen neben dem Nutzungsverhalten z. B. die Kontaktdaten (Telefonnummer, E-Mail-Adresse), der jeweilige Aufenthaltsort, der Inhalt von Suchanfragen, die Musik-Präferenzen (Streaming-Dienste), die Stimme (Sprachbefehle), Textnachrichten (Messenger), aufgenommene Bilder oder Produkte, für die sich der Nutzer interessiert (Preisvergleiche) und die Nutzung von E-Scootern, E-Rollern oder Leih-Fahrrädern – und vieles andere mehr.

Nach einer Langzeitstudie von ARD und ZDF[1] verbrachten die Deutschen im Jahr 2021 rund 3,4 Stunden täglich mit ihrem Smartphone – Tendenz stark steigend. Die dabei erhobenen und an Anbieter und Dienstleister übermittelten Daten liefern damit, einmal zusammengeführt, ein weit genaueres Verhaltensprofil, als Menschen sich das jemals für einen dystopischen Überwachungsstaat ausgemalt haben.

Jede App, die personenbezogene Daten verarbeitet, muss diese Verarbeitung in einer Datenschutzerklärung erläutern. Nur so ist eine „faire und transparente" Verarbeitung der Daten, wie von der DSGVO in Art. 13 (2) gefordert, möglich, da für einen Nutzer beispielsweise nicht offensichtlich ist, ob eine App die Verarbeitung lokal durchführt oder einen Cloud-Dienst in Anspruch nimmt. Geht die Verarbeitung über den eigentlichen Anwendungszweck der App hinaus, weil der Anbieter zusätzliche Daten für eigene (Marketing-) Zwecke erhebt, wie bspw. zur Bildung von Nutzerprofilen, oder gar Daten an Dritte (z. B. verbundene Unternehmen) weitergibt, ist eine Einwilligung der Betroffenen erforderlich – und die ist nur rechtswirksam, wenn sie informiert erfolgt.

Eine am 23.02.2023 veröffentlichte Forschungsstudie der Mozilla Foundation[2] zeigt nun, dass zahlreiche Anbieter dieser Pflicht nicht genügen: Von den 40 Apps mit den höchsten Download-Zahlen im Google Play Store stimmten bei fast 80% die Angaben in der Datenschutzerklärung nicht mit den Angaben der Entwickler in Googles Data Safety Form überein, deren Inhalte vor dem Download im Google Play Store angezeigt werden. Bei 40% der Apps waren die Abweichungen gravierend – so weisen beispielsweise weder TikTok noch Twitter ihre Datenweitergaben an Werbeplattformen aus. Eine auf solchen unvollständigen Informationen beruhende Einwilligung in die Verarbeitung ist damit unwirksam – und die Verarbeitung der Daten somit rechtswidrig.

Diese Ergebnisse sind alarmierend, denn die Studie untersuchte nur die Abweichung der Datenschutzerklärung von den Angaben der Entwickler im Play Store. Welche Daten von den Apps und den dahinter liegenden Plattformen tatsächlich verarbeitet und an Dritte weitergegeben werden, wurde nicht untersucht – hier könnten weitere Diskrepanzen bestehen. Außerdem ist zu befürchten, dass bei Apps mit geringerer Verbreitung eher mehr Abweichungen feststellbar sind als bei Apps von Anbietern großer Konzerne, denen inzwischen bekannt sein dürfte, dass in der EU bei derartigen Verstößen schmerzhafte Bußgelder drohen.

Dass die Aufsichtsbehörden sich dieses Problems noch nicht angenommen haben, lässt befürchten, dass sie derzeit so mit der Behandlung von Bagatellverstößen beschäftigt sind, dass ihnen keine Zeit für die wirklich relevanten Verstöße bleibt. Vielleicht müssen sich auch bei diesem Thema erst Datenschutzaktivisten wie Max Schrems durch die Instanzen klagen, damit der EuGH dazu eine bindende Entscheidung fällt.

Dirk Fox

1 https://www.ard-media.de/fileadmin/user_upload/media-perspektiven/pdf/2021/210708_Kupferschmitt_Mueller_Korr_2021-9-13.pdf

2 https://foundation.mozilla.org/de/campaigns/googles-data-safety-labels/