Masterarbeit

im Studiengang
Masterinformatik

Dark Patterns und Datenschutzerklärungskonformität in (Gesundheits- & Fitness) Apps - Eine Analytische Studie

von

Alexander Herbst

Matrikelnummer:	4136975
Erstprüfer:	Dr. Karsten Sohr
Zweitprüfer:	Prof. Dr. Rainer Malaka
Eingereicht am:	26.01.2024

Universität Bremen

Nachname **Herbst** Matrikelnr. **4136975**

Vorname **Alexander**

Hinweise zu den offiziellen Erklärungen

1. Die folgende Seite mit den offiziellen Erklärungen

   A) Eigenständigkeitserklärung

   B) Erklärung zur Veröffentlichung von Bachelor- oder Masterarbeiten

   C) Einverständniserklärung über die Bereitstellung und Nutzung der Bachelorarbeit / Masterarbeit in elektronischer Form zur Überprüfung durch eine Plagiatssoftware

   ist entweder direkt in jedes Exemplar der Bachelor- oder Masterarbeit fest mit einzubinden oder unverändert im Wortlaut in jedes Exemplar der Bachelor- oder Masterarbeit zu übernehmen.

   Bitte achten Sie darauf, jede Erklärung in allen drei Exemplaren der Arbeit zu unterschreiben.

2. In der digitalen Fassung kann auf die Unterschrift verzichtet werden. Die Angaben und Entscheidungen müssen jedoch enthalten sein.

Zu B)

Die Einwilligung kann jederzeit durch Erklärung gegenüber der Universität Bremen, mit Wirkung für die Zukunft, widerrufen werden.

Zu C)

Das Einverständnis der dauerhaften Speicherung des Textes ist freiwillig.

Die Einwilligung kann jederzeit durch Erklärung gegenüber der Universität Bremen, mit Wirkung für die Zukunft, widerrufen werden.

Weitere Informationen zur Überprüfung von schriftlichen Arbeiten durch die Plagiatsoftware sind im Nutzungs- und Datenschutzkonzept enthalten. Diese finden Sie auf der Internetseite der Universität Bremen.

Universität Bremen

Nachname **Herbst** Matrikelnr. **4136975**

Vorname **Alexander**

A) Eigenständigkeitserklärung

Ich versichere, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel verwendet habe.
Alle Teile meiner Arbeit, die wortwörtlich oder dem Sinn nach anderen Werken entnommen sind, wurden unter Angabe der Quelle kenntlich gemacht. Gleiches gilt auch für Zeichnungen, Skizzen, bildliche Darstellungen sowie für Quellen aus dem Internet.
Die Arbeit wurde in gleicher oder ähnlicher Form noch nicht als Prüfungsleistung eingereicht. Die elektronische Fassung der Arbeit stimmt mit der gedruckten Version überein.
Mir ist bewusst, dass wahrheitswidrige Angaben als Täuschung behandelt werden.

B) Erklärung zur Veröffentlichung von Bachelor- oder Masterarbeiten

Die Abschlussarbeit wird zwei Jahre nach Studienabschluss dem Archiv der Universität Bremen zur dauerhaften Archivierung angeboten. Archiviert werden:

1) Masterarbeiten mit lokalem oder regionalem Bezug sowie pro Studienfach und Studienjahr 10 % aller Abschlussarbeiten
2) Bachelorarbeiten des jeweils ersten und letzten Bachelorabschlusses pro Studienfach und Jahr.

☒ Ich bin damit einverstanden, dass meine Abschlussarbeit im Universitätsarchiv für wissenschaftliche Zwecke von Dritten eingesehen werden darf.

☒ Ich bin damit einverstanden, dass meine Abschlussarbeit nach 30 Jahren (gem. §7 Abs. 2 BremArchivG) im Universitätsarchiv für wissenschaftliche Zwecke von Dritten eingesehen werden darf.

☐ Ich bin nicht damit einverstanden, dass meine Abschlussarbeit im Universitätsarchiv für wissenschaftliche Zwecke von Dritten eingesehen werden darf.

C) Einverständniserklärung zur Überprüfung der elektronischen Fassung der Bachelorarbeit / Masterarbeit durch Plagiatssoftware

Eingereichte Arbeiten können nach § 18 des Allgemeinen Teil der Bachelor- bzw. der Master-prüfungsordnungen der Universität Bremen mit qualifizierter Software auf Plagiatsvorwürfe untersucht werden.
Zum Zweck der Überprüfung auf Plagiate erfolgt das Hochladen auf den Server der von der Universität Bremen aktuell genutzten Plagiatssoftware.

☐ Ich bin damit einverstanden, dass die von mir vorgelegte und verfasste Arbeit zum oben genannten Zweck dauerhaft auf dem externen Server der aktuell von der Universität Bremen genutzten Plagiatssoftware, in einer institutionseigenen Bibliothek (Zugriff nur durch die Universität Bremen), gespeichert wird.

☒ Ich bin nicht damit einverstanden, dass die von mir vorgelegte und verfasste Arbeit zum o.g. Zweck dauerhaft auf dem externen Server der aktuell von der Universität Bremen genutzten Plagiatssoftware, in einer institutionseigenen Bibliothek (Zugriff nur durch die Universität Bremen), gespeichert wird.

Mit meiner Unterschrift versichere ich, dass ich die obenstehenden Erklärungen gelesen und verstanden habe und bestätige die Richtigkeit der gemachten Angaben.

Datum Unterschrift

Abstract

In dieser interdisziplinären Masterarbeit wird der Umgang von personenbezogenen Daten in Fitness- und Gesundheits-Apps untersucht. Hierbei werden die Forschungsfelder Informationssicherheit, Human-Computer-Interaction und Recht miteinander verknüpft. Das Ziel dieser Forschungsarbeit besteht darin, zu untersuchen, inwiefern die Angaben von Datenschutzerklärungen mit der tatsächlichen Nutzung von 20 Fitness- und Gesundheits-Apps konform sind. Zudem erfolgt eine Analyse der Verbreitung von Dark Patterns in den Einwilligungserklärungen, um zu prüfen, inwiefern die Datenschutzerklärungen die Nutzer über die Verwendung ihrer personenbezogenen Daten informieren. Die Ergebnisse dieser Arbeit tragen dazu bei, das Verständnis für den Datenschutz in Fitness- und Gesundheits-Apps zu vertiefen und bieten eine Grundlage für zukünftige Entwicklungen im Bereich der Privatsphäre von App-Nutzern.

Die Methodik dieser Masterarbeit setzt sich aus zwei wesentlichen Teilen zusammen. Zunächst erfolgt eine umfassende Analyse der Datenschutzerklärungen der Apps. Diese Ergebnisse werden anschließend mit den Resultaten einer statischen und dynamischen Analyse von diesen Apps verglichen. Dadurch kann die Konformität der Datenschutzerklärung mit dem tatsächlichen Gebrauch der Apps überprüft werden. Weiterhin liegt ein Schwerpunkt in der Untersuchung von Einwilligungserklärungen auf Dark Patterns. Dabei handelt es sich um Design-Elemente die einen Nutzer zu bestimmten Aktionen bewegen können oder Informationen verschleiern. Dadurch kann insgesamt die Transparenz und der Informationsgehalt von Apps zum Schutz der Privatsphäre von Nutzern bewertet werden.

Die Ergebnisse sollen so einen Einblick der aktuellen Praxis in Apps zeigen und eine Grundlage für zukünftige Forschungen im Bereich App-Nutzung und Datenschutz liefern.

Inhaltsverzeichnis

1. Einleitung

In der zunehmend digitalisierten Welt gewinnen Fitness- und Gesundheits-Apps eine immer größere Bedeutung, da sie individuelle Gesundheitsziele unterstützen und den Zugang zu personalisierten Trainings- und Gesundheitsinformationen erleichtern. Mit dieser wachsenden Relevanz entstehen jedoch auch vermehrt Fragen bezüglich des Schutzes personenbezogener Daten und der Transparenz in Bezug auf Datenschutzpraktiken. Diese Masterarbeit widmet sich einer umfassenden Untersuchung von Datenschutz bezogenen Aspekten in Fitness- und Gesundheits-Apps, indem sowohl eine technische Analyse zur Identifizierung von Datenempfängern und Drittlandübermittlungen als auch eine Analyse der Datenschutzerklärungen durchgeführt wird. Zusätzlich wird eine Analyse von *Dark Patterns* in Einwilligungserklärungen durchgeführt, um die Transparenz und den Informationsgehalt dieser Erklärungen zu bewerten.

Mehr als 70% der Internetnutzer setzen sich nicht intensiv mit den Datenschutzerklärungen von Webseiten auseinander [9]. Die geringe Aufmerksamkeit gegenüber Datenschutzinformationen birgt das Risiko, dass personenbezogene Daten von Nutzern unbemerkt an Dritte weitergegeben oder verkauft werden könnten. Jedoch bräuchten selbst diejenigen Nutzer, die die Motivation haben, sich mit den Erklärungen auseinanderzusetzen, ungefähr 76 Arbeitstage im Jahr, um diese zu lesen [47].
Diese Studien weisen darauf hin, dass es im Umgang mit Apps und Internetseiten ein zweiseitiges Problem gibt. Auf der einen Seite klären viele Unternehmen ihre Nutzer nicht genügend über ihre Handlungen auf oder bieten nur intransparente Disclaimer an [14]. Andererseits neigen Datenschutzerklärungen dazu, äußerst umfangreich und schwer verständlich zu sein, und Nutzer zeigen oft wenig Interesse daran, sich eingehend mit Datenschutzerklärungen auseinanderzusetzen [9, 47].
Diese Studie repräsentiert eine interdisziplinäre Forschung, die Themen aus den Bereichen Informationssicherheit, Human-Computer Interaction und Recht verbindet. Im Bereich der Informationssicherheit wurde bereits Forschungsarbeit geleistet, insbesondere im Hinblick auf die Übertragung personenbezogener Daten an Drittempfänger [15, 35, 37]. Allerdings besteht eine Forschungslücke, besonders im Kontext der Übermittlung an Drittländer. Während Übertragungen an bestimmte Dritte wie beispielsweise *Google* oder *Facebook* beobachtet wurden, bleibt die Übermittlung an bestimmte Länder, die außerhalb des Heimatlandes liegen, und deren rechtliche Konsequenzen bislang wenig erforscht. Weiterhin fehlt ein Abgleich mit den entsprechenden Datenschutzerklärungen. Dies ist re-

levant, da erforscht werden muss, ob die übertragenen Daten und der Ort der Übertragung mit der angegebenen Datenschutzerklärung übereinstimmt. Daraus ergibt sich die erste Forschungsfrage: *Inwiefern entsprechen die in den Datenschutzerklärungen aufgeführten Empfängern von Daten, Drittlandempfänger und die Verwendung personenbezogener Daten den tatsächlichen Ergebnissen einer technischen Analyse?*
Durch die Forschungsfrage wird zum einen die fehlende Untersuchung an Übermittlungen an Drittländern und den damit rechtlichen Konsequenzen untersucht. Zum anderen wird untersucht, ob die in den Datenschutzerklärungen angegebenen Datenempfänger, Drittlandempfänger und die Verwendung personenbezogener Daten mit den tatsächlichen Ergebnissen der technischen Analyse übereinstimmen. Dies ist von größter Relevanz, um Differenzen zu ermitteln, Datenschutzverletzungen zu identifizieren und damit die Integrität der Datenschutzerklärungen von Apps aus dem Bereich Fitness und Gesundheit zu gewährleisten.
Obwohl bereits umfangreiche Forschungsarbeiten zu den einzelnen Themen durchgeführt wurden, besteht eine Forschungslücke in der Verbindung dieser Erkenntnisse. Datenübertragungen von personenbezogenen Daten wurden bereits eingehend untersucht, jedoch fehlt bisher der Bezug zu rechtlichen Fragestellungen und den daraus resultierenden Konsequenzen. Dieser Vergleich schafft eine bisher wenig erforschte Perspektive, die sowohl für Informatiker als auch für Rechtswissenschaftler neue Erkenntnisse erzeugen kann.

Im Bereich der Human-Computer Interaction und insbesondere im Zusammenhang mit Dark Patterns wurden bereits umfangreiche Studien zur Anzahl und den Auswirkungen von Dark Patterns in Apps durchgeführt, wie in Geronimo et al. [29] und Van Kleek et al. [73] gezeigt. Dark Patterns beschreiben die Art und Weise wie angezeigte Design-Elemente die Nutzung der App für den Nutzer beeinflussen können. In Abbildung 1 wird ein beispielhaftes Cookie-Einstellungen-Fenster angezeigt. Ersichtlich ist, dass der Nutzer dazu verleitet wird eher den erleuchteten *Alle akzeptieren*-Button zu verwenden, anstatt sich zunächst mit den anderen Optionen auseinanderzusetzen.

In dieser Arbeit liegt der Fokus speziell auf der Untersuchung der Einwilligungserklärungen zur Datenschutzerklärung, wobei besonderes Augenmerk auf Transparenz und Informationsgehalt für den Nutzer gelegt wird. Daraus ergibt sich die folgende Forschungsfrage: *Wie weit verbreitet sind Dark Patterns in den Einwilligungserklärungen von Fitness- und Gesundheits-Apps?*
Die Fokussierung auf Einwilligungserklärungen zur Datenschutzerklärung in

Abbildung 1: Beispielhafte Anzeige von Cookie-Einstellungen [57]

Fitness- und Gesundheits-Apps trägt zu neuen Forschungen bei. Während bisherige Studien Dark Patterns in Apps im Allgemeinen untersucht haben, liegt hier der Schwerpunkt auf der Interaktion zwischen App-Anbietern und Nutzern mit der Zustimmung zur Datenverarbeitung. Durch die Analyse dieser Einwilligungserklärungen wird versucht neue Kenntnisse zu gewinnen, inwiefern Transparenz und Informationsgehalt für den Nutzer in Apps gegeben sind. Diese Erkenntnisse sind von Bedeutung, um Einblicke in die Gestaltung solcher Einwilligungserklärungen, das Auftreten von Datenschutzverletzungen sowie Möglichkeiten zur Verbesserung zu gewinnen.

Schließlich wird auch der rechtliche Aspekt von Datenschutzerklärungen betrachtet. Oftmals werden in Datenschutzerklärungen Empfänger von Daten oder Drittländer nicht namentlich genannt, sondern lediglich in Kategorien aufgezählt wie etwa *Werbepartner* oder *Empfänger in der Europäischen Union*. Diese ungenauen Angaben werfen die Frage auf, ob Nutzer mithilfe der Datenschutzerklärung genügend über den Gebrauch und der Vermittlung ihrer personenbezogenen Daten aufgeklärt werden. Hieraus ergibt sich die letzte Forschungsfrage dieser Arbeit: *In welchem Maße informieren Datenschutzerklärungen von Fitness-*

und Gesundheits-Apps über Datenempfänger, Drittlandübermittlungen und die Verwendung personenbezogener Daten?
Die letzte Forschungsfrage dieser Arbeit soll aufklären, ob die Informationstransparenz in den Datenschutzerklärungen von Fitness- und Gesundheits-Apps ausreicht und inwiefern den Nutzern eine klare Vorstellung darüber vermittelt wird, wie ihre Daten genutzt und weitergegeben werden. Zusammengefasst werden in dieser Arbeit folgende 3 Forschungsfragen beantwortet:

- Inwiefern entsprechen die in den Datenschutzerklärungen aufgeführten Empfängern von Daten, Drittlandempfänger und die Verwendung personenbezogener Daten den tatsächlichen Ergebnissen der technischen Analyse?
- Wie weit verbreitet sind Dark Patterns in den Einwilligungserklärungen von Fitness- und Gesundheits-Apps?
- In welchem Maße informieren Datenschutzerklärungen von Fitness- und Gesundheits-Apps über Datenempfänger, Drittlandübermittlungen und die Verwendung personenbezogener Daten?

Die formulierten Forschungsfragen wurden so gewählt, das eine umfassende Relevanz für die verschiedenen Forschungsbereiche besteht. Auf diese Weise entsteht eine Schnittstelle zwischen den unterschiedlichen Fachgebieten.

Nach der Benennung der Fragestellungen wird im nächsten Teil der Einleitung die Gliederung der Arbeit beschrieben.
Nach der Einleitung wird zunächst ein Überblick über die aktuelle Forschung der relevanten Bereiche gegeben. Dabei werden für die Bereiche Informationssicherheit, Human-Computer Interaction und Recht notwendige Grundlagen aufgebaut und mit aktuellen Forschungsergebnissen untermauert. Dadurch kann der aktuelle Stand der Wissenschaft in den Fachgebieten übermittelt und Schnittstellen zwischen diesen geschaffen werden.
Im nachfolgenden Abschnitt wird die Methodik dieser Arbeit näher erläutert. Hierbei erfolgt zunächst eine Darstellung des Versuchsaufbaus sowie der verwendeten Tools. Anschließend wird der genaue Ablauf und die Vorgehensweise bei der Analyse der Apps und der Datenschutzerklärungen detailliert beschrieben.
Im Kapitel Studienergebnisse werden die Ergebnisse aus der Studie dargelegt und interpretiert. Die resultierenden Ergebnisse dienen als Grundlage für die Beantwortung der im Vorfeld formulierten Forschungsfragen.
In dem Kapitel Diskussion werden die Forschungsfragen wieder aufgegriffen

und ausführlich beantwortet wobei Bezüge zu relevanten Forschungen gezogen werden. Weiterhin werden die Limitationen und Herausforderungen erläutert, um ein Bild zu schaffen, was in zukünftigen Arbeiten verbessert werden könnte.
Im Kapitel Ausblick wird ein Überblick gegeben, wie die Forschung erweitert werden könnte und wie die Ergebnisse der Arbeit weiter verwendet werden könnten.
Schließlich findet sich im Kapitel Appendix eine Sammlung der resultierenden Ergebnisse der Analyse.

2. Aktueller Forschungsstand

Die interdisziplinäre Ausrichtung dieser Arbeit zeigt sich in der umfangreichen Literatur, die aus verschiedenen Bereichen herangezogen wird, um Herausforderungen, Lücken und Lösungsansätze umfassend zu erforschen. Diese Herangehensweise ermöglicht einen breiten Blickwinkel auf das Forschungsthema und erlaubt es verschiedene Perspektiven zu berücksichtigen.

2.1. Technische Analyse

Bei der technischen Analyse werden zwei Methoden angewandt. Zum einen erfolgt eine dynamische Analyse, bei der die Apps während der Laufzeit untersucht werden. Zum Anderen erfolgt eine statische Analyse, bei der die Apps ohne Ausführung untersucht werden.

2.1.1. Dynamische Analyse

In dynamischen Analysen wird die App während der Ausführung überwacht. Dynamische Analysen sind akkurat, da keine Annäherungen oder Abstraktionen notwendig sind. Auf diese Weise können diese beobachteten Ausführungspfade detailliert dokumentiert werden, einschließlich der erzielten Ergebnisse und der Dauer der Ausführung. Ein Nachteil besteht darin, dass nur der jeweils beobachtete Ausführungspfad erfasst werden kann. Obwohl die dynamische Analyse erneut durchgeführt werden kann, besteht keine Garantie dafür, dass der vorherige Ausführungspfad wieder durchlaufen wird, und es ist auch nicht sicher, dass **alle** möglichen Ausführungspfade erfasst werden können. Somit ist die dynamische Analyse präzise für einen bestimmten Ausführungspfad, kann aber keine umfassende Aussage über die Gesamtausführung der App geben [26].

Eine Form der dynamischen Analyse ist die Netzwerk-Analyse. Dabei wird der Datenverkehr während der Ausführung der App betrachtet und ausgehende und eingehende Datenverkehr aufgenommen (und entschlüsselt), gefiltert und analysiert. Vor allem personenbezogene Daten, Server-Standorte und Empfänger sind für diese Arbeit entscheidend.

Für die Netzwerk-Analyse wird eine sogenannte *Man-in-the-Middle Attack* durchgeführt. Dem Netzwerkverkehr liegt das HTTPS-Protokoll zugrunde, welches

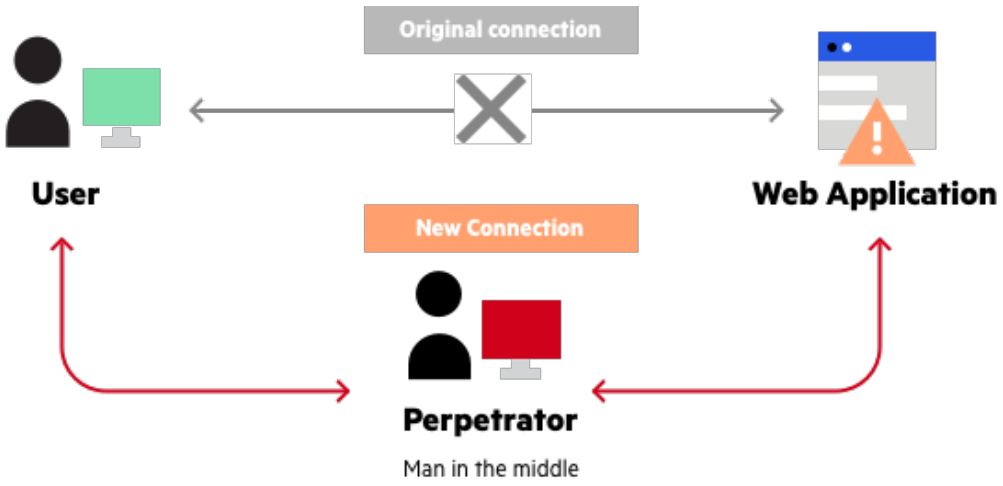


Abbildung 2: Darstellung eines Man-in-the-middle Attacks [39]

notwendig ist, um die Kommunikation zwischen Nutzern und Servern zu verschlüsseln. Das Protokoll dient als Sicherung um sensible Informationen zu schützen, sowie unautorisierte Zugänge zu verhindern und eine Vertrauensbasis für den Nutzer zu schaffen. Bei einer Man-in-the-Middle Attack wird eine falsche Vertrauensbasis aufgebaut, sodass während der Übertragung eine Dritte Partei diese sensiblen Informationen zwischen Partnern abfangen und entschlüsseln kann. Abbildung 2 verdeutlicht solch einen Angriff. Durch diesen Eingriff kann ein Angreifer zu einem bestehenden Kommunikationsfluss zwischen Nutzer und App hinzugefügt werden und fungiert dabei als Vermittler. Im Rahmen dieser Arbeit ist nicht der Nutzer das Ziel des Angriffs, sondern die Inhalte der übertragenen und empfangenen Informationen.
Im normalen Gebrauch sind diese Informationen verschlüsselt, sodass, selbst wenn ein Angreifer es schafft sich zwischen den Client und dem Host zu stellen, dieser keine Möglichkeit hat die Informationen zu lesen. In dem TLS/SSL Protokolls werden Zertifikate verwendet, um die Vertrauensbasis zwischen Host und Client zu gewährleistet und eine Sicherheitsebene bereitzustellen. Wenn jedoch eine Drittpartei ein eigenes Zertifikat erstellt und eigenhändig signiert, besteht die Möglichkeit, diese TLS-Verbindung abzufangen. Dadurch können ausgehende und eingehende Netzwerknachrichten entschlüsselt und eingesehen werden [56, 39, 38].

