



MARKTWÄCHTER
DIGITALE WELT

verbraucherzentrale

WEARABLES, FITNESS-APPS UND DAS RECHT AUF AUSKUNFT: EIN PRAXISTEST

Untersuchung der Verbraucherzentralen
November 2017

INHALTSVERZEICHNIS

1. RECHT AUF AUSKUNFT	4
2. METHODE	5
3. ERGEBNISSE	7
3.1 Erster Kontaktversuch	7
3.2 Zweiter Kontaktversuch	8
4. ABSCHLUSSBETRACHTUNG	10
5. QUELLENVERZEICHNIS	12
6. ANHANG: ANTRAG AUF AUSKUNFT	13

1. RECHT AUF AUSKUNFT

Im April 2017 veröffentlichte das Projekt „Marktwächter Digitale Welt“¹ der Verbraucherzentralen und des Verbraucherzentrale Bundesverbands eine Untersuchung von zwölf Wearables und 24 Fitness-Apps.² Hierbei standen unter anderem das Datensendungsverhalten der geprüften Apps im Vordergrund sowie die Frage, wie Anbieter³ mit geltenden Datenschutzbestimmungen umgehen. Eine technische Prüfung hatte gezeigt, dass bei der Nutzung von Wearables und Fitness-Apps eine Fülle von zum Teil sensiblen personenbezogenen Daten erhoben und auf den Servern der Anbieter verarbeitet wird.

Die rechtliche Prüfung fokussierte sich unter anderem auch auf die Frage, inwieweit Anbieter der Informationspflicht nachkommen, die sie ihren Nutzern⁴ gegenüber haben. Denn: Anbieter müssen ihre Kunden darüber aufklären, welche Daten sie erheben und zu welchem Zweck sie verwendet werden.⁵ Dies tun sie in der Regel in ihren Hinweisen zum Datenschutz.⁶ Die Prüfung hatte ergeben, dass Anbieter dieser Informationspflicht oft nicht hinreichend nachkommen.

Über ihre allgemeine Informationspflicht hinaus müssen Anbieter nach § 34 Bundesdatenschutzgesetz (BDSG) ihren Nutzern auf Anfrage Auskunft darüber erteilen, welche personenbezogenen Daten sie über den Betroffenen gespeichert haben, aus welcher Quelle diese Daten stammen, an welche Empfänger beziehungsweise Kategorien von Empfängern die Daten weitergegeben wurden und zu welchem Zweck die Daten gespeichert werden. In ähnlicher Form sieht auch die Datenschutzgrundverordnung (DS-GVO) der Europäischen Union, die ab dem 25. Mai 2018 anwendbar ist, ein Auskunftsrecht vor. Dieses Recht auf Auskunft soll es Nutzern in erster Linie ermöglichen, Wissen darüber zu erlangen, welche Daten Anbieter von ihnen

gespeichert und gegebenenfalls weitergegeben haben. Nur dann können Verbraucher auch nachfolgende Maßnahmen einleiten: § 35 BDSG sieht vor, dass unrichtige personenbezogene Daten gegebenenfalls durch den Anbieter berichtigt werden müssen. Geregelt wird hier außerdem, dass in bestimmten Fällen personenbezogene Daten gelöscht werden können oder sogar müssen. Im § 35 BDSG ist das informationelle Selbstbestimmungsrecht ausgedrückt. Das Recht auf Berichtigung und das Recht auf Beseitigung unzutreffender personenbezogener Daten kann der Nutzer jedoch nur ausüben, wenn er Kenntnis darüber erhält, welche Daten der Anbieter überhaupt über ihn gespeichert hat.⁷

Daher ist es aus Sicht des Verbrauchers besonders wichtig, dass Nutzer ihr Recht auf Auskunft bei einem Anbieter geltend machen können, dessen Wearable beziehungsweise Fitness-App sie nutzen – nur so haben sie die Chance, die Verarbeitung ihrer teils sensiblen personenbezogenen Daten zu kontrollieren.

In einer bevölkerungsrepräsentativen Befragung gaben 15 Prozent der Teilnehmer an, schon einmal bei einem Unternehmen Auskunft über die dort gespeicherten personenbezogenen Daten beantragt zu haben.⁸ In der digitalen Welt scheint es jedoch schwierig für Verbraucher zu sein, tatsächlich ihrem Auskunftsanspruch nach entsprechend informiert werden zu können. So zeigten Herrmann und Lindemann (2016), dass nur 43 Prozent der im Rahmen der Studie 150 angeschriebenen App-Anbieter Auskunftersuchen zufriedenstellend beantworteten. Eine Studie des Citizen Lab in Kanada lieferte hierzu ähnliche Belege in Zusammenhang mit Anbietern von Wearables und Fitness-Apps.⁹

¹ Im Projekt „Marktwächter Digitale Welt“ beobachten und analysieren der Verbraucherzentrale Bundesverband (vzbv) unter Beteiligung der 16 Verbraucherzentralen den Markt in Deutschland, um Missstände früh zu erkennen und auf Fehlentwicklungen aufmerksam zu machen. Die Verbraucherzentrale NRW ist eine von fünf Schwerpunkt-Verbraucherzentralen im Projekt und beschäftigt sich mit Entwicklungen rund um das Thema Nutzergenerierte Inhalte.