Diese Form der Analyse wurde von Claesson und Bjørstad [15] angewandt. Dabei wurden ebenfalls beliebte Apps auf der Android Plattform untersucht. Es konnte die Übermittlung von personenbezogene Daten wie GPS Location, Geschlecht und Alter in Apps wie Grindr und Okcupid an Werbeunterneh-

men beobachtet werden. Während in dieser Arbeit untersucht wird, ob personenbezogene Daten eventuell schon vor der Zustimmung einer Datenschutzerklärung stattfindet untersuchten Claesson und Bjørstad [15], ob solche Daten auch nach einer Deaktivierung von Ad-Tracking Einstellung stattfinden. Dabei wurde gefunden, dass einige Daten wie die *Advertising-ID* und die GPS Position selbst nach einer Deaktivierung noch versendet wurden. Der *Advertising-Identifier* stellt eine Identifikationsbezeichnung dar, die dazu dient, einem Nutzer eine eindeutige Kennung zuzuweisen, um ihn zu identifizieren. Im Zusammenhang dieser Studie ist insbesondere die *Google Advertising-ID* von großer Relevanz. Diese wird dem Nutzer bei der Erstellung eines Google Play Store-Kontos zugewiesen und dient dazu, seine Aktivitäten bei der Nutzung von Apps zu verfolgen [32].
Weiterhin untersuchten Huckvale et al. [37] ebenfalls die Konformität zwischen Datenschutzerklärungen und Apps aus dem Bereich Depression und Raucherentwöhnung. Es konnte festgestellt werden, dass 69% der Apps keine Datenschutzerklärung anzeigen. Weiterhin konnte ermittelt werden, dass ein Großteil der übermittelten Daten an nur zwei Werbeunternehmen, Google und Facebook, übertragen wurden. Allerdings nannten lediglich 43% Google und 50% Facebook namentlich in der Datenschutzerklärung.
Weitere Analysen bezüglich der Übermittlung personenbezogener Daten stellten Grundy et al. [35] in medizinischen Apps auf. Dabei wurde beobachtet, dass auch Apps aus dem medizinischen Bereich, personenbezogene Daten an Dritte Parteien weitergeben. Hierbei resultierte, dass 79% der Apps personenbezogene Daten an Dritte weiter verschickt haben, es wurde aber nicht untersucht, ob eine Differenz in der Art und Anzahl der verschickten Daten vor und nach einer Einwilligung von Datenschutzerklärungen vorliegt.

2.1.2. Statische Analyse

Statische Analysen betrachten die Programmausführung und alle möglichen Verhaltensweisen des Programms. Statische Analysen sind in der Regel konservativ und genau. Durch diese Analyse können zwar schwächere Eigenschaften eines Programms identifiziert werden, die Ergebnisse könnten jedoch weniger nützlich und aussagekräftig ausfallen.
Bei der statischen Analyse für Apps werden zunächst die *Metadaten* betrachtet. Diese geben Aufschluss über das Verhalten der App. Jede Android-App verfügt über eine Datei namens *AndroidManifest.xml*. Diese Datei enthält unter an-

derem auch Informationen über die verwendeten *Permissions*(Berechtigungen). Diese Permissions informieren darüber, ob die App Zugriff auf Funktionen wie die GPS-Position des Geräts, die Kontrolle über die Kamera oder den Zugriff auf Kontaktdaten hat. Somit können anhand der angeforderten Berechtigungen Rückschlüsse auf gesammelte personenbezogene Daten gezogen werden [70].
Für die statische Analyse muss eine App dekompiliert werden. Dabei wird der Inhalt der App durch die Umwandlung von Maschinen- und Objektcode wieder in einen lesbaren Quelltext generiert. Der Quellcode kann dann analysiert und ausgewertet werden. Hierbei können Tools wie JADX [41] zum Einsatz kommen. JADX ist ein Dex-zu-Java-Decompiler, der Android- und Apk-Dateien in Java-Quelltext zurückübersetzt. Eine teilautomatisierte Analyse kann auch mithilfe von MobSF [5] durchgeführt werden. MobSF ist ein Tool, das unter anderem JADX verwendet, um aus dem gewonnenen Quellcode Informationen wie eingebundene Softwarebibliotheken sowie die im Quellcode hinterlegten Domains und IP-Adressen zu extrahieren. Damit können mögliche Empfänger und Drittländer, an die Daten gesendet werden könnten, identifiziert werden [5, 26, 56, 51]. Eine detaillierte Erklärung zu MobSF erfolgt im Methodik-Abschnitt.

Zusammenfassend lässt sich sagen, dass beide Techniken jeweils ergänzende Stärken und Schwächen aufweisen. Durch dynamische Analysen können präzise Beobachtungen der Ausführungspfade aufgestellt werden, was detaillierte Dokumentationen ermöglicht. Allerdings können diese allein keine umfassende Aussage über das Gesamtbild treffen. Auf der anderen Seite liefern statische Analysen zwar ein Gesamtbild, aber die resultierenden Ergebnisse könnten weniger aussagekräftig sein [26].

2.2. Dark Patterns

UI und UX Design spielen eine entscheidende Rolle in der Entwicklung von Android-Apps, da sie darüber entscheiden, wie Benutzer mit der Anwendung interagieren und welche Eindrücke sie dabei sammeln. Weiterhin können diese auch den Nutzer beeinflussen, indem ansprechende Design-Elemente die Entscheidungen des Nutzers lenken. Wenn UI-Elemente so designed werden, dass der Nutzer zu bestimmten Aktionen verleitet wird, spricht man von sogenannten *Dark Patterns*.

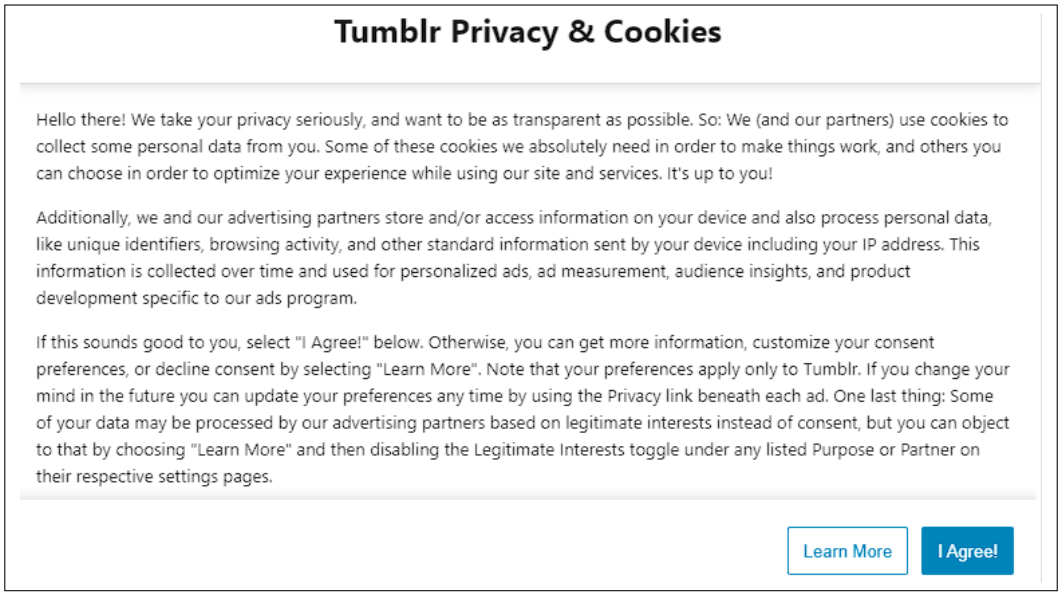


Abbildung 3: Einwilligung zur Datenschutzerklärung und Verwendung von Cookies auf tumblr.com [72]

Das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag definierte 2019 Dark Patterns als „[...] ein Sammelbegriff für Internetmuster oder -designs, die darauf ausgelegt sind, Nutzende von Onlinediensten und sozialen Netzwerken dazu zu bringen, Tätigkeiten auszuführen, die ihren eigentlichen Interessen zuwiderlaufen und mit negativen Konsequenzen verbunden sein können“ [11].
Den Ursprung finden Dark Patterns in der Optimierung von Webseiten und mobilen Anwendungen, um die Bedienbarkeit von diesen zu erleichtern und attraktiver darzustellen. Dadurch, dass Produkte immer weiter optimiert werden, um mehr Kunden zu gewinnen und die Nutzungsdauer zu erhöhen, entstehen Nachteile für den Nutzer in Form von trügerischen Benutzeroberflächen. So gehen die Interessen von Unternehmen gegen die Interessen vom Nutzer. Wenn ein Social-Media-Anbieter den Registrierungsweg so gestaltet, dass der Nutzer mit möglichst wenig *Klicks* und möglichst vielen geteilten personenbezogenen Daten einen Account erstellen kann, handelt es sich aus Sicht des Unternehmens um ein erfolgreiches Design. Für den Nutzer stellt dies einen Nachteil dar, da dieser möglicherweise gar nicht weiß, welche Daten von ihm verarbeitet werden und beispielsweise für Werbezwecke genutzt werden [62]. In Abbildung 3 wird die Einwilligung zur Datenschutzerklärung und Benutzung von Cookies auf *tumblr.com* [72] dargestellt.

Die Farbwahl auf der Webseite ist darauf ausgerichtet, den Besucher im ersten Schritt dazu zu bewegen, den hervorstechenden blauen *I Agree!*-Button zu kli-

cken. Es fällt auf, dass keine klare Option zum Ablehnen angeboten wird. Obwohl ein Feld mit *Learn More* vorhanden ist, tendiert ein Nutzer, der die Webseite schnell besuchen möchte, eher dazu, den *I Agree!*-Button zu betätigen, anstatt auf ein zweites Dialogfeld weitergeleitet zu werden.

In diesem Kontext sind auch *System 1-* und *System 2-thinking* relevant. System 1-thinking, das intuitive Denken, ist das schnelle, automatische und unterbewusste denken. Dieses Denken basiert auf vorherige Erfahrungen, um schnelle Entscheidungen zu treffen. Auf der anderen Seite beschreibt System 2-thinking das reflektierte Denken. Es ist langsam, bewusst und basiert auf logischem Denken, sodass ein aktiver Entscheidungsprozess durchgeführt wird [42, 53].
Im obigen Beispiel lässt sich erkennen, dass die Designer das System-1-thinking ausnutzen. Der Nutzer wird durch die hervorgehobene *I Agree!*-Option dazu gedrängt, eine schnelle und automatische Entscheidung zu treffen, sodass dieser möglicherweise gar nicht erst dazu kommt, das *Learn More*-Feld zu betätigen und zu einem System-2-thinking zu gelangen. Nutzer, welche sich unbewusst auf das System 1-thinking stützen, werden dadurch oft Opfer von manipulativen Techniken im Design.
Dark Patterns beschreiben ein sehr großes Feld mit vielen unterschiedlichen Erscheinungsformen im Design. Deswegen können diese in feinere Kategorien unterteilt werden. Diese Unterteilung ermöglicht eine präzisere Analyse und Beschreibung der verschiedenen Techniken, die in Designentscheidungen eingesetzt werden, um Nutzer bewusst oder unbewusst zu manipulieren. In der für diese Analyse herausgezogene Literatur, wurden spezifische Kategorien von Dark Patterns ausgewählt, die für diese Arbeit relevant sind [33, 19, 36, 34, 13]:

1. **Missing Consent Notices**
2. **Disguised Data Collection**
3. **Obfuscation**
4. **Forced Action**
5. **Misdirection**
6. **Forced Registration**

Im Fall von **Missing Consent Notices** fehlen wesentliche Teile der Benutzeroberfläche, die ein Nutzer normalerweise erwarten würde. Zum Beispiel werden dem Nutzer keine Kontrollkästchen angezeigt, um die angeforderten Abgaben

Abbildung 4: Misdirection durch gefärbten *Alle akzeptieren*-Button [57]

zu personenbezogenen Daten zu spezifizieren. Somit wird ihm nicht die Möglichkeit gegeben, eine Auswahl bei der Einwilligung zu treffen [36].
Bei der **Disguised Data Collection** werden die Daten eines Nutzers verdeckt gesammelt, selbst wenn keine ausdrückliche Einwilligung von ihm vorliegt [34].
Die **Obfuscation** erschwert die Benutzerführung durch das Interface. Dabei werden wesentliche Informationen visuell unterdrückt oder neben weniger wichtigen Informationen in den Vordergrund gestellt, um diese zu verbergen. Abbildung 3 von der Tumblr-Webseite [72] veranschaulicht dieses Dark Pattern. Die entscheidenden Informationen zu gesammelten personenbezogenen Daten sind hinter dem *Learn More*-Button verborgen, während der Nutzer dazu gedrängt wird, die *I Agree!*-Option auszuwählen [19].
Forced Action beschreibt das Manipulieren vom Nutzer, um eine bestimmte Aktion zu erzwingen. Dabei könnten in Einwilligungserklärungen keine Option zum Ablehnen angeboten werden. In diesem Kontext ist das sogenannte **Privacy Zuckering**, welches eine Variante vom Forced Action beschreibt, ebenfalls relevant. Dabei werden beispielsweise bei der Registrierung mehr personenbezogene Daten vom Nutzer herausgelockt als eigentlich notwendig sind. Dies geschieht unter anderem durch vorab ausgefüllte Checkboxen oder das Auffordern vom Nutzer selber weitere Angaben zu geben, obwohl die Registrierung auch ohne diese Angaben abgeschlossen werden kann [33].
Durch eine **Misdirection** wird die Aufmerksamkeit des Nutzers gelenkt. Im Falle von Designelementen können diese in Form von gefärbten oder vergrößerten

Elementen auftreten. In Abbildung 4 ist ein Fenster zu Cookie-Einstellungen sichtbar. Dabei werden einzelne Bereiche der Einstellungen über die Verwendung von Cookies der Website, wie Statistik, Komfort und Personalisierung in kleiner Schriftgröße aufgelistet. Der Nutzer hat die Möglichkeit entweder *Auswahl speichern* oder *Alle Akzeptieren* auszuwählen. Deutlich erkennbar ist das unterschiedliche Design der einzelnen Elemente. Die Option *Auswahl speichern* ist ausgegraut und verblasst dargestellt. Im Kontrast wird *Alle akzeptieren* mit einer deutlichen gelben Farbe präsentiert. Zusätzlich wird das Steuerelement noch einmal umkreist, was den Nutzer dazu verleitet, dieses Element zu wählen [33].
Zuletzt stellt die **Forced Registration** eine weitere Form einer Forced Action dar. In diesem Fall wird der Nutzer dazu gezwungen, ein Konto zu erstellen, um die App weiterhin nutzen zu können. Diese erzwungene Registrierung ermöglicht es, ein Nutzerprofil anzulegen, was wiederum zur Sammlung von personenbezogenen Daten genutzt werden kann [13].
Zusammenfassend ist die Untersuchung von Dark Patterns entscheidend, um sicherzustellen, dass Datenschutzrichtlinien nicht nur formal korrekt, sondern auch für die Benutzer verständlich und akzeptabel sind.

Eine zu dieser Arbeit vergleichbare Untersuchung führten Geronimo et al. [29] zum Anteil an Dark Patterns und der Wahrnehmung der Nutzer durch. Dabei wurden Dark Patterns zunächst in einige Kategorien aufgeteilt und daraufhin 240 beliebte Apps aus dem Google Play Store [31] analysiert. Es konnten in 95% der Apps Dark Patterns aus mindestens einer Kategorie festgestellt werden. 10% der analysierten Apps beinhalteten 0,1 oder 2 Dark Patterns, 37% der Apps beinhalteten 3 bis 6 Dark Patterns, sowie 49% 7 oder mehr. Im nächsten Schritt wurde mithilfe einer Online-Umfrage erarbeitet, wie hoch der Anteil an Nutzern ist, die Dark Patterns in verschiedenen Apps **nicht** feststellen können (*Dark Pattern-Blindness*). Es wurde ermittelt, dass 55% der Befragten keine Dark Patterns finden konnten, 20% sich unsicher waren und 25% die Dark Patterns aufdecken konnten. Dies weist auf eine mangelnde Aufklärung über Dark Patterns bei Nutzern hin.
Während diese Arbeit über den Einsatz von Dark Patterns in Apps aufklärt, versuchten Van Kleek et al. [73] Nutzer schon vor dem Download der App über den Gebrauch ihrer Daten aufzuklären. Mithilfe von sogenannten *Data Controller Indicators* soll die Transparenz im Datenumgang von personenbezogenen Daten für Nutzer verbessert werden. Dabei wurden Indikatoren für einen simulierten App-Store entwickelt. Diese Indikatoren sollen dem Nutzer den im Hintergrund von Apps stattfindenden Datenfluss, den Grund für die Datensammlung

und die Unternehmen, an die die Daten gesendet werden, transparent darstellen. Anschließend wurden Testpersonen gebeten, Apps in diesem simulierten App Store mit der erweiterten Anzeige über den Gebrauch personenbezogener Daten zu verwenden. Die Ergebnisse verdeutlichten, dass Nutzer dazu neigten, Apps zu bevorzugen, die die minimale Menge an verarbeiteten personenbezogenen Daten aufwiesen. Weiterhin konnte festgestellt werden, dass die Nutzer ein höheres Selbstbewusstsein in ihren Entscheidungen besaßen, wenn Apps eine transparentere Darstellung über den Gebrauch der Nutzerdaten hatten. Van Kleek et al. [73] zeigen, dass es möglich ist, Nutzer schon vor dem Download einer App über den Gebrauch ihrer Daten aufzuklären, sodass diese fundiertere Entscheidungen treffen können.

2.3. Die Datenschutz-Grundverordnung

Die Datenschutz-Grundverordnung (DSGVO) ordnet rechtliche Vorgaben zur Weiterverarbeitung von personenbezogenen Daten auf. Sie soll dazu dienen, die Transparenz von Websites, Unternehmen und Apps für den Endnutzer zu erhöhen [69]. Konkret kommen App-Betreiber ihren Verpflichtungen durch die Bereitstellung von Datenschutzerklärungen nach. Oftmals lesen Nutzer diese Erklärungen jedoch nicht, da diese meist zu lang und nicht für juristische Laien verständlich sind [9]. Des Weiteren gibt es keine Möglichkeit für Laien zu überprüfen, ob die Inhalte der Datenschutzerklärung der Wahrheit entsprechen. Laut DSGVO Art. 13 [20] sind Betreiber verpflichtet unter anderem folgende Angaben zu gewährleisten:

- „die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung;“ [20]
- „gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten[...]“ [20]
- „gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln[...]“ [20]

2.3.1. Personenbezogene Daten

Personenbezogene Daten werden bei der DSGVO nach Art. 13 wie folgt definiert: „Personenbezogene Daten sind alle Informationen, die sich auf eine iden-

tifizierte oder identifizierbare lebende Person beziehen“ [45]. Daher ist es entscheidend, bei der App-Analyse zu prüfen, ob die Nutzer anhand der erfassten Daten identifizierbar sind. Beispiele für personenbezogene Daten sind:

- Name und Vorname
- Privatanschrift
- E-Mail-Adresse in Form von: „vorname.nachname@unternehmen.com“
- Standortdaten
- IP-Adresse
- Advertising-Identifier [45]

Weiterhin können verschiedene Teilinformationen, die in Kombination zur Identifizierung einer bestimmten Person führen können, ebenfalls personenbezogene Daten darstellen. Hieraus ergibt sich, dass Apps, die durch eine Kombination von gesammelten Informationen ein umfassendes Bild des Anwenders zeichnen können, personenbezogene Daten sammeln. In Gesundheits-Apps werden zusätzliche Gesundheitsdaten und damit sensible personenbezogene Daten erhoben. Die Informationspflichten beziehen sich nur auf personenbezogene Daten, sodass die statische und dynamische Analyse sicherstellen müssen, dass in den Apps personenbezogene Daten erhoben werden [44, 45, 20].