² Moll, Schulze, Rusch-Rodosthenous, Kunke, & Scheibel, 2017; <http://www.marktwaechter.de/digitale-welt/marktbeobachtung/wearables-und-fitness-apps>

³ Unter „Anbieter“ wird im Rahmen der vorliegenden Untersuchung das Unternehmen verstanden, das das betreffende Wearable unter seiner Marke vertreibt. Dieses kann sowohl die Produktion der Hardware als auch die Programmierung einer kompatiblen Fitness-App an externe Dienstleister ausgelagert haben. Auch in Fällen, in denen der Anbieter nicht die datenverarbeitende Stelle ist, sondern hierfür einen Dienstleister beauftragt hat, ist er für den Umgang mit den personenbezogenen Daten verantwortlich, die in Zusammenhang mit der Nutzung seines Dienstes über seine Kunden erhoben, gespeichert und genutzt werden; § 11 Abs. 1 BDSG.

⁴ Aus Gründen der besseren Lesbarkeit wird im Folgenden mit „Nutzer“ (oder auch „Kunden“, „Verbraucher“ etc.) eine verkürzte, geschlechtsneutrale Formulierung verwendet. Der Text richtet sich daher sowohl an Verbraucherinnen als auch an Verbraucher. Diese Formulierungsregel gilt für die gesamte vorliegende Arbeit.

⁵ § 4 Abs. 3 BDSG, § 13 Abs. 1 TMG.

⁶ Hinweise zum Datenschutz werden von den Anbietern u.a. auch als Datenschutzbestimmung, -erklärung oder -richtlinie bezeichnet.

⁷ Schmidt-Wudy, 2017, § 34, Rn 2-3.

⁸ Die Ergebnisse der Verbraucherbefragung basieren auf einer repräsentativen Telefonbefragung mit 1055 Personen ab 14 Jahren, die in den letzten drei Monaten das Internet genutzt haben; Erhebungszeitraum: 25.08 – 29.09. 2016; durchführendes Institut: *mindline media GmbH*; Fehlertoleranz der Gesamtstichprobe: max. +/- 3 Prozentpunkte (bei einem Anteilswert von 50 Prozent). Die Befragung wurde im Auftrag des Projekts „Marktwächter Digitale Welt“ durchgeführt.

⁹ Hilt, Parson, & Knockel, 2016, S. 50ff.

Die vorliegende explorative Feldstudie untersucht daher folgende Fragen:

1. Inwieweit erhalten deutsche Verbraucher auf Basis des nach § 34 BDSG definierten Anspruchs bei ausgewählten Wearable-Anbietern Antwort auf ihr Auskunftersuchen?
2. Welchen Hindernissen begegnen Verbraucher, wenn sie einen Antrag auf Auskunft bei ausgewählten Wearable-Anbietern stellen?

2. METHODE

Zur Beantwortung der Forschungsfragen führte die Verbraucherzentrale Nordrhein-Westfalen (NRW) im Rahmen des Projekts „Marktwächter Digitale Welt“ die vorliegende Studie durch, in der die Reaktionen von Wearable-Anbietern auf Auskunftersuchen von Verbrauchern dokumentiert wurden.

ANBIETERAUSWAHL

Im Rahmen der genannten Vorgänger-Untersuchung wurden zwölf Wearable-Anbieter aufgrund ihrer globalen und nationalen Marktrelevanz ausgewählt und anschließend in die vorliegende Anschlussstudie aufgenommen.¹⁰ Hierzu zählten folgende Anbieter: *Apple*, *A-Rival*, *Fitbit*, *Garmin*, *Jawbone*, *Polar*, *Runtastic*, *Samsung*, *Striiv*, *Technaxx*, *Withings*¹¹ und *Xiaomi*. Das BDSG ist für alle angeschriebenen Anbieter mit Ausnahme von *Polar*, *Runtastic* und *Xiaomi* anwendbar.¹² Letztere wurden für eine bessere Vergleichbarkeit im Rahmen der vorliegenden Prüfung dennoch auf Basis des BDSG angeschrieben. Sich hieraus ergebende Verstöße sind für diese Anbieter unter Umständen nicht nach dem BDSG verfolgbar.

DATENGENERIERUNG

Um die Studie aus Verbrauchersicht durchzuführen, wurden Auskunftersuchen bei ausgewählten Anbietern unter so weit wie möglich vergleichbaren Bedingungen untersucht. Die Studie wurde mit insgesamt zwölf Testern durchgeführt. Alle Tester waren mindestens 18 Jahre alt sowie im Besitz eines Smartphones mit Betriebssystem iOS (ab Version 6) oder Android (ab Version 4.3).

Nach einer Erstinformation besuchte jeder Tester die Räumlichkeiten der Geschäftsstelle der Verbraucherzentrale NRW, um die App sowie die Verbindung zwischen Wearable und App unter Aufsicht einzurichten. In elf von zwölf Fällen war die Einrichtung eines eigenen Kontos unter Angabe realer Nutzerdaten erforderlich. Bei der App *Samsung S Health* war dies optional, sodass auf die Einrichtung eines Kontos zunächst verzichtet wurde. Innerhalb der App wurden jedoch Angaben gemacht, die bei einem Antrag auf Auskunft und Löschung eine eindeutige Identifizierung der Person ermöglichen würden (z.B. Name).¹³

Die Tester trugen das Wearable über einen Zeitraum von vier Wochen mit der Vorgabe – falls dies nicht automatisch geschah –, das Wearable einmal täglich mit der installierten Smartphone-App zu synchronisieren. Bei Handhabungsproblemen blieben die Tester im Austausch mit Projekt-Mitarbeitern der Verbraucherzentrale NRW.¹⁴

¹⁰ Für nähere Informationen zur kriteriengeleiteten Anbieterauswahl s. Moll et al., 2017, S. 13.

¹¹ *Withings* wurde in der Zwischenzeit von der Firma *Nokia* gekauft, <https://www.heise.de/newsticker/meldung/Internet-der-Dinge-und-Medizintechnik-Nokia-kauft-Withings-3186179.html>

¹² Deren datenverarbeitende Niederlassung befindet sich jeweils im EU-Ausland. Nach § 1 Abs. 5, S. 2 BDSG findet das BDSG keine Anwendung, wenn die letztendlich entscheidungsbefugte datenverarbeitende Stelle des Unternehmens ihre Niederlassung innerhalb der EU hat. Dementgegen findet die DS-GVO mit der Einführung des Marktortprinzips auch Anwendung „auf datenschutzrechtlich relevante Geschäftsaktivitäten von Unternehmen, die keine Niederlassungen in der EU besitzen [...]“ (Datenschutzkonferenz, 2017, S. 1).

¹³ Alle Tester willigten in die Verwendung ihrer im Zuge des Auskunftersuchens durch den Anbieter verschickten Daten durch die Verbraucherzentrale NRW ein.

¹⁴ Im Fall von *A-Rival* funktionierte die Synchronisation des Wearables mit der App nicht. Da bei der *A-Rival*-App im Rahmen der technischen Prüfung jedoch ohnehin kein ausgehender Datenverkehr beobachtet wurde (s. Moll et al., 2017, S. 20), wurde dieser Funktionsfehler im Zuge des Auskunftersuchens nicht weiter berücksichtigt.

ANTRAG AUF AUSKUNFT

Nach Ablauf der vierwöchigen Testphase wurden die Geräte an die Verbraucherzentrale NRW zurückgegeben. Im Zuge dessen wurde den Testern ein vorformuliertes Schreiben zur Verfügung gestellt, das den Antrag auf Auskunft an den Anbieter formulierte (s. Anhang). Innerhalb des Antrags wurde unter Bezugnahme auf § 34 BDSG Auskunft darüber verlangt, über welche personenbezogenen Daten der Anbieter zur Person des Probanden verfügt, aus welcher Quelle diese Daten stammen, an welche Empfänger diese Daten weitergegeben werden und wurden und zu welchem Zweck die Speicherung erfolgt.

Die Auskunftsverlangen wurden im Dezember 2016 gestellt. Für die Beantwortung wurde eine Frist bis zum 30.01.2017 gewährt. Dieses Datum übersteigt nach hier vertretener Auffassung für alle gestellten Anfragen die Frist, innerhalb derer Anbieter auf ein Auskunftsersuchen antworten sollten.¹⁵ Alle Anfragen wurden in deutscher Sprache geschickt. Nachfolgekorespondenz, soweit erforderlich, wurde ebenfalls auf Deutsch durchgeführt. Es kann nicht unterstellt werden, dass jeder anspruchsberechtigte Verbraucher über die notwendigen Kenntnisse der englischen Sprache verfügt, um seine Anfrage zu stellen. In Bezug auf Allgemeine Geschäftsbedingungen hat die Rechtsprechung festgestellt, dass Alltagsenglisch verbreitet sein mag, Vertragssprachliches Englisch jedoch nicht vorausgesetzt werden kann.¹⁶

Alle Kontaktadressen stammten entweder aus der Datenschutzerklärung, die innerhalb der App zur Verfügung stand, oder, falls hierüber nicht ermittelbar, von den Anbieter-Webseiten. Um eine Auskunft zu erhalten, wurden maximal zwei Kontaktversuche gestartet.

ERSTER KONTAKTVERSUCH

Sofern die Anbieter eine digitale Kontaktmöglichkeit boten, wurde diese im ersten Kontaktversuch genutzt.

Hierbei wurden alle Anfragen per E-Mail von derjenigen E-Mail-Adresse verschickt, die der jeweilige Proband im Zuge der App-Installation beziehungsweise App-Nutzung angegeben hatte. Bei Online-Kontaktformularen wurde diese E-Mail-Adresse als Kontaktadresse angegeben.

ZWEITER KONTAKTVERSUCH

Falls auf den ersten Kontaktversuch innerhalb von zwei Wochen keine Empfangsbestätigung eingegangen war, wurde der Anbieter zusätzlich postalisch kontaktiert, da davon ausgegangen wurde, dass die verschickte E-Mail nicht bearbeitet wird. Die postalischen Adressen wurden entweder der Datenschutzerklärung oder, falls hier nicht angegeben, dem jeweiligen Impressum der Anbieter-Homepage entnommen. Hatte der Anbieter auf den ersten (elektronischen) Kontaktversuch zwar reagiert, jedoch hierbei keine vollständige und/oder angemessene Antwort gegeben, wurde unter Bezugnahme auf den ersten Kontaktversuch erneut elektronisch Auskunft verlangt.

BEWERTUNG DER ANBIETERREAKTIONEN

Zur Bewertung der sehr unterschiedlichen Anbieterreaktionen wurde ein inhaltsanalytischer Ansatz gewählt. Hierbei wurde für jede vorliegende Anbieterreaktion zunächst bewertet, ob die im Auskunftsersuchen gestellten Fragen beantwortet wurden – das heißt konkret:

- Welche personenbezogenen Daten gespeichert wurden (Frage 1),
- aus welcher Quelle die Daten stammen (Frage 2),
- zu welchem Zweck die Speicherung erfolgt (Frage 3),
- an welche dritten Stellen die Daten weitergegeben werden/wurden (Frage 4).