2.3.2. Empfänger und Drittländer

Oftmals werden Empfänger von personenbezogenen Daten und Drittländer in Datenschutzerklärungen lediglich umschrieben. Die rechtliche Grundlage für die Angabe von Empfängern personenbezogener Daten sowie Informationen zu Drittlandsübermittlungen ist dabei umstritten. Es gibt Diskussionen darüber, ob die Verwendung allgemeiner Kategorien wie beispielsweise *Advertisement-Partners* oder *Service Partners* anstelle der namentlichen Nennung von Dritten oder Empfängern zulässig ist. Im Falle der Empfänger schreibt Art. 13. Abs. 1 lit. eDSGVO: „gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten[...]“ [45]. Demnach wird in Kühling und Buchner [46] argumentiert, dass nur in dem Falle eines nicht absehbaren Empfängers bei der Datenerhebung, eine Umschreibung nach der Kategorie zulässig sein soll. Sobald ein Empfänger namentlich genannt werden kann, sollte es nicht möglich sein, diesen mit einer Kategorie zu umschreiben. Auf der anderen Seite ist laut

Becker et al. [7] der Wortlaut offen, sodass eine Wahl zwischen namentlicher Nennung oder einer Kategorie möglich ist [46, 64, 30, 52, 7, 44].
Ein ähnlicher Meinungsstreit gilt auch für die Information in den Datenschutzerklärungen über die Drittländer. Es besteht Unklarheit darüber, ob Drittländer gemäß Art. 13 Abs. 1 lit. f DSGVO explizit genannt werden müssen. Der Text der DSGVO legt dies nicht eindeutig fest, da Art. 30 Abs. 1 S. 2 lit. e DSGVO die „Angabe des Drittlandes“ [45] vorschreibt, während dies bei Artikel 13 Absatz 1f nicht der Fall ist. Die Art.-29-Datenschutzgruppe [4] sowie der diese ablösende europäische Datenschutzausschuss [10] vertreten die Meinung, dass das Drittland in der Regel namentlich genannt werden sollte. Die explizite Nennung entspricht auch dem Zweck der Informationspflichten gemäß Artikel 13 der DSGVO, da die Nutzer in die Lage versetzt werden sollen, das Risiko der Datenverarbeitung besser einschätzen zu können. Bei einer allgemeinen Formulierung wie z. B. *außerhalb der Europäischen Union* ist eine präzise Risikoeinschätzung kaum möglich [12, 10, 4].
Es bleibt unklar, wann eine allgemeine Umschreibung für die Information über Drittländer und Empfänger zulässig ist. Durch die statische und dynamische Untersuchung könnte eine Argumentationsbasis geschafft werden, da sie technisch erfasst, wie viele Empfänger und Drittländer in der Praxis unter einer Kategorie zusammengefasst werden [44].

2.3.3. Widerruf und Sprache

In der Studie spielen auch die angebotenen Möglichkeiten zum Widerruf der Einwilligung und die Konsistenz der Sprache in den angezeigten Datenschutzerklärungen eine entscheidende Rolle.
Die Apps werden geprüft, ob sie die Möglichkeit bieten, die Einwilligung zur Verarbeitung personenbezogener Daten zu widerrufen. Hierbei wird nach einer entsprechenden Option innerhalb der App gesucht. Gemäß Art. 7 Abs. 1 lit. 1 der DSGVO hat die betroffene Person das Recht, ihre Einwilligung jederzeit zu widerrufen [25]. Es ist entscheidend, dass die untersuchten Apps klare und leicht zugängliche Möglichkeiten für den Widerruf der Einwilligung bereitstellen, um die Ausübung dieses Rechts zu erleichtern und sicherzustellen, dass die Datenschutzstandards eingehalten werden.

Während die Bedienung der zu untersuchenden Apps in der Regel auf Deutsch erfolgt, wird die Konsistenz der Sprache im Hinblick auf die Datenschutzerklärung geprüft. Die Ausführung der App in deutscher Sprache erfordert eine entsprechende Darstellung der Datenschutzerklärung auf Deutsch. Gemäß Art. 12

Abs. 1 der DSGVO gilt: „Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen[...], die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln[...]“ [24]. Wenn die Datenschutzerklärung in einer anderen Sprache, beispielsweise Englisch, angezeigt wird, obwohl die App auf Deutsch ausgeführt wird, wirft dies Fragen bezüglich des Datenschutzes auf.

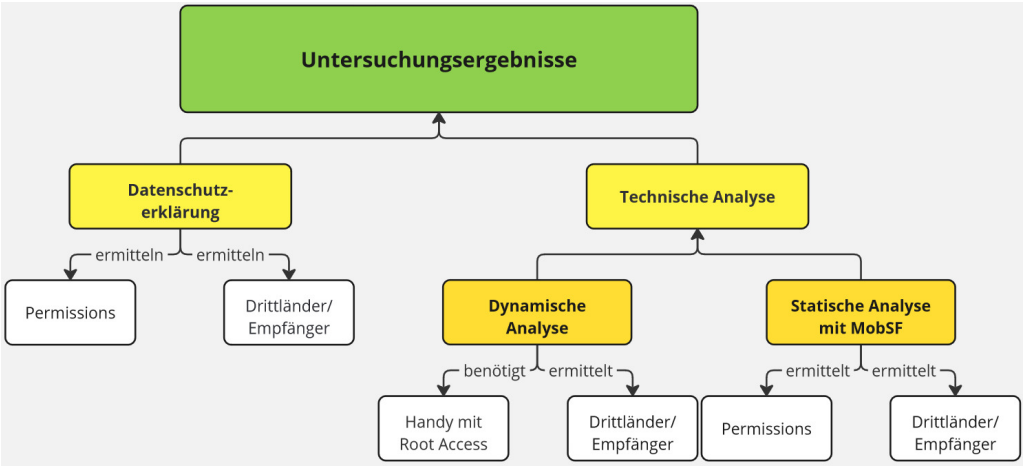


Abbildung 5: Methodologie zur Versuchsdurchführung

3. Methodik

In diesem Abschnitt wird die methodische Herangehensweise an der vorliegenden Studie beschrieben. Zunächst werden die Kriterien und Gründe zum Einschluss oder Ausschluss bei der Auswahl der zu analysierenden Apps betrachtet. Im nächsten Schritt wird die Methode zum Präparieren eines Smartphones für die folgenden Analysen untersucht. Auf dem Handy müssen einige spezifische Berechtigungen aktiviert werden, um die dynamischen Analysen zu ermöglichen. Daraufhin werden die beiden Methoden zur Analyse der Apps vorgestellt. Bei der ersten Methode handelt es sich um eine statische Analyse. Hierbei wird die App analysiert, ohne, dass die App dabei aktiv ausgeführt wird. Dafür wird die Installationsdatei der App selber betrachtet. Im zweiten Schritt wird eine dynamische Analyse durchgeführt. Dabei wird die App ausgeführt, die Ergebnisse aus der statischen Analyse bestätigt und das Verhalten der App bei Nutzereingaben betrachtet. Insbesondere ist das Verhalten der App bei der Vermittlung von Datenschutzerklärungen relevant. Im letzten Schritt wird die Datenschutzerklärung selber betrachtet. Dabei werden die direkte und/oder indirekt genannten Dritten, gesammelte personenbezogene (Gesundheits-)Daten, sowie die Länder, zu denen diese übertragen werden, tabellarisch verzeichnet. Daraufhin können die Ergebnisse miteinander verglichen werden, sodass Übereinstimmungen und Divergenzen zwischen der technischen Seite der App und der Datenschutzerklärung ermittelt werden. In der Abbildung 5 wird der durchzuführende Untersuchungsablauf anschaulich dargestellt.

Einschlusskriterien	Ausschlusskriterien
Apps, welche die höchste Downloadzahl im Google Play Store aufweisen	Covid-19-Apps (insbesondere des Robert-Koch-Instituts)
Apps stammen aus den App Store Kategorien „Gesundheit & Fitness“, sowie „Medizin“	Apps, die auf eine Interaktion mit ärztlichem Personal angewiesen sind (z.B. Terminfindungs-Apps oder Apps zur Videosprachstunde)
Kostenlose Apps	Apps, die auf die Ausbildung von medizinischem Personal ausgerichtet sind
	Digitale Gesundheitsanwendungen – DiGa (Apps auf Rezept)
	Service-Apps der gesetzlichen Krankenkassen in Deutschland

Tabelle 1: Auswahlkriterien zur Auswahl der Apps [5]

3.1. Auswahl der zu untersuchenden Apps

Für die Analyse wurden 20 Apps aus dem Google Playstore in dem Bereich *Gesundheit & Fitness* sowie *Medizin* ausgewählt. Weiterhin sollen folgende Anforderungen erfüllt werden:

- Es soll eine möglichst große Bandbreite an Nutzern angesprochen werden, damit die Analyse die höchste Relevanz aufweisen kann.
- Es sollen Apps aus dem Bereich der Gesundheits- & Fitness-Apps, sowie Medizin-Apps gewählt werden, da hier eine transparente und sichere Kommunikation mit dem Nutzer besonders notwendig ist, da ein Umgang mit sensiblen Daten stattfindet.
- Der Versuchsaufbau muss ohne Interaktionen mit ärztlichem Personal durchführbar sein und die Apps dürfen keinen gesonderten Zugang benötigen (DiGA apps).

In Tabelle 1 werden die Kriterien zur Auswahl der Apps aufgelistet.

Aus diesen Kriterien wurden die Apps anhand der Downloadzahl über die Webseite AndroidRank [6] ermittelt. Die ausgewählten Apps aus dem Bereich Health und Fitness werden in Tabelle 2 und Apps aus dem Bereich Medizin in Tabelle 3 abgebildet.

Rang	Name	Entwickler	Downloadzahl
1.	Samsung Health	Samsung Electronics Co., Ltd	1B
2.	Period Calendar Period Tracker	Simple Design Ltd.	100M
3.	Home Workout – No Equipment	Leap Fitness Group	100M
4.	Zepp Life(MiFit)	Anhui Huami Information Technology Co., Ltd.	100M
5.	MyFitnessPal: Calorie Counter	MyFitnessPal, Inc.	100M
6.	Six Pack in 30 Days	Leap Fitness Group	100M
7.	Google Fit: Activity Tracking	Google LLC	100M
8.	Flo Ovulation & Period Tracker	Flo Health Inc.	50M
9.	Sweatcoin	Sweatco Ltd.	50M
10.	Lose Weight App for Men	Leap Fitness Group	50M

Tabelle 2: Auswahl der untersuchten Apps aus dem Bereich Health und Fitness

Rang	Name	Entwickler	Downloadzahl
1.	My Calendar - Period Tracker	SimpleInnovation	10M
2.	amma Pregnancy & Baby Tracker	PERIOD TRACKER & PREGNANCY AND BABY CALENDAR	10M
3.	Blood Pressure	Klimaszewski Szymon	10M
4.	Ada – check your health	Ada Health	5M
5.	Pregnancy Tracker	Amila	5M
6.	Period and Ovulation Tracker	SMSROBOT LTD	5M
7.	MyTherapy Pill Reminder	MyTherapy	5M
8.	Ladytimer Ovulation Calendar	Vipos Apps	5M
9	Medscape	WebMD, LLC	5M
10.	Ovia Pregnancy & Baby Tracker	Ovia Health	1M

Tabelle 3: Auswahl der untersuchten Apps aus dem Bereich Medizin

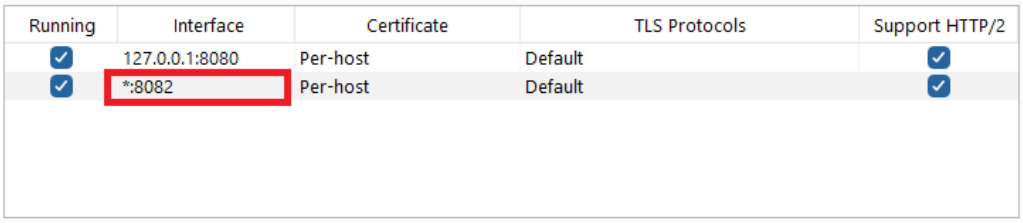


Abbildung 6: Port Einstellungen in Burp Suite [61]

3.2. Dynamische Analyse

3.2.1. Aufbau

Die Methodik der Analyse in dieser Arbeit ist an der Methode von Claesson und Bjørstad [15] angelehnt. Für die Testumgebung wird ein Google Pixel 2 XL mit Android 10 in einem Heimnetzwerk verwendet. In der dynamischen Analyse werden die Netzwerkkommunikationen der Apps zur Betriebszeit mithilfe von Burp Suite [61] analysiert. Burp Suite ist ein Tool der Entwickler Portswigger und wird im Bereich Web Application Security und Testing eingesetzt. Weiterhin kann das Tool für Analysezwecke bei HTTP-Verkehr verwendet werden. Burp Suite besitzt einen abfangenden Proxyserver, welches ausgehende Nachrichten von einer Website oder einem Gerät abfangen kann. Für die Konfiguration muss Burp Suite so eingestellt werden, dass ein sogenannter *Port* erstellt wird, der eine Art Tor für alle ausgehenden Nachrichten darstellt.

Für die Analyse wird in Burp Suite der Proxyserver mit dem Port 8082 erstellt (siehe Abbildung 6). Das bedeutet, dass alle ausgehenden Nachrichten vom Handy, die durch diesen Port laufen von Burp Suite abgefangen werden können. Schließlich müssen die Netzwerkeinstellungen auf dem Handy noch so eingestellt werden, dass alle ausgehenden Netzwerknachrichten vom Handy ebenfalls über den gleichen Port laufen. Daraufhin lassen sich alle vom Handy ausgehenden HTTP-Netzwerknachrichten im Interface von Burp Suite einsehen [61].

Der Großteil des ausgehenden Netzwerkverkehrs wird jedoch verschlüsselt über das HTTPS-Protokoll übertragen. Dennoch müssen personenbezogene Nachrichten, um sie zu identifizieren, entschlüsselt einsehbar sein. Durch die Verwendung des Burp Suite-Tools kann ein selbst signiertes Zertifikat installiert werden, um eine Man-in-the-Middle Attack durchzuführen. Hierbei wird das Zertifikat installiert, sodass die zu untersuchende App Burp Suite als Zwischeninstanz vertraut und somit der Netzwerkverkehr entschlüsselt werden kann.

Obwohl Android 10 das Installieren von selbst signierten Zertifikaten erlaubt, verfügt es über zwei unterschiedliche Speicher. Diese selbst installierten Zertifikate werden im Speicher für Nutzer-Zertifikate abgelegt. Apps, die auf dem Gerät installiert sind vertrauen jedoch keinem Zertifikat aus diesem Speicher. Installierte Apps vertrauen ausschließlich Zertifikaten aus dem *Trusted Credentials*-Speicher [21].
Die Entschlüsselung von Netzwerknachrichten ist somit nicht möglich. Um diese Sicherheitsmaßnahme zu umgehen wird das Handy *gerooted*. Ein gerootetes Handy erlaubt es dem Benutzer privilegierte Aktionen auszuführen, die normalerweise nicht ausführbar sind. In der Regel geschieht dies dadurch, dass Prozesse mit UID zero ausgeführt werden und dadurch alle privilegierten Prozesse die Permission Checks vom Kernel des Systems ignorieren [55]. Auch kann der Benutzer dadurch System Dateien hinzufügen, bearbeiten oder löschen [60].
Zum Rooten des Geräts muss das Handy zunächst vorbereitet werden. Android erschwert es Änderungen an dem System des Kernels vorzunehmen, deswegen liegt es nahe gar keine Änderungen direkt auf dem Kernel des Systems durchzuführen, sondern stattdessen den Bootloader zu bearbeiten. Der Bootloader hat die Funktion, den Kernel auf einem Gerät zu initialisieren und zu starten. Des Weiteren überwacht der Bootloader den Gerätestatus [66]. Um die gesonderten Rechte zu erhalten, muss ein Programm auf den Bootloader installiert werden. Dafür wird der Bootloader zunächst freigeschaltet um Dritte Programme direkt auf dem Bootloader initialisieren zu können. Dies lässt über die von Android bereitgestellten erweiterten Optionen umsetzen.
Nach dem Freischalten des Bootloaders wurde Magisk [55] auf dem Bootloader installiert. Magisk ist ein Tool, welches benutzt wird, um Modifikationen auf Android Geräten durchzuführen, ohne das eigentliche System zu verändern. Magisk wird als *systemlose* rooting Methode bezeichnet und erlaubt es dem Nutzer die komplette Kontrolle über das Handy zu erhalten. Magisk wird nicht auf dem System des Geräts installiert, sondern wird durch den Bootloader direkt beim Start des Geräts initialisiert [54]. Ein weiterer Vorteil dieser Methode ist, dass viele Apps rooted Geräte aufspüren können, unter Anderem Googles *SAFETYNET* [22]. Die Aufspürung des rooted Geräts, welches die Ausführung der App und damit die Ergebnisse der Analyse beeinflussen könnte, wird mit einer Installierung auf dem Bootloader erleichtert. Nach der Installation von Magisk auf dem Bootloader wird ein voll privilegierter Magisk Daemon mit einer UID:0 beim Start des booting Prozesses ausgeführt. Der Magisk Daemon kann nun jedem Prozess, welches Root-Rechte benötigt, diese erteilen [55]. Schließlich erlaubt es Magisk auch Erweiterungen zu installieren. Für die Analyse wurde unter anderem die Erweiterung *Magisk Trust User Certs [8]* installiert. Das Mo-

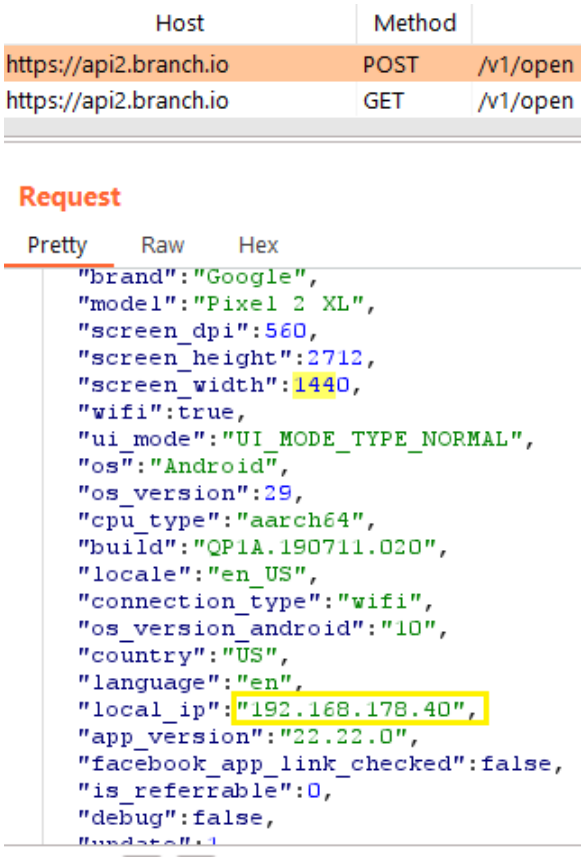


Abbildung 7: Überwachte Netzwerkkommunikation mithilfe von Burp Suite [5].

dul erlaubt es alle vom Nutzer installierten Zertifikate beim Systemstart in den Speicher der vertrauten Zertifikate zu installieren, sodass alle Apps auf dem Gerät diesen Zertifikaten vertrauen. Dadurch können in Zusammenhang mit Burp Suite alle verschlüsselten ausgehenden und eingehenden HTTPS Nachrichten vom Gerät entschlüsselt werden.

3.2.2. Durchführung der dynamischen Analyse

Nachdem das Handy vorbereitet wurde, werden die Netzwerkaktivitäten mithilfe von Burp Suite untersucht. Dabei dient Burp Suite als abfangender HTTPS-Proxy, der die verschlüsselten TLS-Daten in einem lesbaren Format darstellt. In Abbildung 7 wird dies beispielhaft vorgestellt. Hierbei werden einige personenbezogene Daten, wie die lokale IP-Adresse, Land und Sprache vom Host *branch.io* verschickt. Durch Burp Suite lässt sich die Übertragung abfangen und entschlüsseln [16]. Zu erwähnen ist, dass viele der verschickten Nachrichten zusätzlich noch in einem nicht-lesbaren Format kodiert sind. Kodierungen sind

streng genommen keine Verschlüsselungen, sondern werden oftmals verwendet, um die Dateigröße von übertragenen Informationen zu verringern. Gängige Kodierungsarten, welche Einsatz in HTTPS Nachrichten finden sind: URL, Base64, ASCII Hex, Octal, Binary oder GZIP. Ist die Kodierungsart bekannt, lassen sich die Nachrichten meist dekodieren und in einem lesbaren Format darstellen. Jedoch wird die Kodierungsart oftmals nicht beim Versenden der Nachrichten bekannt gegeben, sodass das Dekodieren erschwert wird. Burp Suite bietet Tools, die die Kodierungsform finden und entsprechend dekodieren können. Diese Möglichkeit wurde in der Analyse häufig genutzt, allerdings konnten einige Nachrichten, hauptsächlich von Google, nicht dekodiert werden, wodurch diese nicht lesbar waren [17].

Für die Durchführung der dynamischen Analyse wurde eine Testperson namens *Petra Muster* erstellt. Dabei wurden einige Gesundheitsdaten wie Gewicht, Alter, Geschlecht, Temperatur und Geburtsdatum generiert. Zusätzlich wurden technische Daten wie die Google Advertising-ID und die Device-ID erfasst, um das Auffinden dieser im Datenstrom der Netzwerkübertragungen zu erleichtern.