¹⁵ In der Literatur wird teilweise das Erfordernis unverzüglicher Auskunftserteilung angenommen, s. Simitis, 2014, § 34 Rn. 42, teils wird auf den Einzelfall abgestellt (Taeger, 2013, § 34, Rn. 39), eine Beantwortungsfrist zwischen zwei und vier Wochen wird jedenfalls weitestgehend als passende Fristbemessung angesehen (bspw. Gola & Schomerus, 2015, § 34, Rn. 16).

¹⁶ KG Berlin, Urteil vom 08.04.2016, 15 O 44/13.

Die Antworten wurden insgesamt als grundsätzlich vollständig bewertet, wenn alle im Auskunftersuchen genannten Fragen angesprochen wurden (Tabelle 1).¹⁷ In Bezug auf Frage 1 wurde zunächst bewusst eine niedrige Schwelle angelegt: Damit sie als beantwortet gelten konnte, mussten lediglich Kategorien personenbezogener Daten genannt werden.¹⁸ Wünschenswert aus Verbrauchersicht wäre jedoch, dass die Angabe zu den gespeicherten, personenbezogenen Daten so präzise wie möglich ist und das jeweilige Datum konkret nennt, anstatt nur die jeweilige Datenkategorie. Nur so ist es möglich, weitere Betroffenenrechte auf etwaige Löschung oder Berichtigung wirksam auszuüben (s. Abschnitt 1).

Zusätzlich wurde bewertet, ob die Antwort subjektiv als angemessen empfunden wurde. Hierdurch konnten Antworten differenziert bewertet werden, die möglicherweise nicht jede der Fragen beantworteten, davon abgesehen jedoch aus Verbrauchersicht als entgegenkommend erachtet wurden.

Da in der vorliegenden Untersuchung die Frage im Vordergrund stand, inwieweit Verbraucher Antwort auf ein konkretes Auskunftersuchen erhalten, wurden ausschließlich die tatsächlichen Anbieter-Antworten auf das jeweilige Auskunftersuchen inhaltlich bewertet. Beispielsweise wurden keine Hinweise bei der Auswertung berücksichtigt, die ausschließlich den Datenschutzerklärungen zu entnehmen sind. Insofern wurde auch ein bloßer Verweis auf die Inhalte der Datenschutzerklärung nicht als Beantwortung der Fragen gewertet, selbst wenn die Datenschutzerklärung auf die genannten Fragen einging. Es wurde ebenso nicht bewertet, ob der Anbieter einen Webservice zur Verfügung stellt, der ein Abrufen der eigenen Aktivitäten ermöglicht, da dieses Angebot alleine den Anbieter nicht von der Pflicht entbindet, ein Auskunftersuchen zu beantworten. Zusätzlich ist für Verbraucher nicht

notwendigerweise ersichtlich, dass die im Webservice angezeigten Informationen eine vollumfängliche Auflistung der über ihn gespeicherten Daten darstellt.

3. ERGEBNISSE

3.1 ERSTER KONTAKTVERSUCH

ANTWORTRATE

Auf den ersten Kontaktversuch reagierten insgesamt sieben der zwölf angeschriebenen Anbieter mit Antworten, die mehr als eine bloße Empfangsbestätigung der Anfrage darstellten, zum Beispiel indem sie thematisch auf die Anfrage eingingen (Tabelle 1: *Apple, A-Rival, Fitbit, Polar, Runtastic, Samsung* und *Striiv*). Diese Antworten gingen innerhalb weniger Tage nach der ursprünglichen Anfrage bei den Probanden ein. Fünf Anbieter (*Garmin, Jawbone, Technaxx, Withings* und *Xiaomi*¹⁹) reagierten nicht auf den ersten Kontaktversuch.

BEWERTUNG

Zwei der sieben erhaltenen Anbieter-Antworten (*A-Rival, Polar*) wurden als vollständig und angemessen bewertet: Der Anbieter *A-Rival* gibt an, keinerlei Daten über den betreffenden Nutzer zu haben, insofern erübrigten sich auch Informationen über die Datenquelle, den Speicherungszweck und die Weitergabe an Dritte. Diese Negativauskunft deckt sich darüber hinaus mit dem Befund aus der technischen Prüfung, in der für die Anbieter-App kein ausgehender Datenverkehr beobachtet werden konnte.²⁰

Der Anbieter *Polar* nennt in seiner Antwort konkrete Datenkategorien, die Datenquellen sowie den Zweck der Speicherung. Auf Nachfrage²¹ spezifiziert er außerdem, dass Daten ohne explizite Einwilligung nicht

¹⁷ Die Antworten wurden von drei Mitarbeitern der Verbraucherzentrale NRW unabhängig voneinander dichotom kodiert. Die Inter-Rater-Übereinstimmung wurde über Fleiss' Kappa ermittelt und war mit $K = 0.603$ zufriedenstellend (Landis & Koch, 1977, S. 165; s. auch Wirtz & Casper, 2002). Voneinander abweichende Kodierungen wurden hinterher gemeinsam diskutiert, um eine gemeinsame Bewertung der Rater zu erzielen (dargestellt in Tabelle 1).

¹⁸ Ein bloßer Verweis auf diejenigen Daten, zu deren Erhebung das Gerät technisch in der Lage ist, wurde nicht als ausreichende Beantwortung von Frage 1 bewertet.

¹⁹ *Xiaomi* war unter der zum Testzeitpunkt in der Datenschutzerklärung angegebenen E-Mail-Adresse dataprotectionSG@xiaomi.com nicht erreichbar (Fehlermeldung).

²⁰ Moll et al., 2017, S. 18.

²¹ Die Nachfrage wurde innerhalb des ersten Kontaktversuchs gewertet, da in der ursprünglichen Antwort bereits drei der vier gestellten Fragen beantwortet wurden.

an Dritte weitergegeben werden. *Polar* verweist zusätzlich auf die Darstellung von Nutzerdaten im *Polar* Webservice.

Die Antworten der restlichen fünf Anbieter, die auf das Auskunftersuchen reagierten, wurden als unvollständig und nicht angemessen bewertet: Drei Anbieter (*Fitbit*, *Samsung*²², *Striiv*) gehen zwar thematisch auf das Thema Datenschutz ein, beantworten jedoch die im Auskunftersuchen gestellten Fragen nicht – einige der Antworten sind vermutlich vorgefertigte Standardantworten.²³ *Striiv* antwortete darüber hinaus auf die deutschsprachige Anfrage ausschließlich in englischer Sprache.

IDENTIFIKATIONSNACHWEISE

Apple und *Runtastic* forderten weitere Identifikationsnachweise als Bedingung für eine inhaltliche Antwort auf das Auskunftersuchen. Die entsprechende Folgekommunikation wurde jeweils innerhalb des ersten Kontaktversuchs gewertet.

Die von *Apple* geforderten Nutzer-Informationen wurden zur Verfügung gestellt, sofern sie aus Perspektive der Verbraucherzentrale NRW als unter Umständen erforderlich für die Identifikation des Probanden eingeschätzt wurden. Dazu zählten: Vor- und Zuname, E-Mail-Adresse des *Apple*-Accounts, Postadresse, sowie die Seriennummer des registrierten Produkts (zusätzlich gefordert wurden: Telefonnummer, iTunes-Store-Bestellnummer und falls bekannt die *Apple*-ID). Der österreichische Anbieter *Runtastic* forderte die Vorlage einer Personalausweiskopie.²⁴ Diese wurde Ende Januar anteilig geschwärzt²⁵ auf postalischem Weg an den Anbieter verschickt, woraufhin jedoch keine Reaktion mehr seitens des Anbieters erfolgte.

Die angeforderten Informationen wurden weder von *Apple* noch von *Runtastic* bis zum Redaktionsschluss der vorliegenden Studie (21.11.2017) bereitgestellt.

3.2 ZWEITER KONTAKTVERSUCH

ANTWORTRATE

An acht Anbieter wurde ein weiteres Auskunftersuchen geschickt. *Garmin*, *Jawbone*, *Technaxx*, *Withings* und *Xiaomi* hatten nicht auf den elektronischen ersten Kontaktversuch reagiert. Daher wurde an diese Anbieter zusätzlich ein vom jeweiligen Probanden im Original unterschriebenes Auskunftersuchen postalisch verschickt, das im Wortlaut den zuvor verschickten E-Mails entsprach. *Fitbit*, *Samsung* und *Striiv* erhielten unter Bezugnahme auf den ersten Kontaktversuch ein weiteres Auskunftersuchen per E-Mail, da sie auf den ersten Kontaktversuch zwar reagiert hatten, die im Auskunftersuchen gestellten Fragen jedoch nicht zufriedenstellend beantwortet hatten.

Auf den zweiten Kontaktversuch reagierten drei der acht erneut angeschriebenen Anbieter (*Fitbit*, *Striiv* und *Withings*). Die übrigen fünf Anbieter reagierten gar nicht beziehungsweise im Falle von *Garmin* erst über vier Monate nach Ablauf der im Auskunftersuchen genannten Frist.²⁶

BEWERTUNG

Fitbit und *Striiv* stellten auch im zweiten Kontaktversuch keine vollständige oder angemessene Antwort bereit. *Fitbit* gab lediglich einen Hinweis darauf, dass sie Daten bearbeiten, die vom Kunden auf ihrem *Fitbit*-Konto angegeben werden und von den *Fitbit*-Produkten gesammelt werden. Als Zweck gab *Fitbit* an, dass sie mit den Daten die Qualität der Produkte kontrollieren möchten. *Striiv* gab im Wortlaut dieselbe Antwort wie nach dem ersten Kontaktversuch, die schon dort als unvollständig gewertet worden war.

Withings forderte im Verlauf des zweiten Kontaktversuchs die postalische Zusendung der E-Mail-Adresse des Testers, unter der das *Withings*-Konto geführt

²² Bei *Samsung* wurde zunächst auf die Einrichtung und Verknüpfung eines *Samsung*-Kontos verzichtet (s. Abschnitt 2). Die unvollständige Rückmeldung des *Samsung* Customer Supports ließ darauf schließen, dass ein *Samsung*-Konto erforderlich ist, um unter der kontaktierten Adresse die gewünschte Auskunft zu erhalten. Um zu untersuchen, ob das Auskunftersuchen wegen fehlender Kontoregistrierung gescheitert war, wurde ein Konto angelegt und ein erneutes Auskunftersuchen über das Kontaktformular geschickt. Die Antwort auf dieses zweite Auskunftersuchen führte zur gleichen Bewertung wie die im Ergebnisbericht und Tabelle 1 thematisierte Antwort.