Zu Beginn der dynamischen Analyse wird die App neu installiert und für 5 Minuten ohne Interaktion ausgeführt. Während dieses Zeitraums werden die Netzwerkübertragungen betrachtet. Im nächsten Schritt wird die App bis zu dem Punkt ausgeführt, an dem eine Einwilligung zu einer Datenschutzerklärung erforderlich ist. Falls zu diesem Zeitpunkt bereits personenbezogene Daten übertragen werden, stellt dies einen Verstoß gegen die Datenschutzerklärung dar, da zu diesem Zeitpunkt noch keine Einwilligung gegeben wurde. Ebenfalls wird untersucht, ob die Sprache der angezeigten Datenschutzerklärung konsistent mit der Sprache der Ausführung ist. Anschließend wird die Einwilligung erteilt, und die App wird durch alle Funktionalitäten durchgeführt, um festzustellen, ob die übertragenen Daten und die Länder, an die die Daten verschickt werden, mit der Datenschutzerklärung konform sind. Schließlich wird überprüft, ob ein Widerruf zur Einwilligung der Datenschutzerklärung innerhalb der App angeboten wird.

3.3. Statische Analyse

Für die statische Analyse wird die App untersucht, ohne ausgeführt zu werden. Für diesen Teil werden die Apps mit dem Tool Mobile Security Framework

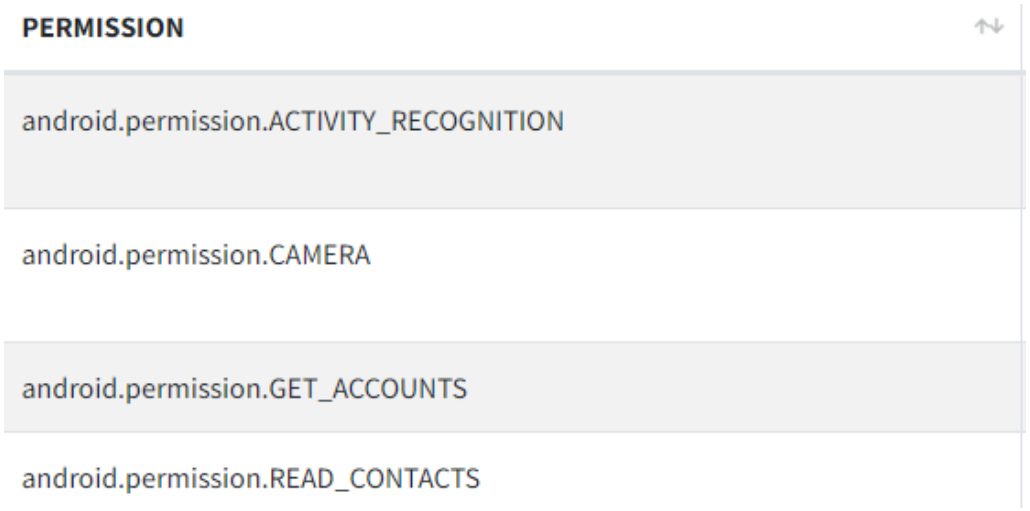


Abbildung 8: Übersicht der ermittelten Permissions einer App mithilfe von MobSF [5]

(MobSF) [5] analysiert. Dabei handelt es sich um ein Framework für Penetrationstests, eine Malware Analyse und Security Assessments mithilfe von statischen Analysen. MobSF ist ein umfangreiches Tool und es werden nicht alle bereitgestellten Funktionen in der Arbeit verwendet. Im Folgenden werden die relevanten Funktionen für diese Arbeit näher erläutert.
MobSF ermöglicht es, die verwendeten Permissions einer App zu betrachten. Diese Berechtigungen werden aus dem AndroidManifest.xml ermittelt. Im Manifest werden die Berechtigungen aufgeführt, für die eine App den Nutzer um Zustimmung bitten kann. Wenn eine solche Erlaubnis erforderlich ist, erhält der Nutzer ein angezeigtes Fenster, in dem er zustimmen kann. Solche Berechtigungen können den Nutzer beispielsweise um Standortinformationen oder um Zugriff auf die Kamera bitten. Abbildung 8 zeigt, wie diese aufgelistet sind. Es wird untersucht, ob sich anhand der Permissions mögliche gesammelte personenbezogene Daten herleiten lassen, um diese später mit den Angaben über personenbezogene Daten aus Datenschutzerklärungen vergleichen zu können. Permissions können Hinweise darüber geben, ob beispielsweise, Rechte an die App erteilt werden, um den Standort einer Person zu ermitteln [44].

Durch das Auflisten der verschiedenen Permissions kann in späteren Schritten tiefer auf auffällige Permissions eingegangen werden [68].
Im nächsten Schritt können im Abschnitt der Security Analysis die Netzwerksicherheit betrachtet werden(siehe Abbildung 9). Die Ergebnisse können ähnlich wie bei den Permissions auf mögliche Probleme hinweisen, welche näher analysiert werden müssen. In der Abbildung 9 ist anhand des ersten Eintrages zu sehen, dass die App auch unverschlüsselte Nachrichten versendet. Hinweise

NO	ISSUE	SEVERITY
1	Clear text traffic is Enabled For App [android:usesCleartextTraffic=true]	high
6	**Activity** (com.myfitnesspal.feature.recipes.ui.activity.RecipesAndFoods) is not Protected. [android:exported=true]	high
7	**Activity** (com.facebook.CustomTabActivity) is not Protected. [android:exported=true]	high

Abbildung 9: Übersicht der ermittelten Netzwerken-Eigenschaften einer App in MobSF [5]

dieser Art erfordern weitere Untersuchungen, da die Sicherheit der personenbezogenen Daten des Nutzers nicht gewährleistet sein könnten.
MobSF erlaubt es zudem, die Kommunikation zwischen der zu analysierenden App und verteilten Servern zu ermitteln. Informationen wie der Standort, IP-Adresse, sowie Domain-Name des jeweiligen Servers können dadurch ergründet werden. Mithilfe der IP-Adresse und des Domain-Namen können nähere Informationen über die Betreiber des Servers ermittelt werden. Dadurch kann festgestellt werden, ob es sich um eine Dritte Partei handelt und aus welcher Branche diese Partei stammt, wie etwa ein Werbeunternehmen oder ein Servicebetreiber. Durch die Standort-Informationen wird geprüft, ob die Daten ins Ausland verschickt werden. In Abbildung 10 wird ein Ausschnitt einer untersuchten Healthcare App dargestellt. Hier ist zu sehen, dass eine Kommunikation an das Werbeunternehmen *Inmobi* besteht. Inmobi ist ein in Indien basiertes Werbeunternehmen [40]. Die statische Analyse ermöglicht das Erforschen verwendeter Libraries und dient als Basis für die weiterführenden Schritte, insbesondere der dynamischen Analyse. Die Ergebnisse aus dieser Untersuchung werden schließlich katalogisiert und mit den Einträgen aus den Datenschutzerklärungen abgeglichen [68].

3.4. Dark Patterns

Bei Dark Patterns handelt es sich um UX-Design Elemente, um das Verhalten von Nutzern zu beeinflussen. Unternehmen haben unterschiedliche Interessen, sodass Benutzeroberflächen entwickelt werden, um bestimmte Geschäftsziele zu erreichen. In dieser Arbeit wurden Dark Patterns in angezeigten Einwilligungserklärungen betrachtet. Dafür wurden alle angezeigten Fenster bezüg-

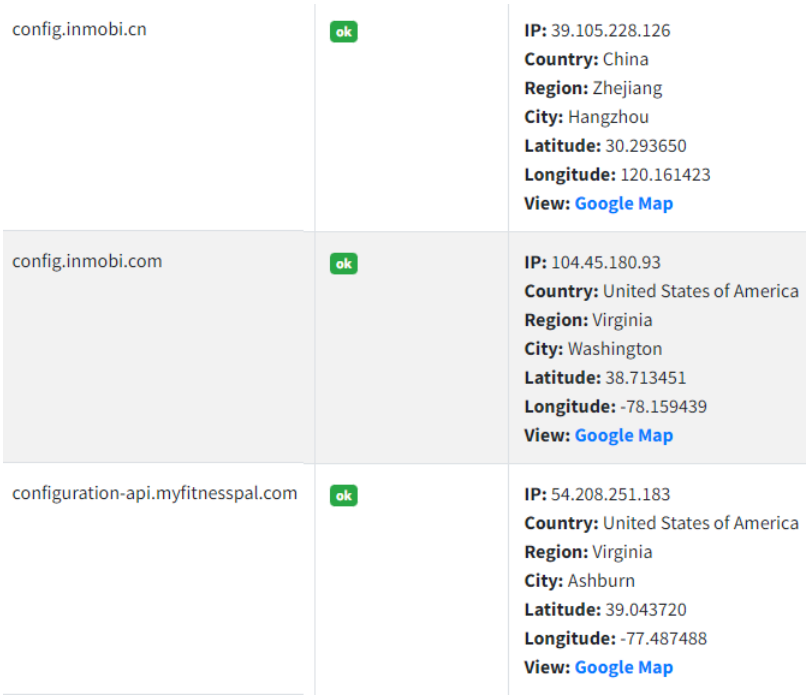


Abbildung 10: Übersicht der ermittelten Server durch MobSF [5]

lich Einwilligungserklärungen während der dynamischen Analyse mithilfe von Screenshots gespeichert und im weiteren Verlauf analysiert [62].

Zunächst wurde ein Überblick über mögliche Dark Patterns geschaffen, und die auftretenden Fälle dokumentiert. Anschließend wurde eine Liste von Dark Patterns erstellt, die wiederholt auftraten. Dadurch konnten die Einwilligungserklärungen der Apps in diese Kategorien eingeordnet werden. Die resultierende Liste enthielt folgende mögliche Dark Patterns: Misdirection, Forced Action, Obfuscation, Disguised Data Collection, Missing Notices and Options und Forced Registration. Im Abschnitt aktuelle Forschungen und Studienergebnisse werden diese näher erläutert.

3.5. Analyse der Datenschutzerklärung

Vor der technischen Analyse erfolgt die Untersuchung der Datenschutzerklärung. Dabei wird die jeweilige Datenschutzerklärung gelesen, und alle Drittempfänger, Drittländer und gesammelten personenbezogenen Daten werden katalogisiert.
Im ersten Schritt werden alle genannten Drittempfänger erfasst. Diese können entweder eindeutige Bezeichnungen wie Google oder Facebook sein, aber auch

allgemeinere Umschreibungen wie *Business Partners* oder *Companies for purposes of analytics*.
Im nächsten Schritt wird die Datenverarbeitung im Ausland betrachtet. Alle genannten Länder im Ausland werden aus der Datenschutzerklärung ermittelt, und die zugehörige Rechtsgrundlage wird identifiziert. Auch hier werden Drittländer entweder namentlich genannt oder es werden Umschreibungen wie *Outside European Economic Area* verwendet.
Schließlich werden alle genannten personenbezogenen Daten sowie Gesundheitsdaten katalogisiert.
Die erfassten Ergebnisse werden abschließend tabellarisch mit den ebenfalls ermittelten Daten aus der statischen und dynamischen Analyse verglichen. Auf diese Weise können Überschneidungen und Unterschiede zwischen der Datenschutzerklärung und dem tatsächlichen Betrieb der App aufgeklärt werden.

4. Studienergebnisse

4.1. Empfänger

Ein wesentlicher Bestandteil der Analyse lag in der Betrachtung der Empfänger, an die eine Kommunikation aufgebaut wurde. Die gefundenen Empfänger können in folgende Gruppen eingeteilt werden:

- Werbeunternehmen: Unternehmen, die auf Werbung spezialisiert sind und Daten für gezielte Werbung nutzen.
- Analytische Dienste: Dienste, die das Sammeln, Messen und Analysieren des Nutzerverhaltens in der App durchführen. Hierzu gehören Aktivitäten wie die Interaktionsdauer, Bindung zur App und personalisiertes Marketing.
- Information: Empfänger, die nützliche Informationen für den Nutzer bereitstellen, z. B. über Essverhalten, Schlafverhalten, sportliche Aktivitäten oder Krisenhilfen.
- Staatlich: Empfänger, die Informationen und Standards auf staatlicher Ebene bereitstellen.
- Dienstleister: Eine breite Kategorie, die verschiedene Dienste für Apps bereitstellt, darunter Cloud-Computing, Entwicklungstools, Mediaplayer, Kodierungsdienste, Datenbanken, GPS-Funktionen, kartografische Dienste und künstliche Intelligenz.
- Social Media: Soziale Netzwerke wie Facebook, Twitter oder Instagram.
- Potenziell bösartig: Hosts, die möglicherweise einen Betrug darstellen oder Viren verbreiten.
- Partner: Empfänger, die wahrscheinlich einen Vertrag mit der jeweiligen App abgeschlossen haben und in irgendeiner Weise kooperieren. Diese Kategorie kann aufgrund der Informationen aus der Datenschutzerklärung oder der Netzwerkkommunikation eingestuft werden, ist jedoch aufgrund der Art der vorliegenden Daten möglicherweise unscharf.

Die Einstufung der Empfänger in Kategorien erfolgte durch das Betrachten der Ergebnisse der statischen und dynamischen Analyse, eine Einsicht in die Datenschutzerklärung und eine darauf folgende *Whois*-Suche auf Google.

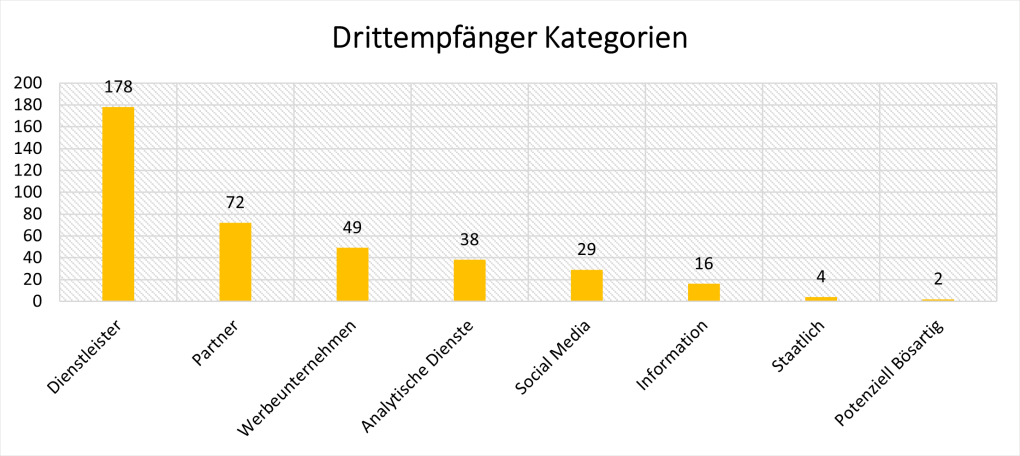


Abbildung 11: Anzahl an gefunden Empfänger der jeweiligen Kategorien

Es ist zu beachten, dass einem Empfänger auch mehreren Kategorien zugeordnet werden kann. Zum Beispiel können analytische Dienste hauptsächlich Daten verarbeiten, aber genau diese Daten könnten auch zu Werbezwecken gesammelt werden. Auch die Whois?-Suche auf Google kann zwar ermitteln, wofür ein Empfänger hauptsächlich bekannt ist, jedoch könnte die Verwendung dieses Empfängers im spezifischen Kontext der App eine andere sein.

Abbildung 11 zeigt das Kategorisieren der Empfänger in der Analyse. Auf der y-Achse wird die Häufigkeit des Auftretens eines Empfängers aus einer Kategorie pro App dargestellt. Dabei können zwei unterschiedliche Apps beide Google als Werbeunternehmen verwenden, und dies wird in dem Diagramm reflektiert. Empfänger aus den Kategorien werden nicht einzigartig im Diagramm abgebildet. Die Abbildung zeigt, dass Dienstleister und Partner den größten Teil der Empfänger ausmachen. Dienstleister bieten wichtige Tools und Funktionen für Apps, sodass der hohe Anteil zu erwarten war. Ebenfalls kollaborieren die meisten Apps mit vielen unterschiedlichen Partnern zu unterschiedlichen Zwecken. Dadurch, dass es sich um eine breite Kategorie handelt, besteht ein hoher Anteil der Empfänger aus dieser Kategorie.
Insgesamt werden Empfänger aus der Kategorie Werbeunternehmen 49 Mal verwendet. Die hohe Durchschnittszahl von $2,45$ Werbeunternehmen pro App verdeutlicht, dass Apps oft auf eine Vielzahl von Werbeunternehmen setzen. Die intensive Verwendung von Werbeunternehmen kann auch Auswirkungen auf die Benutzererfahrung haben, da eine erhöhte Anzahl möglicherweise ein höheres Maß an gesammelten personenbezogenen Daten suggeriert. Dieses Ergebnis betont die Notwendigkeit einer transparenten Kommunikation bezüglich der Verwendung von Werbeunternehmen in den Datenschutzerklärungen, um den Nutzern eine informierte Entscheidung zu ermöglichen.

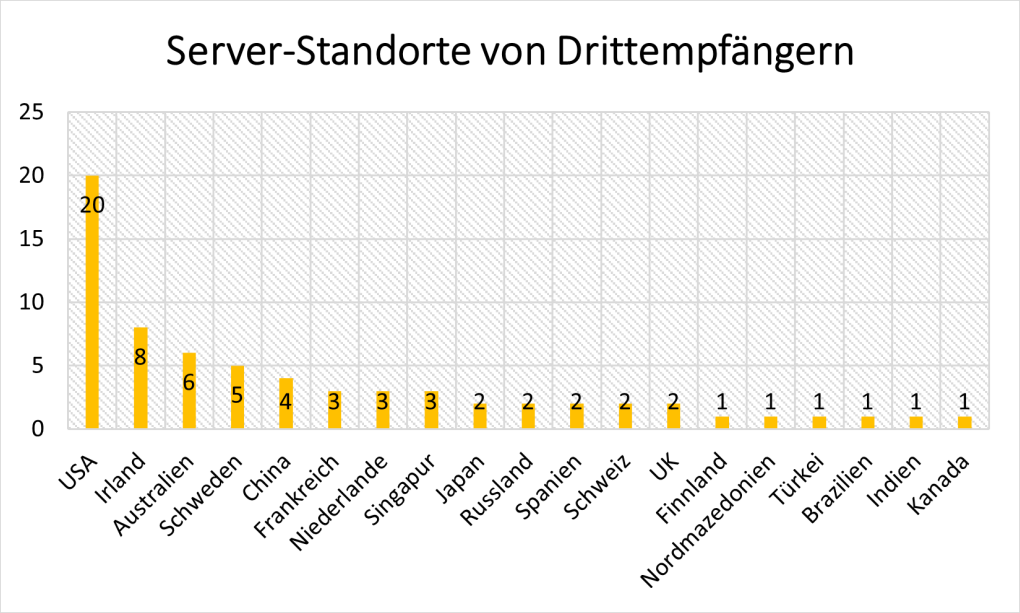


Abbildung 12: Server-Standorte von Empfängern

Hervorzuheben ist, dass in der App *Sweatcoin* (Entwickelt von: Sweatco Ltd) [3] eine Kommunikation mit zwei potenziell schädlichen Hosts festgestellt wurde. Diese Hosts, *dewrain* und *akisinn*, wurden von MobSF als mögliche Schadsoftware eingestuft. Bei der Durchführung einer Whois?-Suche konnten keine konkreten Ergebnisse für diese Hosts erzielt werden.

4.2. Drittlandsübermittlungen

In Abbildung 12 sind die Server-Standorte der Empfänger zu sehen, an die Daten gesendet wurden. Die Mehrheit der untersuchten Apps wurde in den USA entwickelt oder für Nutzer aus den USA konzipiert. Darüber hinaus kommuniziert jede App auf unterschiedliche Weise mit Google, sei es als Werbeunternehmen oder als analytischer Dienst. Die Standorte von Google sind zwar verteilt, haben aber in jedem Fall mindestens einen Sitz in den USA. Dies führt dazu, dass alle 20 untersuchten Apps ihre Daten in die USA senden. Darüber hinaus zeigt die Abbildung, dass 40% der Kommunikationen nach Irland gesendet werden. Irland ist aufgrund seines günstigen Klimas für die Kühlung von Servern und seiner niedrigen Unternehmenssteuersätze ein bevorzugter Hauptsitz für viele große Industrien in Europa [23, 18, 71].