²³ Auszug aus der Antwort von *Fitbit* auf das Auskunftersuchen: „Fitbit nimmt die Datensicherheit und die Privatsphäre der Nutzer sehr ernst. Wir verwenden Industriestandard-Methoden, um Benutzerdaten zu schützen. Wir verkaufen niemals Informationen, die von Fitbit Produkten gesammelt werden. Fitbit Nutzer haben die volle Kontrolle über Ihre Daten und Informationen und wann und ob diese mit anderen geteilt werden. Beispielsweise können Nutzer selbst entscheiden, ob sie Informationen in einem Sozialen Netzwerk teilen möchten oder nicht. Alle Voreinstellungen im Fitbit Konto sind auf „privat“ eingestellt, wenn ein Nutzer ein Fitbit-Konto erstellt. Wenn ein Nutzer Daten jeglicher Art mit dritten teilen möchte, muss dies zuerst in den Einstellungen geändert und anschließend zugestimmt werden.“

²⁴ Es sei darauf hingewiesen, dass nach dem hier maßgeblichen österreichischem Recht (§ 26 Abs. 1 DSGVO 2000) die Schriftform gilt und die verantwortliche Stelle explizit berechtigt ist einen Identitätsnachweis durch Personalausweis zu fordern (Bundesministerium des Inneren Rep. Österreich, Auskunftsrecht gemäß § 26 Datenschutzgesetz DSGVO 2000, S. 3, http://www.bmi.gv.at/402/files/Beilage_zum_Auskunftsrecht_2015.pdf)

²⁵ Geschwärzt wurden folgende Informationen: Seriennummer, Zugangsnummer, Augenfarbe, Größe, Ausstellungsdatum, ausstellende Behörde; folgende Informationen blieben ungeschwärzt: Name, Anschrift, Geburtsdatum und Gültigkeit des Dokuments; s. LDI NRW, 2014, S. 3 ff.

²⁶ Die Antwort von *Garmin* erfolgte, nachdem die Verbraucherzentrale den Anbieter wegen der zuvor ausbleibenden Antwort abgemahnt hatte. Insgesamt hat die Verbraucherzentrale NRW auf Basis der Untersuchungsergebnisse sechs Anbieter abgemahnt, s. <https://ssl.marktwaechter.de/digitale-welt/marktbeobachtung/wearables-fitness-apps-und-das-recht-auf-auskunft-ein-praxistest>

wird. Daraufhin erhielt der Tester eine Antwort auf sein Auskunftersuchen per E-Mail, das zwar nicht vollständig war (der Zweck der Speicherung wurde nicht genannt), übergreifend jedoch als angemessen beurteilt wurde.

TABELLE 1

ANBIETER-ANTWORTEN AUF AUSKUNFTSERSUCHEN

Anbieter	Erster Kontaktversuch				Zweiter Kontaktversuch			
	Kontaktkanal	reagiert	Antwort grundsätzlich vollständig	Antwort angemessen	Kontaktkanal	reagiert	Antwort grundsätzlich vollständig	Antwort angemessen
Apple ^a	online ^d	ja	- ^f	- ^f	-	-	-	-
A-Rival ^b	online ^e	ja	ja	ja	-	-	-	-
Fitbit ^b	online ^e	ja	nein	nein	online	ja	nein	nein
Garmin ^a	online ^e	nein	-	-	postalisch	nein ^g	-	-
Jawbone ^a	online ^e	nein	-	-	postalisch	nein	-	-
Polar ^{b,c}	online ^e	ja	ja	ja	-	-	-	-
Runtastic ^{b,c}	online ^e	ja	- ^f	- ^f	-	-	-	-
Samsung ^b	online ^d	ja	nein	nein	online	nein	-	-
Striiv ^b	online ^e	ja	nein	nein	online	ja	nein	nein
Technaxx ^b	online ^e	nein	-	-	postalisch	nein	-	-
Withings ^b	online ^e	nein	-	-	postalisch	ja	nein	ja
Xiaomi ^{b,c}	online ^e	nein	-	-	postalisch	nein	-	-
GESAMT	12	7	2	2	8	3	0	1

^a Für das Betriebssystem iOS.

^b Für das Betriebssystem Android.

^c Das BDSG ist nicht anwendbar. Sich hieraus ergebende Verstöße sind für diese Anbieter unter Umständen nicht verfolgbar.

^d Online-Kontaktformular auf der Webseite des Anbieters.

^e Per E-Mail.

^f Der Anbieter forderte Identifikationsnachweise, die daraufhin zur Verfügung gestellt wurden. Das Auskunftersuchen wurde bis zum Datum der Veröffentlichung inhaltlich nicht beantwortet.

^g *Garmin* hat das Auskunftsverlangen mittlerweile beantwortet. Da die Frist hierfür jedoch bei Eingang der Antwort über vier Monate abgelaufen war, wird diese nicht im Rahmen der vorliegenden Studie bewertet.

4. ABSCHLUSSBETRACHTUNG

ZUSAMMENFASSUNG

In der vorliegenden explorativen Studie wurde untersucht, inwieweit Nutzer von Wearables und Fitness-Apps Antwort auf ein Auskunftersuchen nach § 34 BDSG erhalten (Forschungsfrage 1) und welchen Hindernissen sie dabei begegnen (Forschungsfrage 2).