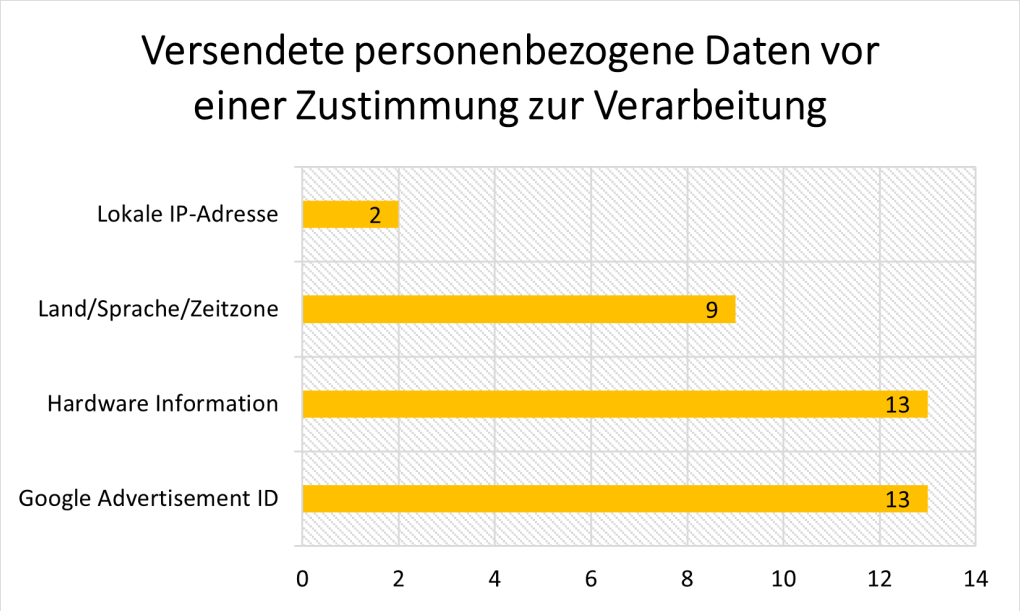


Abbildung 13: Daten, die vor einer Zustimmung zur Datenschutzerklärung versandt wurden

4.3. Personenbezogene Daten

Eine weitere Anforderung der Analyse ist das Untersuchen von personenbezogenen Daten, die verschickt werden. Vor allem das Versenden dieser vor einer Einwilligung zum Verarbeiten von personenbezogenen Daten ist relevant. Auch der Standort an denen die Daten versandt werden ist wichtig, da auch die Einwilligung zum Verschicken der Daten an Drittländer durch die Datenschutzerklärung notwendig ist. Dieser Teil der Analyse wurde mit der dynamischen Analyse durchgeführt. Die ermittelten Daten können daher kein vollständiges Ergebnis liefern; es werden nur die Daten dargestellt, die bei der Untersuchung gefunden oder entschlüsselt wurden (siehe Abbildung 13).

Wie im vorherigen Kapitel beschrieben, stellen nicht alle gesammelten Daten direkt personenbezogene Daten dar. Die DSGVO definiert personenbezogene Daten als Informationen, die zur Identifizierung einer Person genutzt werden können [45]. Abbildung 13 zeigt, dass in 13 der untersuchten Apps, die Google Advertising-ID ermittelt werden konnte. Diese ID ist eine eindeutige Kennung für Werbezwecke, die jedem Android-Gerät über Google Play zugeordnet wird. Diese ID lässt sich zurücksetzen, jedoch nicht deaktivieren [32]. Die Europäische Kommission klassifiziert diese Information als personenbezogenes Datum und bezeichnet sie als: „die Werbekennung Ihres Telefons;“ [45]. Noyb.eu reichte 2020 ebenfalls eine formelle DSGVO-Beschwerde gegen Google ein und argu-

mentierte, dass es sich bei der Google Advertising-ID um ein personenbezogenes Datum handelt [59].
In 13 Apps konnten Hardware Informationen, sowie in 9 Apps Länderdaten, Sprachen oder Zeitzonen ermittelt werden. Diese Daten stellen laut der DSGVO keine personenbezogenen Daten dar, sodass keine Einwilligung zur Datenschutzerklärung notwendig ist [45]. Zu beachten ist, dass Hardwareinformationen, Länderdaten und ähnliche Daten, die nach der DSGVO nicht als personenbezogene Daten gelten, dennoch Rückschlüsse auf das Nutzerverhalten und Präferenzen zulassen können. Obwohl für diese konkreten Daten keine ausdrückliche Zustimmung erforderlich ist, besteht dennoch die Möglichkeit, dass sie zur Erstellung eines umfassenden Nutzerprofils genutzt werden.
Zuletzt konnte die versandte lokale IP-Adresse gefunden werden. Die lokale IP-Adresse reicht noch nicht aus, um einen Bezug zur Person darzustellen. Diese Untersuchungen wurden alle in einem Heimnetzwerk durchgeführt. Wenn sich ein Nutzer jedoch außerhalb eines Heimnetzes bewegt, verwendet dieser in der Regel mobile Daten. Auch wenn mobile Daten verwendet werden, wird eine dynamische IP-Adresse vergeben, damit eine Kommunikation zwischen Servern und dem mobilen Gerät bestehen kann. Allerdings reicht diese dynamische IP-Adresse in der Regel nicht aus, um den genauen Standort einer Person zu ermitteln, da diese nicht geografisch angeordnet sind [58]. Alternativ könnten auch Triangulationen mit Mobilfunkmasten genutzt werden, um ein mobiles Gerät zu orten [63]. Ob diese Möglichkeiten der Ortung ohne Einverständnis genutzt werden, lässt sich nicht aus den Ergebnissen sagen.
In sämtlichen Fällen, in denen eine Übermittlung personenbezogener Daten festgestellt wurde, erfolgte diese an Server in den USA. Zudem wurden in zwei Fällen auch Übermittlungen an Kanada sowie Russland identifiziert. Somit wird deutlich, dass personenbezogen Daten, insbesondere die Google Advertising-ID, bereits vor einer expliziten Einwilligung ins Ausland übertragen werden.

4.4. Dark Patterns

Während der Nutzer durch eine Einwilligungserklärung über die Verwendung seiner personenbezogenen Daten informiert werden kann, besteht auch die Möglichkeit, dass er durch bewusst platzierte Designelemente getäuscht wird. Diese können den Nutzer dazu verleiten, der Verarbeitung zuzustimmen, ohne dass sich dieser über die Inhalte der gesammelten Daten bewusst ist. In diesem Abschnitt werden die Ergebnisse der Untersuchung von Dark Patterns vorgestellt. Wie im Methodik-Abschnitt beschrieben, wurden die Einwilligungserklärungen

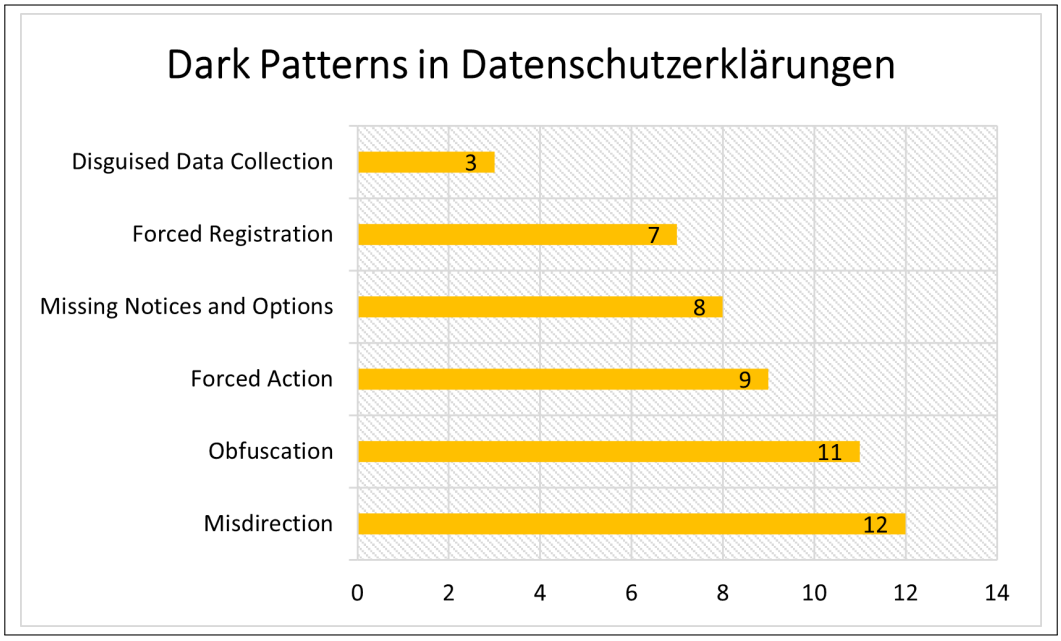
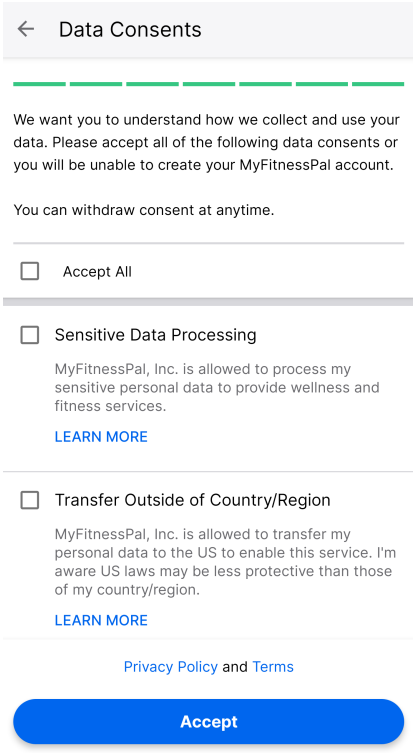


Abbildung 14: Gefundene Dark Patterns im Design von Einwilligungserklärungen zur Datenverarbeitung

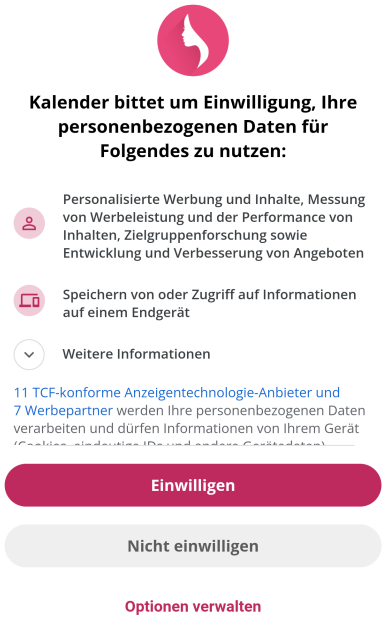
der Apps auf mögliche Dark Patterns untersucht. Die Apps *Blood Pressure* (Entwickelt von: K. Zsymon) [43] und *Ladytimer Ovulation Calendar* (Entwickelt von: Vipos Apps) [74] ermöglichten keine Zustimmung zur Datenschutzerklärung. Es wurde kein Fenster angezeigt, das den Nutzer über die Verarbeitung personenbezogener Daten aufklärt und eine Zustimmung ermöglicht. Die Verlinkung zur Datenschutzerklärung war nur über die Einstellungen der jeweiligen Apps erreichbar. Diese Apps wurden in diesem Teil der Auswertung nicht berücksichtigt. Die App *My Calendar- Period Tracker* (Entwickelt von: Simple Design Ltd.) [65] präsentierte zwar ein Fenster zur Zustimmung der Datenschutzerklärung, doch wurde dieses Fenster erst beim zweiten Start der App angezeigt. Dabei könnte es sich um einen Softwarefehler handeln. Trotzdem wurde bereits beim Erststart eine Verarbeitung personenbezogener Daten festgestellt. Diese App wurde dennoch auf Dark Patterns untersucht, und die Ergebnisse wurden beim zweiten Start der App aufgezeichnet. Insgesamt wurden 18 von 20 Apps auf das Vorhandensein von Dark Patterns analysiert.

Abbildung 14 stellt die Ergebnisse der Auswertung dar. Im Abschnitt Aktuelle Forschungen werden die unterschiedlichen Formen von Dark Patterns näher beschrieben. In diesem Abschnitt werden sie kurz angeschnitten und mit Fallbeispielen untermalt. In jeder untersuchten App konnte mindestens ein Fall von einem Dark Pattern festgestellt werden. Abbildung 15 stellt 4 Einwilligungen zu Datenschutzerklärungen von einer Auswahl von Apps dar, anhand derer die

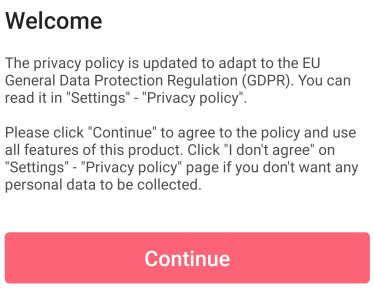
(a) Sweatcoin (Entwickelt von: Sweatco Ltd.) [3]



(b) My Fitness Pal (Entwickelt von: MyFitnessPal, Inc.) [1]



(c) My Calendar (Entwickelt von: SimpleInnovation) [2]

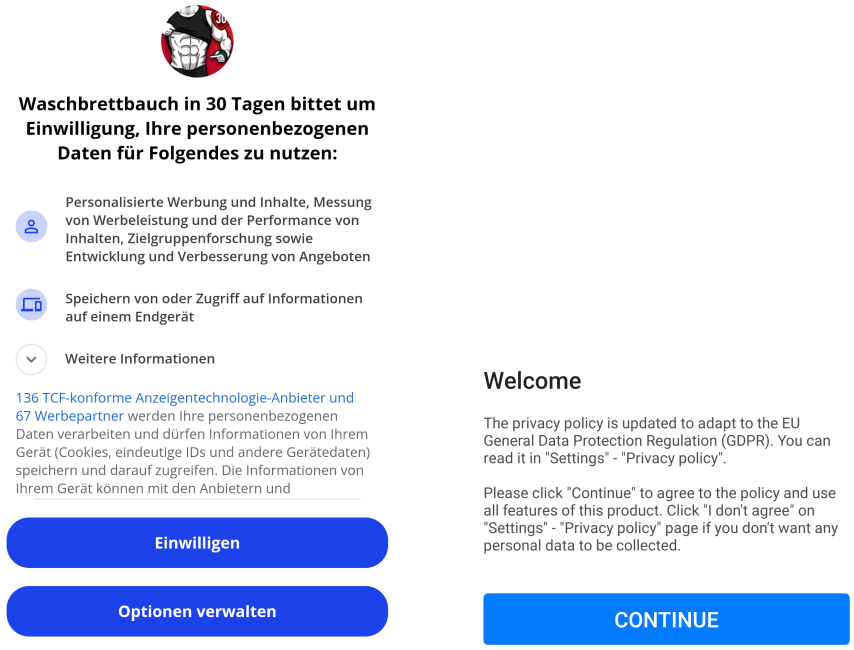


(d) My Calendar (Entwickelt von: Simple Design Ltd) [65]

Abbildung 15: Datenschutzeinwilligungen in untersuchten Apps

gefundenen Dark Patterns gezeigt werden.
Am häufigsten konnten Misdirections festgestellt werden. Im Falle von Misdirections wird der Nutzer durch Designelemente von wichtigen Informationen abgelenkt. Beispiel (a) stammt aus der *Sweatcoin App* (Entwickelt von: Sweatco Ltd.) [3]. Ersichtlich ist, dass für die verschiedenen Buttons unterschiedliche Farben gewählt wurden. Zum einen wird der *Registrieren mit Google*-Button mit einer weißen Hintergrundfarbe erhellt und in den Vordergrund gestellt. Der Nutzer soll möglichst diese Option auswählen. Zum Anderen befindet sich unter den oberen beiden Optionen ein Text, welcher die Datenschutzerklärung erläutern soll. Da, der Text einen grauen Font besitzt und keine Untermalung durch weitere Designelemente besitzt, fällt dieser nur wenig auf. Ähnlich werden Designelemente zur Manipulation des Nutzers in Beispiel (c) verwendet, in dem der Nutzer dazu bewegt wird den *Einwilligen*-Button zu bedienen. Eine andere Version einer Misdirection findet sich in Beispiel (b). Hier werden die gesammelten sensiblen Daten zwar aufgelistet, es fällt jedoch auf, dass dem Nutzer die Zustimmung *erleichtert* wird, indem eine *Accept All*-Checkbox angeboten wird. Dabei handelt es sich ebenfalls um eine Form von Misdirection, da der Nutzer dazu verleitet wird sich nicht über die gesammelten sensitiven Daten zu informieren, sondern diesen Schritt zu überspringen und direkt allen Optionen zuzustimmen.
Bei einer Obfuscation werden dem Nutzer gezielt wichtige Informationen nicht angezeigt. Im Falle von Beispiel (a) werden gar keine Informationen an der Nutzer gegeben. Dieser muss sich selbstständig die Datenschutzbestimmung durchlesen, indem er die Verlinkung zu der Datenschutzerklärung öffnet, um sich über den Umgang seiner personenbezogen Daten zu informieren. Ähnlich wie in (a) werden auch im Dialog von Beispiel (d) keine Informationen präsentiert. Zusätzlich ist es nicht möglich, die Datenschutzerklärung zu öffnen, sodass für den Nutzer keine Möglichkeit besteht sich zu informieren. Auch werden wichtige Informationen nur teilweise abgebildet. In Beispiel (b) und (c) werden zwar einige Informationen aufgelistet, jedoch muss der Nutzer über die jeweiligen *LEARN MORE*-Buttons in Beispiel (b) und über den dargestellten *Optionen verwalten*-Button in Beispiel (c) gehen, um sich umfassend zu informieren. Dennoch wird sowohl in Beispiel (b) als auch (c) kein Gesamtbild über alle gesammelten sensiblen Daten präsentiert.
Im Falle einer Forced Action wird dem Nutzer keine Möglichkeit zur Ablehnung gegeben. Ihm wird keine Wahl gelassen, als die App weiterzunutzen und eine bestimmte Aktion auszuführen. Beispiel (a), (b) und (d) geben dem Nutzer keine Möglichkeit, eine Sammlung personenbezogener Daten abzulehnen und dennoch weiterhin die App zu nutzen. In Beispiel (a) und (d) fehlen Design-

Elemente, die eine Ablehnung ermöglicht. Beispiel (b) besitzt zwar Checkboxen, welche vom Nutzer unausgefüllt gelassen werden können, eine weitere Verwendung der App ist dennoch nicht möglich. Beispiel (c) dagegen liefert auch eine Möglichkeit die Sammlung sensibler Daten abzulehnen und dennoch mit der Benutzung der App fortzufahren. Zu erwähnen ist ebenfalls, dass einige Apps wie z. B. *MyFitnessPal* (Entwickelt von: MyFitnessPal, Inc) [1] zwar bei der Erstellung des Accounts und dem Einwilligen zur Datenschutzerklärung die Möglichkeit nennen, dass ein Widerruf jener Rechte möglich ist, jedoch wird nicht informiert, dass dabei auch der Account gelöscht werden muss. Der Nutzer hat zu diesem Zeitpunkt aber eventuell schon eine Bindung zu der App aufgebaut, sodass das Löschen des Accounts für den Nutzer erschwert wird.
Weiterhin geben 8 von den 18 untersuchten Apps keine Bescheide über eine Einwilligung, stellen keine Checkboxen für die jeweiligen Gruppen von personenbezogenen Daten zur Verfügung oder bieten dem Nutzer keine Optionen zur Verwaltung der eingezogenen Rechte. Dies stellt eine Form der Missing Consent Notices and Options dar. Mit Ausnahme von Beispiel (b) bieten keine der vorgestellten Apps dem Nutzer die Möglichkeit, einzelnen Gruppen von Informationen wie z.B. Gesundheitsdaten, Fitnessdaten oder Lokalisierungsdaten zuzustimmen. Es wird lediglich nach einer allgemeinen Einwilligung aller gefragt, ohne die Möglichkeit zur personenbezogenen Anpassung zu geben.
Im Falle einer Forced Registration wird der Nutzer dazu gezwungen sich zu Registrieren und einen Account zu erstellen. Dieses Dark Pattern findet sich häufig zusammen mit einem Forced Action, dennoch sind diese zu Unterscheiden. Während in Beispiel (a), (b) und (d) ein Fall von einer Forced Action zu finden ist, muss im Beispiel von (d) kein Account zur Nutzung der App erstellt werden. Die App ist dabei auch ohne Account funktionstüchtig, sofern eine Zustimmung der Datenschutzerklärung vorliegt. 7 Apps erforderten jedoch eine Accounterstellung, welche dem App-Entwickler die Möglichkeit gibt Daten über den Nutzer zu speichern.
Zuletzt wurde der Fall von Disguised Data Collection betrachtet. Hierbei werden personenbezoge Daten des Nutzers ohne direkte Zustimmung der Datenschutzerklärung gesammelt. Beispiel (a) erwähnt zwar, dass durch die Erstellung eines Accounts der Datenschutzerklärung zugestimmt wird, aber in Kombination mit weiteren Dark Patterns, wie der Misdirection, könnte dem Nutzer möglicherweise nicht vollständig bewusst sein, dass er bereits in diesem Schritt der App-Verwendung der Datenschutzerklärung zustimmt.
Weiterhin wurde festgestellt, dass sich das Design von Einverständniserklärungen selbst in Apps von gleichen Unternehmen unterscheidet. Es wurden insgesamt drei verschiedene Apps von der Leap Fitness Group analysiert. Während



(a) 30 days sixpack (Entwickelt von: Leap Fitness Group) [49]

(b) Home Workout - No Equipment (Entwickler: Leap Fitness Group) [48]

Abbildung 16: Datenschutzeinwilligungen in Apps vom Entwickler Leap Fitness Grup

sich die Einverständniserklärung der Apps *30 days sixpack* (Entwickelt von: Leap Fitness Group) [49] und *Lose Weight for App for Men* (Entwickelt von: Leap Fitness Group) [50] nicht unterschieden und dem Nutzer einige Informationen über die Verwendung seiner Daten präsentierte, erschien der Dialog zur Bestätigung bei der App *Home Workout - No Equipment* (Entwickelt von: Leap Fitness Group) [48] veraltet und bot keinerlei Information für den Nutzer (siehe Abbildung 16).

In den Apps *Home Workout - No Equipment* [48] (siehe Abbildung 16 - (b) und *My Calendar* [65] (siehe Abbildung 15 - (d)) wurde festgestellt, dass dem Nutzer zwar ein Interfaceelement angezeigt wird, indem er einer Datenschutzerklärung zustimmen kann, dem Nutzer wird aber keine Möglichkeit gegeben die Datenschutzerklärung zu betrachten (Beispielsweise über einen Link). Der Nutzer muss der Datenschutzerklärung in diesen Apps zustimmen bevor er die Möglichkeit hat diese zu lesen [33, 19, 36, 34, 13].