Nach zwei Kontaktversuchen hatten acht von zwölf Anbietern auf das Auskunftsverlangen in irgendeiner Form reagiert. Lediglich drei der zwölf angeschriebenen Anbieter beantworteten jedoch das Auskunftersuchen auf angemessene Art und Weise.

Einer dieser Anbieter (*A-Rival*) speichert keine Nutzerdaten und erteilt eine Negativauskunft. Die beiden anderen Anbieter (*Polar* und *Withings*) beantworteten die Frage nach den gespeicherten Daten mit der Nennung abstrakter Datenkategorien, ohne aber das Datum zu präzisieren, das sie in der jeweiligen Kategorie über den Nutzer gespeichert haben. Zusätzlich verweisen beide auf die Darstellung gespeicherter Nutzerdaten in ihrem Webservice.

Festzuhalten bleibt, dass im Rahmen der vorliegenden Studie ein Großteil der Anbieter nicht beziehungsweise nicht vollständig auf die im Auskunftersuchen gestellten Fragen antwortete. Dieser Befund deckt sich mit den Ergebnissen aus vergangenen Untersuchungen²⁷ und ist somit ein Indiz dafür, dass die Schwierigkeit für Verbraucher, ihrem Auskunftsanspruch nach entsprechend informiert zu werden, eine übergreifende Problematik auf dem Markt der digitalen Produkte und Dienstleistungen zu sein scheint.

IDENTIFIKATIONSNACHWEISE

Ein Hindernis, das sich Verbrauchern im Zuge ihres Auskunftsverlangens in den Weg stellt, sind durch den Anbieter geforderte Identifikationsnachweise. In der vorliegenden Studie forderten drei Anbieter (*Apple*, *Runtastic*, *Withings*) weitere Informationen zum Identifikationsnachweis.

Bei elektronischem Schriftverkehr reicht es zur erfolgreichen Identifikation in der Regel aus, wenn die Anfrage von dem E-Mail-Account gesendet wurde, das bei dem Unternehmen als Kontakt hinterlegt ist.²⁸ Dies wurde bei allen Testern sichergestellt, die sich im Rahmen der Studie über einen Account angemeldet hatten. Der Anbieter *Withings*, an den im zweiten

Kontaktversuch ein postalisches Auskunftersuchen geschickt worden war, forderte eben diese E-Mail-Adresse – vermutlich als Identifikationsnachweis. Das Auskunftersuchen wurde schließlich per E-Mail beantwortet.

In Zweifelsfällen dürfen weitere Identifikationsnachweise vom Anbieter gefordert werden, wobei jedoch keine überzogenen Anforderungen gestellt werden dürfen. Allerdings forderte *Apple* – nach hier vertretener Auffassung – Informationen, die über das erforderliche Maß hinaus gingen (z.B. die Produkt-Bestellnummer). Diese Informationen wurden dem Anbieter nicht mitgeteilt. *Apple* antwortete daraufhin, dass die zur Verfügung gestellten Informationen entweder nicht ausreichend seien oder nicht mit den im Account hinterlegten Informationen übereinstimmen – man könne aus Datenschutzgründen nicht offenbaren, welche weiteren Informationen benötigt würden. Im vorliegenden Fall blieb daher bis zuletzt unklar, warum *Apple* nicht dazu in der Lage war, den Tester korrekt zu identifizieren.

In Ausnahmen ist es zulässig, einen Identifikationsnachweis anhand von amtlichen Legitimationspapieren zu fordern wie den Personalausweis²⁹, beispielsweise um einen Abgleich mit den hinterlegten Adressdaten vorzunehmen – stimmen die angegebenen Adressdaten des Betroffenen mit den gespeicherten Angaben überein, kann von der Berechtigung des Auskunftersuchens ausgegangen werden.³⁰

Bei einer solchen Forderung müssen jedoch strenge Voraussetzungen erfüllt sein, wie beispielsweise eine Schwärzung nicht erforderlicher Informationen, auf deren Notwendigkeit der Anbieter hinweisen muss.³¹

Ein Identifikationsnachweis anhand einer Personalausweiskopie wurde von *Runtastic* auf Grundlage des österreichischen Rechts gefordert. Allerdings beantwortete der Anbieter das Auskunftersuchen bis zur Veröffentlichung dieser Untersuchung nicht, obwohl ihnen eine anteilig geschwärzte Personalausweiskopie des Testers geschickt wurde.

In der vorliegenden Studie führte das Nachfordern von Informationen aus Verbraucherperspektive zu – nach hier vertretener Auffassung – nicht hinnehmbaren Verzögerungen der geforderten inhaltlichen Antwort beziehungsweise nicht hinnehmbaren Erschwernissen.

²⁷ z.B. Herrmann & Lindemann (2016).

²⁸ Gola & Schomerus, 2015, § 34, Rn. 6-7.

²⁹ Schmidt-Wudy, 2017, § 34 Rn. 26-29.

³⁰ vgl. Gola, 2012, zur diesbezüglichen Auffassung der Aufsichtsbehörden.