Zusammenfassend lässt sich feststellen, dass Dark Patterns wie Misdirections und Obfuscations weit verbreitet sind und scheinbar einen festen Bestandteil im Design von Benutzeroberflächen darstellen. Während das Navigieren des Nut-

zers durch eine App mit farblichen Untermalungen, sowie angepassten Größen von Designelementen sinn- und vorteilhaft für den Nutzer erscheint, muss die Wiedergabe von wichtigen Informationen erhöht werden.

4.5. Widerruf und Sprache

Ein weiterer Aspekt der Analyse umfasste die Sprachen, in denen die Datenschutzerklärungen angezeigt wurden, sowie die Möglichkeit für den Nutzer, die Einwilligung zur Erklärung zu widerrufen. Von den 20 untersuchten Apps boten 2 keine Option, die Datenschutzerklärung anzuzeigen, sodass nur 18 Apps in Betracht gezogen wurden. Bei der Betrachtung der Möglichkeiten zum Widerruf der eingeforderten Rechte stellte sich heraus, dass 7 der Apps keine solche Option anboten. Die fehlende Möglichkeit, die Datenschutzerklärung anzuzeigen, sowie das Fehlen von Optionen zum Widerruf eingeforderter Rechte in einigen Apps könnten Auswirkungen auf die Transparenz und die Selbstbestimmung der Nutzer haben. Ein mangelnder Zugriff auf die Datenschutzerklärung könnte die Fähigkeit der Benutzer beeinträchtigen, sich umfassend über die Verarbeitung ihrer personenbezogenen Daten zu informieren. Gleichzeitig könnte es für Nutzer schwierig sein, ihre Einwilligung zur Datenverarbeitung zurückzuziehen und die Kontrolle über ihre personenbezogenen Daten zu behalten, wenn es keine klaren Optionen zum Widerruf der Rechte gibt.

Im nächsten Schritt wurde die Sprache der angezeigten Datenschutzerklärungen genauer untersucht. Von den verbleibenden 18 Apps waren lediglich 2 ausschließlich auf Englisch verfügbar, weshalb sie bei dieser Auswertung ausgeschlossen wurden. Alle untersuchten 16 Apps waren in Deutsch erhältlich, und sämtliche Bildschirme während der Benutzung wurden in dieser Sprache angezeigt. Interessanterweise waren die Datenschutzerklärungen in 10 der Apps ausschließlich auf Englisch verfasst. Das bedeutet, dass ein deutscher Nutzer ohne Englischkenntnisse in 63% der untersuchten Apps keine Möglichkeit gehabt hätte, sich über den Umgang mit seinen personenbezogenen Daten zu informieren, abgesehen vom ursprünglichen Einwilligungsdialog. Es besteht die Möglichkeit, dass einige Nutzer aufgrund der Sprachbarriere möglicherweise nicht vollständig verstehen, wie ihre personenbezogenen Daten verwendet werden. Dies könnte die Transparenz und das Vertrauen in Bezug auf den Datenschutz beeinträchtigen.

4.6. Datenschutzerklärung

Für die Analyse der Datenschutzerklärungen wurde mittels der statischen und dynamischen Analyse ein Abgleich mit den Angaben aus den Datenschutzerklärungen durchgeführt.
Durch die statische Analyse konnte die Drittlandübermittlung mit den in den jeweiligen Datenschutzerklärungen gemachten Angaben verglichen werden. In zwei Fällen fehlten in der Datenschutzerklärung jegliche Hinweise auf eine Drittlandübermittlung, obwohl diese in der statischen Analyse nachweisbar war. Insgesamt wurden in 55% der untersuchten Apps keine konkreten Länder benannt, sondern lediglich allgemeine Kategorisierungen verwendet. Dies geschah beispielsweise durch die Angabe der *Europäischen Union* oder die Verarbeitung außerhalb der *operating offices*. Zudem wurden häufig Kombinationen aus Drittländern und Kategorien verwendet, wie etwa die wiederholte Nennung der USA in Verbindung mit der Europäischen Union. Dadurch wird für den Nutzer die Nachverfolgung des Datenversands eingeschränkt. Nach der Katalogisierung der gefundenen Länder durch die statische Analyse und den Vergleich mit den definierten Kategorien und namentlich genannten Ländern wurde dennoch nur eine Übereinstimmung von 75% ermittelt. In fünf der untersuchten Apps hat der Nutzer damit keine Möglichkeit, sich über die Drittlandübermittlung zu informieren. Es ist wichtig zu betonen, dass die fehlenden oder ungenauen Angaben zu Drittlandübermittlungen in den Datenschutzerklärungen die Transparenz für die Nutzer erheblich einschränken. Die ungenauen oder ausweichenden Formulierungen können dazu führen, dass Nutzer nicht vollständig darüber informiert werden, wohin ihre personenbezogenen Daten tatsächlich übermittelt werden.

In Analogie dazu wurden auch die Empfänger der übermittelten Daten katalogisiert. Obwohl jede Datenschutzerklärung Namen oder Kategorien potenzieller Empfänger enthielt, ergab sich dennoch eine Übereinstimmung von insgesamt 85% zwischen den Ergebnissen der statischen Analyse und den Angaben in den entsprechenden Datenschutzerklärungen.

Die Datenschutzerklärungen der Apps neigten dazu, Empfänger hauptsächlich kategorisiert anzugeben, wobei 60% der Apps hauptsächlich Kategorien statt namentlich genannter Empfänger verwendeten. Diese Kategorisierung erfolgte häufig mithilfe weit gefasster Begriffe wie *Service-Partner*, *Analytics-Partner* oder *Advertisement-Partner*. Interessanterweise umfassten 55% dieser Kategorien

mehr als zehn potenzielle Empfänger. Eine solche Anzahl von möglichen Empfängern innerhalb einer einzelnen Kategorie wirft die Frage auf, ob diese Kategorie möglicherweise zu weit gefasst ist. Im Gegensatz dazu konnten in 40% der Datenschutzerklärungen nur zwei oder weniger Empfänger in einer Kategorie ermittelt werden. Diese Kategorien waren oft sehr breit definiert, enthielten jedoch letztendlich nur wenige tatsächliche Empfänger, was die Nennung der einzelnen Empfänger in der Datenschutzerklärung sinnvoll erscheinen lässt. Darüber hinaus konnte in 55% der Apps festgestellt werden, dass mehr Kategorien aufgeführt wurden, als tatsächlich identifizierte Empfänger vorhanden waren. In diesen Fällen wurden Kategorien für Empfänger aufgeführt, die möglicherweise nicht existieren, was die Transparenz der Datenschutzerklärungen beeinträchtigen könnte.
Anschließend wurde überprüft, ob große und häufig verwendete Unternehmen im Zusammenhang mit Datenweitergabe, insbesondere im Bereich Werbenetzwerke oder Trackingdienste wie *Google Analytics*, namentlich genannt wurden. Dabei wurden solche Unternehmen nur in 75% der untersuchten Fälle ausdrücklich benannt [44]. Dies wirft die Frage auf, ob es sinnvoll ist, weit verbreitete Werbeunternehmen und Trackingdienste in allgemeinere Kategorien zu erfassen, anstatt sie explizit namentlich zu benennen, um die Transparenz für den Nutzer zu erhöhen [4, 30, 46, 10, 52, 7, 64, 12].

Schließlich wurden auch die angeforderten personenbezogenen Daten betrachtet. Obwohl sämtliche in den Datenschutzerklärungen aufgeführten personenbezogene Daten katalogisiert werden konnten, gestaltete sich der Abgleich mit den entsprechenden Apps als herausfordernd. Die Permissions, die mithilfe der statischen Analyse und MobSF ermittelt wurden, enthielten nur wenig Informationen über personenbezogene Daten. Bei den meisten Apps wurde lediglich festgestellt, dass sie die Berechtigung haben, den Nutzer nach Standortinformationen zu fragen. Diese Feststellung konnte jedoch in der dynamischen Analyse nicht bestätigt werden. Des Weiteren decken Permissions, die im Androidmanifest.xml definiert sind, keine personenbezogenen Daten ab. Daher konnte in der statischen Analyse keine potenzielle Übertragung von personenbezogenen Daten entdeckt werden.

Weiterhin wurde auch untersucht, ob ein Datenfluss von personenbezogene Daten während des Betriebs der App stattfindet. In keiner der Apps konnte jedoch ein solcher Datenfluss von personenbezogene Daten ermittelt werden. Dies könnte darauf zurückzuführen sein, dass die Daten kodiert oder verschlüsselt sind

und somit nicht über die angewandten Analysemethoden umgangen werden konnten. Insgesamt lässt sich daher keine klare Aussage über die Konformität der in der Datenschutzerklärung angeforderten personenbezogene Daten im Vergleich zur tatsächlichen Ausführung der App treffen.

Zusammenfassend konnte gezeigt werden, dass personenbezogene Daten, insbesondere die Advertising-ID, bereits vor der Einwilligung in 13 der untersuchten Apps identifiziert wurden. Dies wirft Fragen hinsichtlich der Definition und des Schutzes personenbezogener Daten auf. Des Weiteren wurden die Einwilligungserklärungen auf Dark Patterns untersucht. Dabei wurde gezeigt, dass in jeder untersuchten App Dark Patterns in den Einwilligungserklärungen vorhanden waren, was auf eine weit verbreitete Praxis hindeutet. Diese Dark Patterns, vornehmlich Formen von Forced Action und Obfuscation, zeigen, dass Nutzer oft dazu gedrängt werden, ohne ausreichende Information zuzustimmen. Hinsichtlich der Übereinstimmung von Datenschutzerklärungen mit der tatsächlichen App-Ausführung ergab sich eine Trefferquote von 75% für Drittländer und 85% für Empfänger. Dabei wurde darauf hingewiesen, dass die hohe Übereinstimmung auf der Kategorisierung von Empfängern und Drittländern beruht. Schließlich konnte keine aussagekräftige Meinung zur Übereinstimmung von gesammelten personenbezogenen Daten und den Angaben in den Datenschutzerklärungen abgegeben werden, da weder in der statischen noch in der dynamischen Analyse ausreichend Nachweise über personenbezogene Daten gefunden werden konnten.

5. Diskussion

In diesem Kapitel werden die erzielten Ergebnisse in den Kontext der gestellten Forschungsfragen gesetzt. Es erfolgt eine Analyse, Interpretation und kritische Auseinandersetzung mit den Ergebnissen. Weiterhin werden die Ergebnisse mit bestehenden Forschungsergebnissen aus der Literatur verglichen. Daraufhin werden die Limitationen und Herausforderungen, die mit der Studie entstanden sind, besprochen. Mit der Diskussion soll ein tieferer Einblick in die Thematik gewährt werden.

5.1. Ergebnisse

Die Ergebnisse der dynamischen Analyse konnten zeigen, wie sich Apps vor einer Zustimmung der Datenschutzerklärungen verhielten, insbesondere wurden dabei die Übermittlung von personenbezogenen Daten an Dritte untersucht. Eine besonders hervorstechende personenbezogene Information war dabei die Google Advertising-ID. Ähnliche Befunde wurden auch von Claesson und Bjørstad [15] festgestellt, die weitere Übertragungen von personenbezogenen Daten wie GPS-Position, Geschlecht und Alter an Dritte ermittelten. Grundy et al. [35] fanden vergleichbare Ergebnisse im medizinischen Bereich, wobei personenbezogene Daten wie Geburtsdatum und Geschlecht übertragen wurden. Zwar konnten in dieser Arbeit die Zeitzone, Hardwareinformationen und die Lokale IP-Adresse ermittelt werden, aber neben der Advertising-ID, die direkt auf einen Nutzer weist, welches eine Voraussetzung für ein personenbezogenes Datum laut der DSGVO [45] ist, konnten keine weitere Übermittlung von personenbezogenen Daten gefunden werden. Es können verschiedene Gründe dafür zugrunde liegen. Möglicherweise werden die personenbezogenen Daten zunächst an die Hauptserver des App-Betreibers gesendet und erst in einem weiteren Schritt an Dritte weitergegeben, was durch den Aufbau der Studie nicht ersichtlich ist. Weiterhin können die Daten zusätzlich verschlüsselt oder kodiert sein, so waren die meisten Übermittlungen an Google kodiert und nicht einsehbar. Dennoch gibt das Auffinden der Google Advertising-ID in 65 % der untersuchten Apps noch vor einer Einwilligung den Hinweis, dass klarer definiert werden muss, was genau ein personenbezogenes Datum ist. Denn laut DSGVO [45] sollte es sich dabei eigentlich um genau das handeln, in der Praxis fehlt jedoch eine einheitliche Umsetzung.

Die statische Analyse wurde verwendet, um Drittländer und Datenempfänger zu identifizieren und mit den in den Datenschutzerklärungen genannten Drittländern und Empfängern zu vergleichen. In Bezug auf die Drittländer, fällt auf, dass 65% der Datenschutzerklärungen Länder größtenteils kategorisiert haben, anstatt sie namentlich zu benennen. Dennoch zeigte sich, dass lediglich eine Übereinstimmung von 75% mit der technischen Analyse besteht. Das bedeutet, dass in einem Viertel der Fälle die Nutzer nicht vollständig darüber informiert wurden, wohin ihre Daten übermittelt werden. Zudem stellt es für Nutzer eine Herausforderung dar, Informationen über den Datenbrauch in Apps zu erhalten, die scheinbar eine Übereinstimmung mit der technischen Analyse aufweisen. Die Unklarheit, welche durch das Kategorisieren von Drittländern verursacht wird, erschwert es für den Nutzer festzustellen, wohin seine Daten tatsächlich gesendet werden könnten. Die Zulässigkeit des Kategorisierens von Drittländern wurde in der erforschten Literatur diskutiert, wobei unterschiedliche Ergebnisse zu finden sind [12, 10]. Dennoch unterstreicht das Ergebnis der Analyse die Relevanz einer klareren Definition bei der Offenlegung von Drittländern in Datenschutzerklärungen. Die Ergebnisse legen nahe, dass eine präzisere Angabe dieser Länder, statt allgemeiner Kategorien, zur Verbesserung der Transparenz und Verständlichkeit für die Nutzer beitragen könnte. Durch einheitlich definierte Standards oder Richtlinien in Bezug des Umgangs mit Drittländern könnten diese Ziele erreicht werden. Solche Empfehlungen könnten dazu beitragen, die Datenschutzpraktiken von Fitness- und Gesundheits-Apps zu verbessern und die Nutzer in die Lage zu versetzen, fundierte Entscheidungen über den Umgang mit ihren Daten zu treffen.

Zu ähnlichen Ergebnissen und Diskussionen konnte auch bei der Ermittlung von Empfängern geschlossen werden. Dabei wurden hier sogar eine Übereinstimmung von 85% mit der technischen Analyse festgestellt. Dennoch bleibt die Kategorisierung ein umstrittenes Thema, das verschiedene Standpunkte hervorruft, wie in den Arbeiten von Kühling und Buchner [46], Simitis et al. [64] und Gola und Heckmann [30] ausführlich diskutiert wurden. Die vorgestellten Ergebnisse führen zurück auf die erste Forschungsfrage: *Inwiefern entsprechen die in den Datenschutzerklärungen aufgeführten Empfängern von Daten, Drittlandempfänger und die Verwendung personenbezogener Daten den tatsächlichen Ergebnissen der technischen Analyse?*

Die Resultate zeigen, dass lediglich ein eingeschränktes Sichtfeld in Bezug auf personenbezogener Daten gesammelt werden konnte. Dennoch konnten mögliche Datenschutzverletzungen mit dem Aufdecken der Google Advertising-ID

festgestellt werden. Weiterhin ließen sich klare Ergebnisse mit der Übereinstimmung von Empfängern und Drittlandempfänger erzielen, die eine Übereinstimmung von 75 % bzw. 85 % aufwiesen.

Im gleichen Zug kann auch folgende Forschungsfrage beantwortet werden: *In welchem Maße informieren Datenschutzerklärungen von Fitness- und Gesundheits-Apps über Datenempfänger, Drittlandübermittlungen und die Verwendung personenbezogener Daten?*

Die Ergebnisse verdeutlichen, dass der Großteil der Datenschutzerklärungen eine umfassende Abdeckung aller möglichen Empfänger und Drittlandübermittlungen durch eine Kategorisierung vornimmt. Personenbezogene Daten wurden jedoch in den meisten Erklärungen einzeln aufgeführt. Trotz dieser Ergebnisse bleibt eine rechtliche Unklarheit bezüglich der Angabe von Kategorien von Drittländern und Empfängern, die einer detaillierten juristischen Untersuchung bedarf.

Die letzte Forschungsfrage lautete: *Wie weit verbreitet sind Dark Patterns in den Einwilligungserklärungen von Fitness- und Gesundheits-Apps?*

In dieser Untersuchung konnte gezeigt werden, dass in jeder App die eine Einwilligungserklärung besaß mindestens eine Form von Dark Pattern gefunden werden konnte. Diese Ergebnisse bestätigt sich in der untersuchten Literatur. So wurden auch in Geronimo et al. [29] mindestens eine Form von Dark Pattern in jeder App gefunden. Insgesamt lässt sich feststellen, dass eine weite Verbreitung von Dark Patterns in Einwilligungserklärungen stattfindet. Insbesondere Formen von Forced Action und Obfuscations waren in nahezu allen Apps präsent. Daraus lässt sich ableiten, dass in den meisten der untersuchten Apps die Nutzer entweder zur Einwilligung gedrängt werden, um die App weiter nutzen zu können, oder dass ihnen unzureichende Informationen über die gesammelten Daten zur Verfügung gestellt werden. Diese Ergebnisse werfen nicht nur Fragen zur Transparenz auf, sondern könnten auch erhebliche Auswirkungen auf die Privatsphäre der Nutzer haben, da sie möglicherweise nicht in der Lage sind, informierte Entscheidungen über die Nutzung ihrer Daten zu treffen. Angesichts dieser Entwicklungen sind rechtliche Überlegungen als auch Überlegungen im Kontext der Human-Computer Interaction notwendig, um den Datenschutz und das Vertrauen der Nutzer im App-Bereich zu stärken.

5.2. Einschränkungen und Herausforderungen

Während der Untersuchung und des Versuchsaufbaus traten einige Einschränkungen und Herausforderungen auf, die berücksichtigt werden mussten.
Für die statische Analyse konnte zwar MobSF [5] verwendet werden, es gab jedoch aber kaum alternative Tools die benutzt werden konnten. Es wäre zwar möglich gewesen, den Decompiler JADX einzeln zu verwenden, jedoch ist der von JADX produzierte Code sehr kryptisch, sodass eine Wiederauffindung von nützlichen Informationen wie Libraries oder mögliche Empfänger zu umständlich für diese Arbeit war, sodass diese Option letztlich nicht weiter verfolgt wurde.
Für die Durchführung der dynamischen Analyse war es erforderlich, das Handy zu rooten. Das Rooten des Geräts birgt Risiken, da Fehler bei der Installation der Rooting-Software dazu führen kann, dass das Gerät nicht mehr funktionsfähig ist. Daher musste der Rooting-Prozess äußerst vorsichtig durchgeführt werden.
Für die Durchführung der Analyse wurde ein physisches Mobilgerät verwendet. Es bestand ebenfalls die Möglichkeit, das Gerät über virtuelle Maschinen zu emulieren, wie zum Beispiel den Android Studio Simulator [67] oder Genymotion [28]. Beide Emulatoren wurden zu Beginn des Studienaufbaus in Betracht gezogen. Es stellte sich jedoch heraus, dass die Emulatoren für die Untersuchungen anfällig für Fehler waren, und eine kontinuierliche Ausführung der Apps auf dem verwendeten PC nicht zuverlässig gewährleistet werden konnte. Zudem war das Ziel eine möglichst realistische Ausführung der Apps zu erzielen, weshalb die Nutzung eines physischen Mobilgeräts bevorzugt wurde. MobSF bat ebenfalls die Option einer dynamischen Analyse sowohl mit emulierten, als auch mit physischen Geräten an. Diese Möglichkeit wurde verworfen, da auch hier keine zuverlässige Ausführung der Apps gewährleistet werden konnte. Einige Apps ließen sich gar nicht ausführen, während andere fehleranfällig waren und häufig abstürzten.
Eine zusätzliche Einschränkung bestand darin, dass einige Apps die Fähigkeit besaßen, gerootete und emulierte Geräte zu erkennen. In Abbildung 17 werden übermittelte Hardwareinformationen an einen Facebook-Server in der App *My Calendar* (Entwickt von: SimpleInnovation) [2] dargestellt. Der markierte Bereich zeigt den Eintrag *ROOTED:1*, was darauf hinweist, dass die App möglicherweise erkennt, dass es sich um ein gerootetes Handy handelt. Für diese Situationen wurde ein Magisk-Modul installiert, das den Status des gerooteten Handys verbergen sollte. Trotzdem bestand die Möglichkeit, dass einige Apps in der Lage waren, den gerooteten Status des Handys aufzudecken. Dies könnte dazu führen, dass die App ihr Verhalten anpasst. Es besteht die Möglichkeit,

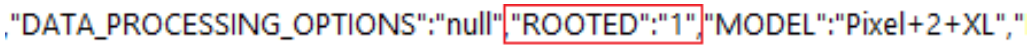


Abbildung 17: Mit MobSF [5] ermittelte Hardware Informationen an Facebook-Server. Rot umrandet: *Rooted:1*-Tag

dass weniger oder andere Daten an Dritte übermittelt werden. Ebenso könnte die Nutzung der App selbst anders verlaufen, wodurch eine vollständig realistische Ausführung der App nicht garantiert werden kann.

Wie schon im vorherigen Abschnitt angeschnitten, war auch die Ermittlung von personenbezogenen Daten, abgesehen von der Google Advertising-ID eine Herausforderung. Es konnten in Einzelfällen Übermittlungen von Angaben wie das Gewicht oder Geburtsdaten an den Host-Server des App-Betreibers gefunden werden, jedoch keine Übermittlung an Dritte. Ein Grund dafür kann die häufige Verwendung von kodierten Daten sein. Vor allem Datenübermittlung an die Server von Google waren kodiert und konnten auch nicht mit den gängigen Dekodierungsverfahren aufgedeckt werden. Dadurch kann keine klare Aussage über den Umgang von personenbezogenen Daten hinsichtlich der technischen Analyse gegeben werden. Weiterhin könnten die Daten zunächst kodiert oder verschlüsselt an den Host-Server des App-Betreibers versendet worden sein, bevor sie dann an Dritte weitergegeben wurden. Mit dem Versuchsaufbau waren solche Vorgehen nicht einsehbar.

Eine zusätzliche Herausforderung ergab sich beim Versuchsaufbau. Obwohl alle ausgehenden Netzwerkaktivitäten des Handys in Burp Suite angezeigt wurden, lag der Schwerpunkt auf der Beobachtung der Aktivitäten der untersuchten App. Dabei wurden auch einige Daten von den Hintergrundsystemen des Android-Betriebssystems übermittelt, die sich nicht direkt herausfiltern ließen und gemeinsam mit den Aktivitäten der untersuchten App in Burp Suite angezeigt wurden. Um den Einfluss dieser Hintergrundaktivitäten zu minimieren, wurden die Netzwerkaktivitäten des Handys ohne laufende App überwacht und die auftretenden Aktivitäten wurden entsprechend markiert. In der anschließenden Analyse der Apps wurden wiederkehrende Netzwerkdaten, die vom Android-System ausgingen, ignoriert. Trotz der aufgewandten Sorgfalt, um dies zu verhindern, kann nicht garantiert werden, dass keine Ergebnisse durch diese Hintergrundaktivitäten verfälscht wurden.

6. Ausblick

Die erzielten Ergebnisse bieten nicht nur einen Beitrag zu aktuellen Diskussion über Datenschutz in Fitness- und Gesundheits-Apps, sondern auch eine Grundlage für weiterführende Untersuchungen und Verbesserungen. Dieses Kapitel reflektiert noch einmal über die gesammelten Ergebnisse und wirft einen Blick auf potenzielle praktische Anwendungen, die dazu beitragen können, die Datenschutzstandards in Apps weiter zu stärken.

Im Bereich der Informationssicherheit wurde in der Arbeit eine Grundlage für die Analyse von Apps geschaffen. Sie verbindet statische und dynamische Analysen und ihre damit verbundenen Stärken und Schwächen. Es konnten mit der statischen Analyse Informationen wie Server-Standorte und Empfänger gesammelt werden und damit verdeutlichen wie mit den Daten von Nutzern umgegangen wird.
In der dynamischen Analyse wurden Apps zur Laufzeit untersucht. Vor allem der Datenverkehr vor einer Zustimmung der Datenschutzerklärung spielte eine entscheidende Rolle. Die Ergebnisse der Untersuchung verdeutlichen, dass die Google Advertising-ID in praktisch allen Apps bereits vor einer Zustimmung versendet wurde. Dies bietet eine relevante Grundlage für die Diskussion darüber, ab welchem Zeitpunkt Daten als personenbezogen betrachtet werden können. Diese Erkenntnisse erfordern weiterführende Untersuchungen sowohl im Bereich der Informatik, als auch im rechtlichen Kontext.
Im Kontext des Human-Computer Interaction wurden Einwilligungserklärungen auf Dark Patterns untersucht. Es konnte gezeigt werden, dass Dark Patterns in allen untersuchten Apps vorhanden waren. Darüber hinaus zeigen diese auf, dass Nutzer nicht ausreichend über die Verwendung ihrer Daten informiert und dazu verleitet werden, sich nicht ausreichend mit der Datenverarbeitung auseinanderzusetzen.
Zuletzt wurden Datenschutzerklärungen untersucht und Drittlandübermittlungen, Drittempfänger sowie personenbezogene Daten katalogisiert. Die Ergebnisse verdeutlichen, dass App-Betreiber in ihren Datenschutzerklärungen häufig auf Kategorien zurückgreifen, um eine möglichst große Bandbreite an Drittempfängern und Drittländern zu erfassen. Die Untersuchung konnte damit verdeutlichen, dass diese Art der Kategorisierung dem Nutzer keine Möglichkeit gibt sich näher mit dem Gebrauch seiner Daten zu beschäftigen und somit eine intransparente Informationsquelle darstellt.

Mit dieser Arbeit konnten in begrenztem Umfang die Verhaltensweisen von App-Betreibern sowohl innerhalb der App als auch in der Datenschutzerklärung beleuchtet werden. Zukünftige Arbeiten könnten andere Tools verwenden, um genauere Ergebnisse zu erzielen. Abschließend wäre es auch denkbar gewesen, das Tool Frida [27] einzusetzen. Frida ist ein Code-Injektionstool, mit dem zur Laufzeit einer App Code eingefügt werden kann, um die Funktionalität der untersuchten App zu beeinflussen. Durch den Einsatz von Frida hätte es möglicherweise ermöglicht werden können, den gerooteten Status weiter zu verschleiern oder zu verhindern, dass Daten kodiert versendet werden, was die Möglichkeit zur Einsicht in personenbezogene Daten verbessert haben könnte. Eine Schwierigkeit hier wäre gewesen, dass der Einsatz von Frida Auswirkungen auf die Funktionalität der App haben könnte und die Ergebnisse der Analyse beeinflussen würde.

In dieser Arbeit wurden 20 Apps untersucht, was eine solide Grundlage darstellt. Dennoch könnte die Anzahl der untersuchten Apps möglicherweise nicht ausreichen, um eine umfassende Meinung zu bilden. Weiterhin wurde sich in dieser Arbeit auf Fitness- und Gesundheits-Apps spezialisiert. In diesen Apps ist der Umgang mit personenbezogenen Daten besonders relevant. In zukünftigen Arbeiten könnten weitere App-Genres betrachtet werden, da diese ein noch breiteres Spektrum an Nutzern haben.
Im Bereich der Dark Patterns könnten zusätzlich Nutzerstudien durchgeführt werden. Diese Studien könnten das Verhalten von Nutzern bei der Konfrontation mit Dark Patterns genauer zeigen und relevante Ergebnisse liefern. Darüber hinaus könnten Umfragen oder Interviews durchgeführt werden, um die Wahrnehmung von Datenschutz und Einwilligungserklärungen besser zu verstehen. Dies würde zusätzliche Einsichten darüber ermöglichen, wie Nutzer mit Datenschutzrichtlinien interagieren und inwieweit sie in der Lage sind, informierte Entscheidungen zu treffen.
Die Analyse ergab, dass in einigen Apps, insbesondere solchen von kleinen Entwicklerstudios, wenig Wert auf die informative Gestaltung von Einwilligungserklärungen gelegt wurde. Hieraus ergibt sich eine Möglichkeit, ethische Designrichtlinien für Entwickler zu erstellen, die nach der Analyse der Dark Patterns in Apps als Leitfaden dienen könnten. Diese Leitfäden könnten Entwicklern Hilfestellungen im Design von Einwilligungserklärungen bieten, um diese möglichst transparent und informativ zu gestalten.
In dieser Arbeit wurden analytische Untersuchungen durchgeführt und der Grundstein im Bereich Anwenderaufklärung über Datennutzung in Apps gelegt. Eine

Weiterentwicklung könnte die Entwicklung einer Software umfassen, die Nutzer transparent über den Umgang mit ihren Daten informiert. Im ersten Schritt könnte ein Parser entwickelt werden, welcher Datenschutzerklärungen analysiert, Empfänger, Drittländer und personenbezogene Daten identifiziert und deren rechtliche Grundlage klärt. Der Parser könnte dann mit einer Software kombiniert werden, welche eine statische Analyse anhand der APK einer App durchführt und ebenfalls relevante Daten herausstellt. Die Ergebnisse können dann zusammengefasst werden, um ein umfassendes Bild über die Datennutzung der App zu präsentieren. Ähnlich wie Van Kleek et al. [73] könnte eine solche Software bereits im App-Store schon vor dem Download der App aufklärende Informationen für den Nutzer präsentieren.

Die gewonnenen Erkenntnisse tragen dazu bei, ein umfassenderes Verständnis für die Herausforderungen im Datenschutz im Kontext von Fitness- und Gesundheits-Apps zu entwickeln. Durch die Integration von Informationen aus den Bereichen Informationssicherheit, Human-Computer Interaction und Recht bietet diese Arbeit einen interdisziplinären Ansatz. Dies eröffnet Möglichkeiten für vertiefte Analysen in jedem dieser Forschungsbereiche.
Die Verbindung von Informationssicherheit und Datenschutz trägt dazu bei, Schwachstellen und potenzielle Bedrohungen in Bezug auf die Vertraulichkeit und Integrität der Nutzerdaten aufzudecken. Gleichzeitig ermöglicht die Einbeziehung von Aspekten der Human-Computer Interaction eine genauere Untersuchung der Nutzererfahrung und -wahrnehmung im Hinblick auf Datenschutzpraktiken. Dies ist entscheidend, um sicherzustellen, dass Datenschutzrichtlinien nicht nur formal korrekt sind, sondern auch für die Benutzer verständlich und akzeptabel.
Die Berücksichtigung rechtlicher Aspekte in der Analyse bietet eine Grundlage für die Diskussion über die Einhaltung geltender Datenschutzgesetze und die Identifizierung von möglichen Lücken oder Unsicherheiten. Diese Masterarbeit fördert somit einen Ansatz zur Weiterentwicklung von Datenschutzmaßnahmen in Fitness- und Gesundheits-Apps.

Literatur

[1] MyFitnessPal, Inc. My fitness pal, 2023. URL https://play.google.com/store/apps/developer?id=MyFitnessPal,+Inc.&hl=de&gl=US.

[2] SimpleInnovation . My calendar, 2023. URL https://play.google.com/store/apps/details?id=com.lbrc.PeriodCalendar&hl=en&gl=US.

[3] Sweatco Ltd. Sweatcoin, 2023. URL https://play.google.com/store/apps/details?id=in.sweatco.app&hl=en&gl=US.

[4] Artikel 29-Gruppe. *Leitlinien für Transparenz gemäß der Verordnung 2016/679*. WP 260, 2018.

[5] Ajin Abraham. Mobile-security-framework-mobsf, 2022. URL https://github.com/MobSF/Mobile-Security-Framework-MobSF. Zuletzt eingesehen am 24.05.2023.

[6] AndroidRank. Free android market data, history, ranking, 2023. URL https://www.androidrank.org/. Zuletzt eingesehen am 05.01.2023.

[7] Thomas Becker, Patrick Braunmühl, Axel Bussche, Jan-Michael Grages, Valerian Jenny Nils Hullen, Wulf Kamlah, Niclas Krohm, Michael Kuhnke, Kai-Uwe Plath, Jan Dirk Roggenkamp, Lutz Schreiber, Katrin Stamer, und Jörn Wittmann. *DSGVO/BDSG*, volume 3. Aufl. Dr. Otto Schmidt, 2018.

[8] Jeroen Beckers, Eduardo Novella, und Michael Kuc. Magisk trust user certs, 2022. URL https://github.com/NVISOsecurity/MagiskTrustUserCerts. Zuletzt eingesehen am 19.12.2023.

[9] Holger Bleich. Studie: Datenschutzerklärungen werden wenig gelesen, 2022. URL https://www.heise.de/newsticker/meldung/Studie-Datenschutzerklaerungen-werden-wenig-gelesen-4516406.html. Zuletzt eingesehen am 24.05.2023.

[10] THE EUROPEAN DATA PROTECTION BOARD. Endorsement 1, 2018.

[11] Christoph Bogenstahl. Dark patterns – mechanismen (be)trügerischen internetdesigns. *Themenkurzprofil*, 30, 2019.

[12] Dr. Stefan Brink. *BeckOK Datenschutzrecht*, volume 23. Edition. C.H.BECK München, 2018.

[13] Christoph Bösch, Benjamin Erb, Frank Kargl, Henning Kopp, und Stefan Pfattheicher. Tales from the dark side: Privacy dark strategies and privacy dark patterns. *Proceedings on Privacy Enhancing Technologies*, 2016:237–254, 07 2016. doi: 10.1515/popets-2016-0038.

[14] Wolfie Christl. Corporate surveillance in everyday life. *Cracked Labs*, 2017.

[15] Andreas Claesson und Tor E. Bjørstad. „Out of Control" – a review of data sharing by popular mobile apps. Technical report, Norwegian Consumer Council, Oslo, 2020.

[16] Andreas Claesson und Tor E. Bjørstad. Technical report „Out of Control" - a review of data sharing by popular mobile apps. Technical report, Norwegian Consumer Counci, 2020.

[17] Cloud03. So verwenden sie den burp suite-decoder, 2023. URL https://cloudo3.com/de/internet/so-verwenden-sie-den-burp-suite-decoder/33302323. Zuletzt eingesehen am 22.01.2024.

[18] CNN. Ireland's data centers are an economic lifeline. environmentalists say they're wrecking the planet, 2022. URL https://edition.cnn.com/2022/01/23/tech/ireland-data-centers-climate-intl-cmd/index.html. Zuletzt eingesehen am 29.12.2023.

[19] Gregory Conti und Edward Sobiesk. Malicious interface design: Exploiting the user. *World wide web*, page 271–280, 2010. doi: 10.1145/1772690.1772719. URL https://doi.org/10.1145/1772690.1772719.

[20] Dejure. Informationspflicht bei erhebung von personenbezogenen daten bei der betroffenen person, 2023. URL https://dejure.org/gesetze/DSGVO/13.html. Zuletzt eingesehen am 23.11.2023.

[21] Android Developers. Security with network protocols, 2023. URL https://developer.android.com/privacy-and-security/security-ssl. Zuletzt eingesehen am 19.12.2023.

[22] Android Developers. Protect against security threats with safetynet, 2023. URL https://developer.android.com/privacy-and-security/safetynet. Zuletzt eingesehen am 22.01.2024.

[23] Eithne Dodd. A natural progression? why there are so many data centres in ireland, 2023. URL https://www.buzz.ie/news/irish-news/data-centres-ireland-economy-energy-25529167. Zuletzt eingesehen am 29.12.2023.

[24] DSGVO. Transparente information, kommunikation und modalitäten für die ausübung der rechte der betroffenen person, 2023. URL https://dsgvo-gesetz.de/art-12-dsgvo/. Zuletzt eingesehen am 22.01.2024.

[25] DSGVO. Bedingungen für die einwilligung, 2023. URL https://dsgvo-gesetz.de/art-7-dsgvo/. Zuletzt eingesehen am 22.01.2024.

[26] Michael D. Ernst. Static and dynamic analysis: synergy and duality. *International Conference on Software Engineering*, pages 25–29, 2003.

[27] Frida. Welcome - what is frida, exactly?, 2022. URL https://frida.re/docs/home/. Zuletzt eingesehen am 13.07.2023.

[28] genymotion. Genymotion desktop 3.6.0, 2024. URL https://www.genymotion.com/. Zuletzt eingesehen am 10.01.2024.

[29] Linda Di Geronimo, Larissa Braz, Enrico Fregnan, Fabio Palomba, und Alberto Bacchelli. Ui dark patterns and where to find them: A study on mobile applications and user perception. *CHI*, 2020.

[30] Peter Gola und Dirk Heckmann. *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG*, volume 3. Auflage. C.H.BECK, 2022.

[31] Google. Google playstore, 2023. URL https://play.google.com/. Zuletzt eingesehen am 16.06.2023.

[32] Google. Advertising id, 2023. URL https://support.google.com/googleplay/android-developer/answer/6048248?hl=en. Zuletzt eingesehen am 29.12.2023.

[33] Colin Gray, Yubo Kou, Bryan Battles, Joseph Hoggatt, und Austin Toombs. The dark (patterns) side of ux design. *CHI Conference on Human Factors in Computing Systems*, 04 2018. doi: 10.1145/3173574.3174108.

[34] Saul Greenberg, Sebastian Boring, Jo Vermeulen, und Jakub Dostal. Dark patterns in proxemic interactions: A critical perspective. *conference on Designing interactive systems*, page 523–532, 2014. doi: 10.1145/2598510.2598541. URL https://doi.org/10.1145/2598510.2598541.

[35] Quinn Grundy, Kellia Chiu, Fabian Held, Andrea Continella, Lisa Bero, und Ralph Holz. Data sharing practices of medicines related apps and the mobile ecosystem: traffic, content, and network analysis. *BMJ*, 2019.

[36] Johanna Gunawan, Amogh Pradeep, David Choffnes, Woodrow Hartzog, und Christo Wilson. A comparative study of dark patterns across web and

mobile modalities. *ACM*, 5(CSCW2), oct 2021. doi: 10.1145/3479521. URL https://doi.org/10.1145/3479521.

[37] Kit Huckvale, John Torous, und Mark E. Larsen. Assessment of the data sharing and privacy practices of smartphone apps for depression and smoking cessation. *Jama Network Open*, 2019.

[38] Martin Husák, Milan Cermák, Tomas Jirsík, und Pavel Celeda. Https traffic analysis and client identification using passive ssl/tls fingerprinting. *Journal on Information Security*, 04 2016.

[39] imperva. Man in the middle (mitm) attack, 2023. URL https://www.imperva.com/learn/application-security/man-in-the-middle-attack-mitm/. Zuletzt eingesehen am 06.11.2023.

[40] Inmobi. Our story, 2022. URL https://www.inmobi.com/company/. Zuletzt eingesehen am 13.07.2023.

[41] Jadx. Kali jadx, 2022. URL https://www.kali.org/tools/jadx/. Zuletzt eingesehen am 24.05.2023.

[42] Udo Kannengiesser und John S Gero. Empirical evidence for kahneman's system 1 and system 2 thinking in design. *Human Behavior in Design*, pages 89–100, 2019.

[43] Klimaszewski Szymon. Blood pressure, 2023. URL https://play.google.com/store/apps/details?id=com.szyk.myheart&hl=en&gl=US.

[44] Matthias Kohn, Merle Freye, Mehrdas Bahrini, und Alexander Herbst. Gesundheits-apps auf dem prüfstand –Überprüfung der angaben in datenschutzerklärungen zur datenweitergabe. In *INFORMATIK 2023 - Designing Futures: Zukünfte gestalten*, pages 677–688. Gesellschaft für Informatik e.V., Bonn, 2023. ISBN 978-3-88579-731-9. doi: 10.18420/inf2023_78.

[45] Europäische Kommission. Was sind personenbezogene daten?, 2023. URL https://commission.europa.eu/law/law-topic/data-protection/reform/what-personal-data_de. Zuletzt eingesehen am 21.11.2023.

[46] Jürgen Kühling und Benedikt Buchner. *Datenschutz-Grundverordnung, Bundesdatenschutzgesetz: DS-GVO / BDSG*, volume 3. Aufl. C.H.BECK, 2020.

[47] Mirko Laudon. 76 tage pro jahr für das lesen von agb, 2022. URL https://www.strafakte.de/rechtspolitik/76-tage-pro-jahr-lesen-agb/. Zuletzt eingesehen am 14.07.2023.

[48] Leap Fitness Group. Home workout - no equipment, 2023. URL https://play.google.com/store/apps/details?id=homeworkout.homeworkouts.noequipment&hl=en&gl=US.

[49] Leap Fitness Group. Six pack in 30 days, 2023. URL https://play.google.com/store/apps/details?id=sixpack.sixpackabs.absworkout&hl=en&gl=US.

[50] Leap Fitness Group. Lose weight app for men, 2023. URL https://play.google.com/store/apps/details?id=menloseweight.loseweightappformen.weightlossformen&hl=en&gl=US.

[51] Li Li, Tegawendé F. Bissyandé, Mike Papadakis, Siegfried Rasthofer, Alexandre Bartel, Damien Octeau, Jacques Klein, und Le Traon. Static analysis of android apps: A systematic literature review. *Information and Software Technology*, 88:67–95, 2017. ISSN 0950-5849. doi: https://doi.org/10.1016/j.infsof.2017.04.001. URL https://www.sciencedirect.com/science/article/pii/S0950584917302987.

[52] Bernd Lorenz. *Datenschutzrechtliche Informationspflichten*. VuR, 2019.

[53] Jamie Luguri und Lior Jacob Strahilevitz. Shining a light on dark patterns. *Journal of Legal Analysis*, 13:1–42, 2021.

[54] Magisk. Magisk root, 2019. URL https://magiskroot.com/. Zuletzt eingesehen am 19.12.2023.

[55] Magisk. Bootloader-Übersicht, 2023. URL https://topjohnwu.github.io/Magisk/. Zuletzt eingesehen am 19.12.2023.

[56] Avijit Mallik. Man-in-the-middle-attack: Understanding in simple words. *Cyberspace: Jurnal Pendidikan Teknologi Informasi*, 2, 2018.

[57] Arunesh Mathur, Jonathan Mayer, und Mihir Kshirsagar. What makes a dark pattern... dark? *Conference on Human Factors in Computing Systems*, 21:1–19, 2021.

[58] Nixintel. Geolocating mobile phones with an ip, 2020. URL https://nixintel.info/osint/geolocating-mobile-phones-with-an-ip/. Zuletzt eingesehen am 29.12.2023.