³¹ Für die vollständigen Voraussetzungen s. LDI NRW (2014, S. 3 ff.), s. auch https://www.personalausweisportal.de/DE/Buergerinnen-und-Buerger/Der-Personalausweis/Ausweis_kopieren/ausweis_kopieren_node.html

FAZIT

Die Ergebnisse der Vorgängeruntersuchung von insgesamt zwölf Wearables und 24 Fitness-Apps³² hatten gezeigt, dass Wearable-Anbieter in ihren Datenschutzerklärungen oft nicht ausreichend über den Umgang mit ihren Daten informieren. Die vorliegende Studie ergänzt dies um die Feststellung, dass Verbraucher auch auf wiederholte und formelle Nachfrage beim Anbieter in den meisten Fällen keine detaillierte Auskunft zu den über sie gespeicherten personenbezogenen Daten erhalten, die Anbieter im Zuge der Nutzung über Verbraucher erheben und verarbeiten. Eine tatsächliche Kontrolle der Verbraucher über ihre eigenen Daten, beispielsweise eine Berichtigung, Sperrung oder gar Löschung der eigenen personenbezogenen Daten, wird hierdurch erschwert.

³² Moll et al., 2017.

5. QUELLENVERZEICHNIS

LITERATUR

Gola, P. (2012). Aus den Tätigkeitsberichten der Aufsichtsbehörden. Recht der Datenverarbeitung, 28. Jahrgang (Heft 4), S. 184-186.

Herrmann, D. & Lindemann, J. (2016). Obtaining personal data and asking for erasure: Do app vendors and website owners honour your privacy rights? CoRR, abs/1602.0. Abgerufen von <http://arxiv.org/abs/1602.01804> [Stand: 11.01.2017].

Hilts, A., Parsons, C., & Knockel, J. (2016). Every step you fake: A comparative analysis of Fitness Tracker privacy and security. Open Effect Report (2016). Abgerufen von https://openeffect.ca/reports/Every_Step_You_Fake.pdf [Stand: 11.01.2017].

Datenschutzkonferenz (2017). DSK-Kurzpapier Nr. 7 – Marktortprinzip. Abgerufen von https://www.lda.bayern.de/media/dsk_kpnr_7_marktortprinzip.pdf [Stand: 09.10.2017].

Landis, R. & Koch, G. G. (1977). The measurement of observer agreement for categorical data. Biometrics, 33(1), S. 159-174.

LDI NRW (2014). Personalausweis und Datenschutz. Stellungnahme des Landesdatenschutzbeauftragten für Datenschutz und Informationsfreiheit NRW. Abgerufen von https://www.ldi.nrw.de/mainmenu_Service/submenu_Newsarchiv/Inhalt_/Personalausweis_und_Datenschutz/Personalausweis_und_Datenschutz1.pdf [Stand: 25.09.2017].

Moll, R., Schulze, A., Rusch-Rodosthenous, M., Kunke, C., & Scheibel, L. (2017). Wearables, Fitness-Apps und der Datenschutz: Alles unter Kontrolle?. Verbraucherzentrale NRW e.V. (Hrsg.). Abgerufen von <http://www.marktwaechter.de/digitale-welt/marktbeobachtung/wearables-und-fitness-apps>

Wirtz, M. & Caspar, F. (2002). Beurteilerübereinstimmung und Beurteilerreliabilität. Göttingen: Hogrefe.

KOMMENTARE UND HANDBÜCHER

Gola, P. & Schomerus, R. (2015). BDSG Kommentar. In: P. Gola & R. Schomerus (Hrsg.), Bundesdatenschutzgesetz Kommentar (12. Auflage). München: C. H. Beck.

Schmidt-Wudy, F. (2017). BDSG Kommentar. In: H. A. Wolff & S. Brink (Hrsg.), BeckOK Datenschutzrecht (20. Auflage). München: C. H. Beck.

Simitis, S. (2014). BDSG Kommentar. In: S. Simitis (Hrsg.), Bundesdatenschutzgesetz (8. Auflage). Baden-Baden: Nomos.

Taeger, J. (2013). BDSG Kommentar. In: J. Taeger & D. Gabel (Hrsg.), Bundesdatenschutzgesetz (2. Auflage). Frankfurt am Main: Deutscher Fachverlag.

6. ANHANG: ANTRAG AUF AUSKUNFT

Maria Mustermann
Musterstraße 21
00000 Musterstadt

Musterstadt, Datum

Anschrift
des
Anbieters

Sehr geehrte Damen und Herren,

ich mache hiermit Ihnen gegenüber meinen Auskunftsanspruch nach § 34 Bundesdatenschutzgesetz geltend. Folglich fordere ich Sie auf, mir folgende Auskünfte zu erteilen:

Über welche gespeicherten personenbezogenen Daten zu mir verfügen Sie und aus welcher Quelle haben Sie diese Daten bezogen?

An welche Empfänger oder sonstige Stellen werden und wurden diese Daten weitergegeben?
Zu welchem Zweck erfolgt diese Speicherung?

Ich setze Ihnen zur Erfüllung meines Anspruchs eine Frist bis zum 30.01.2017.

Mit freundlichen Grüßen

Impressum

Herausgeber

Verbraucherzentrale NRW e.V.
Mintropstr. 27
40215 Düsseldorf
Tel. (0211) 3809 0
Fax. (0211) 3809 172
marktwaechter@verbraucherzentrale.nrw

Text: Dr. Ricarda Moll, Miriam Rusch-Rodosthenous,
Lisa Scheibel, Christopher Kunke

Titelbild: Production Perig / Fotolia

Gestaltung: Katharina Ploog

Stand: November 2017

© Verbraucherzentrale NRW e.V.

Gefördert durch:



Bundesministerium
der Justiz und
für Verbraucherschutz

aufgrund eines Beschlusses
des Deutschen Bundestages

verbraucherzentrale