[59] Noyb. Google: Du willst nicht getrackt werden? wie wär's mit einer neuen tracking-id!, 2020. URL https://noyb.eu/de/beschwerde-gegen-google-tracking-id-eingereicht. Zuletzt eingesehen am 29.12.2023.

[60] Okta. Rooted devices: Definition, benefits & security risks, 2023. URL https://www.okta.com/identity-101/rooted-device/. Zuletzt eingesehen am 19.12.2023.

[61] PortSwigger. Burp suite documentation, 2022. URL https://portswigger.net/burp/documentation/desktop. Zuletzt eingesehen am 13.07.2023.

[62] Sebastian Rieger und Caroline Sinders. Dark patterns: Design mit gesellschaftlichen nebenwirkungen. Technical report, UStiftung Neue Verantwortung e.V., 2020.

[63] Shazir Shafeeque, G. S. N. Meedin, und H. U. W. Ratnayake. *Locating the Position of a Cell Phone User Using GSM Signals*. Springer Singapore, Singapore, 2019.

[64] Spiros Simitis, Gerrit Hornung, und Indra Speicker gen. Döhmann. *Datenschutzrecht*. Nomos, 2019.

[65] Simple Design Ltd. My calendar, 2023. URL https://play.google.com/store/apps/details?id=com.popularapp.periodcalendar&hl=en&gl=US.

[66] Android Source. Bootloader-Übersicht, 2023. URL https://source.android.com/docs/core/architecture/bootloader?hl=de. Zuletzt eingesehen am 19.12.2023.

[67] Android Studio. Android studio, 2024. URL https://developer.android.com/studio. Zuletzt eingesehen am 10.01.2024.

[68] Burp Suite. Burp suite documentation, 2023. URL https://portswigger.net/burp/documentation. Zuletzt eingesehen am 22.01.2024.

[69] Sumup. Datenschutzgrundverordnung (dsgvo) – was ist die dsgvo?, 2023. URL https://www.sumup.com/de-de/rechnungen/lexikon/dsgvo/. Zuletzt eingesehen am 23.11.2023.

[70] Temenos. The android manifest file, 2024. URL https://docs.kony.com/konylibrary/visualizer/visualizer_user_guide/Content/AndroidManifest_File.htm. Zuletzt eingesehen am 08.01.2024.

[71] The Irish Times. The irish times view on data centres: a system under strain, 2023. URL https://www.siliconrepublic.com/enterprise/data-centre-network-ireland. Zuletzt eingesehen am 29.12.2023.

[72] tumblr, 2023. URL https://www.tumblr.com/. Zuletzt eingesehen am 20.06.2023.

[73] Max Van Kleek, Ilaria Liccardi, Reuben Binns, Jun Zhao, Daniel J. Weitzner, und Nigel Shadbolt. Better the devil you know: Exposing the data sharing practices of smartphone apps. *CHI Conference on Human Factors in Computing Systems*, page 5208–5220, 2017. doi: 10.1145/3025453.3025556. URL https://doi.org/10.1145/3025453.3025556.

[74] Vipos Apps. Ladytimer ovulation timer, 2023. URL https://play.google.com/store/apps/details?id=com.ladytimer.ovulationcalendar&hl=en&gl=US.

A. Appendix

Im Appendix sind die umfassenden Ergebnisse der Forschungsuntersuchung dargestellt. Des Weiteren wurden individuelle Berichte für jede App erstellt, die auf dem beigefügten USB-Stick abgerufen werden können.

Übermittlungen an Drittempfänger

Pregnancy & Baby Tracker (Amma)
Adapty
Adcolony
Adobe
Amazon Web Services
Amplitude
Android Development Tools
AOMedia
Apple
Applovin
AppsFlyers
ByteDance
Depositphotos
Example.com
Exoplayer
Facebook
Firebase
Flurry
Github
Google
Google Analytics
Huggies
Inmobi
JourneyApps
Mail.ru
Mixpanel
Mobile Dimensions
Mozilla
MyTarget
MyTracker
PGBonus
Skillbox
Storyly
SupersonicAds
Telecomdom
TikTok
Twitter
W3
XML-Pull
Yahoo
Yandex

Sweatcoin (Sweatco Ltd)
Adcolony
Adobe
Akisinn (Malware)
Amazon Web Services
Android Development Tools
AOMedia
Appcenter
Apple
Applovin
Bugsnag
Cloudflare
Codepush
Dewrain
Exoplayer
Facebook
Firebase
Fyber
Github
Google
Inmobi
Kochava
Microsoft
Pangle
Pinterest
Pollfish
Rayjump
Smartlink
SSDK
SupersonicAds
SWMansion
Tapjoy
TikTok
Twitter
Vaicore
Vungle
W3
Whatwg.org
XML-Pull

Samsung Health (Samsung)
Adobe
Ahnlab
Amap
Amazon Web Services
Android Development Tools
Apache
Boohee
Facebook
Fatsecret
Fireeye
Fitbit
Garmin
Giphy
Github
Glowing
Google
ImHealth
Jawbone
Komoot
Microsoft
Misfitwearables
MyWelness
Naturecycles
Nvidia
Peg Tech Inc.
Runkeeper
Sleepcycle
Topografix
W3
Weathercn
XML-Pull

Zepp Life (Anhui Huami Information Technology Co. Ltd)
Adobe
Airoha
Alibaba Group
Amap
Amazfit
Amazon Web Services
Apple
Auth0
Autonavi
Bcebos
Bouncycastle
Cluetrust
ffmpeg
Garmin
Github
Google
IEC
Ifengimg
Jivesoftware
Line
Meishesdk
Mwallet
Netty
Openssl
Tencant
Topografix
Twitter
Videolan
W3
Weibo
Xiaomi
XML-Pull

Ovia Pregnancy & Baby Tracker
Adobe
Amazon Web Services
Amplitude
Android Development Tools
Babylist
Crisistextline.org
Dashif
drugs
Enfamil
Example.com
Facebook
Findahelpline
Github
Giveusashout
Google
Helpshift
Instagram
Lifeline
Ngs
Pieta
Pinterest
Saptel
slf4j
Spuk
Talksuicide
Text50808
Twitter

My Calendar (SimpleInnovation)
Adobe
Amazon Web Services
Android Development Tools
AOMedia
Apple
Applovin
ByteDance
Exoplayer
Facebook
Firebase
Fyber
Github
Google
Inmobi
Microsoft
Mintegral
Pangle
Smaato
SSDK
SupersonicAds
TikTok
Verizon
Vungle
W3
XML-Pull

Medscape(WebMD,LLC)
1trust
Adobe
Apache
Apple
BranchIO
Braze
Contextweb
Events
Firebase
Github
Google
Ibclick
Jbpm
Ktor
Material.io
Onetrust
Onlineexperiences
Openssl
Otdev
Qxmd
Scorecardresearch
W3
XML-Pull

MyFitnessPal (MyFitnessPal, Inc.)
AdsbyNimbus
Amazon Ad Services
Amplitude
Bipm
BranchIO
Brightcove
CDN
Events
Facebook
Firebase
Github
Google
Inmobi
Oeis.org
Samsung
Split
Twitter
UnityAds
W3
Zendesk

Blood Pressure (K. Szymon)
Adobe
Android Development Tools
Example.com
Exoplayer
Facebook
Firebase
Github
Google
Google Analytics
Huawei
Tensorflow

Flo Ovulation & Period Tracker (Flo Health Inc.)
AppsFlyers
Cloudflare
Docs.rs
Example.com
Firebase
Fitbit
Github
Google
MongoDB

MyTherapy (SmartPatient)
Adobe
Amazon Web Services
Android Development Tools
AOMedia
Apotheke.com
Apothekenfinder
Apple
Avo
Comjoo
Demartology.org
Example.com
Firebase
Github
Global Allergy and Asthma European Network
Google
IP-API
Manateeworks
Medworx
Novartis
W3
Zetetic

Pregnany Tracker (Amila)
Adobe
Amazon Web Services
Android Development Tools
AOMedia
Apple
Applovin
Exoplayer
Firebase
Github
Google
Microsoft
W3

My Calendar - Period Tracker (Simple Design Ltd.)
Adobe
Amazon Ad Services
Apache
Dropbox
Firebase
Google
Google Analytics
Huawei
Mail.ru
Microsoft
MyTarget
MyTracker
W3
XML-Pull
Yahoo

Lose Weight App for Men (Leap fitness)
Adobe
Android Development Tools
Apple
Exoplayer
Firebase
Github
Google
Huawei
Microsoft
MyTarget
Rustore
W3
XML-Pull

Health (Ada)
Adjust
Braze
Facebook
Github
Google
Openssl
Pinterest
Twitter

Home Workout - No Equipment (Leap fitness group)
Facebook
Firebase
Github
Google
Google Analytics
Period Calendar
Pis.com
XML-Pull

Google Fit Activity Tracking (Google)
Aasm
Adobe
American Heart Association
Android Development Tools
Github
Tensorflow
World Health Organization

Period and Ovulation Tracker (SMSROBOT LTD)
Amazon Web Services
Android Development Tools
Facebook
Firebase
Google
labcorp

Ladytimer Ovulation Calendar (Vipos Apps)
Android Development Tools
Applovin
BranchIO
Google
MagicGirl.me

30 days sixpack (Leap fitness group)
AOMedia
Google
Mail.ru

Kategorisierung der Empfänger

Drittempfänger	**Drittempfänger-Kategorie**
1trust	Service
Aasm	Information
Adapty	Advertisement
Adcolony	Advertisement
Adjust	Advertisement
Adobe	Service
AdsbyNimbus	Advertisement
Appcenter	Service
Ahnlab	Service
Airoha	Service
Akisinn (Malware)	Malware
Alibaba Group	Service
Amap	Service
Amazfit	Service
American Heart Association	Information
Amazon Ad Services	Advertisement
Amazon Web Services	Service
Amplitude	Analytics
Codepush	Service
Android Development Tools	Service
Apache	Service
Apothekenfinder	Information
Apotheke.com	Information
Apple	Partner
Applovin	Analytics
AppsFlyers	Analytics
AOMedia	Service
Auth0	Service
Autonavi	Service
Avo	Analytics
Babylist	Partner
Bcebos	Advertisement
Bipm	Governmental
Boohee	Service
Bouncycastle	Service
BranchIO	Service
Braze	Advertisement
Brightcove	Service
Bugsnag	Analytics
ByteDance	SocialMedia
CDN	Service
Cloudflare	Service

Drittempfänger	**Drittempfänger-Kategorie**
Comjoo	Information
Contextweb	Advertisement
Cluetrust	Service
Crisistextline.org	Information
Dashif	Service
Demartology.org	Information
Depositphotos	Service
Dewrain	Malicious
Docs.rs	Service
Dropbox	Partner
drugs	Information
Enfamil	Advertisement
Events	Partner
Example.com	Service
Exoplayer	Service
Facebook	Social Media
Fatsecret	Partner
ffmpeg	Service
Findahelpline	Information
Fireeye	Service
Firebase	Service
Fitbit	Partner
Flurry	Analytics
Fyber	Advertisement
Global Allergy and Asthma European Network	Government
Garmin	Partner
Giphy	Service
Giveusashout	Information
Glowing	Partner
Google	Advertisement/Partner
Google Analytics	Analytics
Github	Service
Helpshift	Information
Huawei	Partner
Huggies	Partner
Ibclick	Service
IEC	Government
Ifengimg	Service
ImHealth	Government
Inmobi	Advertisement
Instagram	Social Media
IP-API	Service

Drittempfänger	**Drittempfänger-Kategorie**
Jawbone	Partner
Jivesoftware	Service
JourneyApps	Service
Jbpm	Service
Kochava	Analytics
Komoot	Partner
Ktor	Service
labcorp	Partner
Lifeline	Information
Line	Social Media
Manateeworks	Service
MagicGirl.me	Partner
Mail.ru	Service
Material.io	Service
Medworx	Partner
Meishesdk	Service
Microsoft	Partner
Mintegral	Advertisement
Misfitwearables	Partner
Mixpanel	Analytics
Mobile Dimensions	Service
MongoDB	Service
Mozilla	Partner
Mwallet	Service
MyTarget	Advertisement
MyTracker	Analytics
MyWelness	Partner
Naturecycles	Service
Netty	Service
Ngs	Service
Novartis	Partner
Nvidia	Partner
Oeis.org	Service
Onetrust	Service
Onlineexperiences	Service
Openssl	Service
Otdev	Service
Pangle	Advertisement
Peg Tech Inc.	Service
Period Calendar	Partner
PGBonus	Partner
Pieta	Information

Drittempfänger	**Drittempfänger-Kategorie**
Pinterest	Social Media
Pis.com	Service
Pollfish	Service
Qxmd	Partner
Rayjump	Advertisement
Rustore	Partner
Runkeeper	Partner
Samsung	Partner
Saptel	Information
Scorecardresearch	Analytics
Skillbox	Partner
Sleepcycle	Partner
slf4j	Service
Smaato	Advertisement
Smartlink	Service
Split	Advertisement
Spuk	Partner
SSDK	Service
SupersonicAds	Advertisement
Storyly	Partner
SWMansion	Service
Talksuicide	Information
Tapjoy	Advertisement
Telecomdom	Analytics
Tencant	Partner
Tensorflow	Service
Text50808	Information
TikTok	Social Media
Topografix	Service
Twitter	Social Media
UnityAds	Advertisement
Videolan	Service
Vaicore	Advertisement
Verizon	Services
Vidyo	Service
Vungle	Advertisement
W3	Service
Weathercn	Partner
Weibo	Partner
World Health Organization	Information
Whatwg.org	Service
Xiaomi	Partner

XML-Pull	Service
Yahoo	Social Media
Yandex	Service
Zendesk	Service
Zetetic	Service

Übermittlung an kategorisierte Empfänger

Untersuchte Apps	**Werbe-Unternehmen**	**Analytische Dienste**	**Information**
Pregnancy & Baby Tracker (Amma)	6	8	0
Sweatcoin (Sweatco Ltd)	9	4	0
Samsung Health (Samsung)	1	1	0
Zepp Life (Anhui Huami Information Technology Co. Ltd)	2	1	0
Ovia Pregnancy & Baby Tracker	2	2	9
MyTherapy (SmartPatient)	1	2	4
My Calendar (SimpleInnovation)	6	3	0
Medscape(WebMD,LLC)	2	2	0
MyFitnessPal (MyFitnessPal, Inc.)	6	2	0
My Calendar - Period Tracker (Simple Design Ltd.)	3	2	0
Lose Weight App for Men (Leap fitness)	2	1	0
Pregnany Tracker (Amila)	1	2	0
Flo Ovulation & Period Tracker (Flo Health Inc.)	1	1	0
Blood Pressure (K. Szymon)	1	1	0
Health (Ada)	2	1	0
Home Workout - No Equipment (Leap fitness group)	1	1	0
Period and Ovulation Tracker (SMSROBOT LTD)	1	1	0
Google Fit Activity Tracking (Google)	0	0	3
Ladytimer Ovulation Calendar (Vipos Apps)	1	2	0
30 days sixpack (Leap fitness group)	1	1	0
Summe	49	38	16

Untersuchte Apps	**Staatlich**	**Dienstleister**	**Social Media**
Pregnancy & Baby Tracker (Amma)	0	15	5
Sweatcoin (Sweatco Ltd)	0	19	4
Samsung Health (Samsung)	1	19	2
Zepp Life (Anhui Huami Information Technology Co. Ltd)	1	19	2
Ovia Pregnancy & Baby Tracker	0	9	4
MyTherapy (SmartPatient)	1	13	1
My Calendar (SimpleInnovation)	0	10	3
Medscape(WebMD,LLC)	0	17	0
MyFitnessPal (MyFitnessPal, Inc.)	1	7	1
My Calendar - Period Tracker (Simple Design Ltd.)	0	7	1
Lose Weight App for Men (Leap fitness)	0	7	0
Pregnany Tracker (Amila)	0	8	0
Flo Ovulation & Period Tracker (Flo Health Inc.)	0	7	0
Blood Pressure (K. Szymon)	0	5	1
Health (Ada)	0	3	3
Home Workout - No Equipment (Leap fitness group)	0	4	1
Period and Ovulation Tracker (SMSROBOT LTD)	0	3	1
Google Fit Activity Tracking (Google)	0	3	0
Ladytimer Ovulation Calendar (Vipos Apps)	0	1	0
30 days sixpack (Leap fitness group)	0	2	0
Summe	4	178	29

Untersuchte Apps	**Potenziell Bösartig**	**Partner**
Pregnancy & Baby Tracker (Amma)	0	7
Sweatcoin (Sweatco Ltd)	2	3
Samsung Health (Samsung)	0	15
Zepp Life (Anhui Huami Information Technology Co. Ltd)	0	5
Ovia Pregnancy & Baby Tracker	0	4
MyTherapy (SmartPatient)	0	4
My Calendar (SimpleInnovation)	0	3
Medscape(WebMD,LLC)	0	4
MyFitnessPal (MyFitnessPal, Inc.)	0	3
My Calendar - Period Tracker (Simple Design Ltd.)	0	4
Lose Weight App for Men (Leap fitness)	0	5
Pregnany Tracker (Amila)	0	3
Flo Ovulation & Period Tracker (Flo Health Inc.)	0	2
Blood Pressure (K. Szymon)	0	2
Health (Ada)	0	1
Home Workout - No Equipment (Leap fitness group)	0	2
Period and Ovulation Tracker (SMSROBOT LTD)	0	2
Google Fit Activity Tracking (Google)	0	0
Ladytimer Ovulation Calendar (Vipos Apps)	0	2
30 days sixpack (Leap fitness group)	0	1
Summe	2	72

Untersuchte Apps	**Drittländer übereinstimmung**	**Empfänger übereinstimmung**	**Anzahl an Namentlich gennanten Drittländern**
Pregnancy & Baby Tracker (Amma)	1	1	0
Sweatcoin (Sweatco Ltd)	0	1	1
Samsung Health (Samsung)	1	1	0
Zepp Life (Anhui Huami Information Technology Co. Ltd)	0	1	7
Ovia Pregnancy & Baby Tracker	0	0	1
MyTherapy (SmartPatient)	1	1	1
My Calendar (SimpleInnovation)	1	0	0
Medscape(WebMD,LLC)	1	1	1
MyFitnessPal (MyFitnessPal, Inc.)	1	1	2
My Calendar - Period Tracker (Simple Design Ltd.)	1	1	0
Lose Weight App for Men (Leap fitness)	1	1	0
Pregnany Tracker (Amila)	1	1	3
Flo Ovulation & Period Tracker (Flo Health Inc.)	1	1	2
Blood Pressure (K. Szymon)	0	1	0
Health (Ada)	1	0	3
Home Workout - No Equipment (Leap fitness group)	1	1	0
Period and Ovulation Tracker (SMSROBOT LTD)	1	1	1
Google Fit Activity Tracking (Google)	1	1	1
Ladytimer Ovulation Calendar (Vipos Apps)	0	1	0
30 days sixpack (Leap fitness group)	1	1	0
Prozentanteil	75%	85%	

Untersuchung der Kategorisierung und namentlichen Nennung von Empfängern

Untersuchte Apps	**Anzahl an Kategorien bei Drittländern**	**Größtenteils kategorisierte Drittländer**	**Anzahl an Namentlich gennanten Empfängern**
Pregnancy & Baby Tracker (Amma)	1	1	14
Sweatcoin (Sweatco Ltd)	1	1	2
Samsung Health (Samsung)	1	1	2
Zepp Life (Anhui Huami Information Technology Co. Ltd)	0	0	6
Ovia Pregnancy & Baby Tracker	0	0	8
MyTherapy (SmartPatient)	2	1	9
My Calendar (SimpleInnovation)	1	1	14
Medscape(WebMD,LLC)	1	1	3
MyFitnessPal (MyFitnessPal, Inc.)	3	1	1
My Calendar - Period Tracker (Simple Design Ltd.)	1	1	4
Lose Weight App for Men (Leap fitness)	1	1	6
Pregnany Tracker (Amila)	0	0	1
Flo Ovulation & Period Tracker (Flo Health Inc.)	2	1	24
Blood Pressure (K. Szymon)	0	0	2
Health (Ada)	2	0	16
Home Workout - No Equipment (Leap fitness group)	1	1	10
Period and Ovulation Tracker (SMSROBOT LTD)	1	0	3
Google Fit Activity Tracking (Google)	2	1	1
Ladytimer Ovulation Calendar (Vipos Apps)	0	0	0
30 days sixpack (Leap fitness group)	1	1	8
Prozentanteil		65%	

Untersuchte Apps	**Anzahl an Kategorien bei Empfängern**	**Größtenteils kategorisierte Empfänger**	**Unter zwei Empfänger pro Kategorie**
Pregnancy & Baby Tracker (Amma)	7	0	1
Sweatcoin (Sweatco Ltd)	11	1	0
Samsung Health (Samsung)	6	1	0
Zepp Life (Anhui Huami Information Technology Co. Ltd)	14	1	1
Ovia Pregnancy & Baby Tracker	10	1	1
MyTherapy (SmartPatient)	3	0	0
My Calendar (SimpleInnovation)	1	0	0
Medscape(WebMD,LLC)	4	1	0
MyFitnessPal (MyFitnessPal, Inc.)	7	1	1
My Calendar - Period Tracker (Simple Design Ltd.)	6	1	1
Lose Weight App for Men (Leap fitness)	6	0	1
Pregnany Tracker (Amila)	1	1	0
Flo Ovulation & Period Tracker (Flo Health Inc.)	2	1	0
Blood Pressure (K. Szymon)	0	0	0
Health (Ada)	1	0	1
Home Workout - No Equipment (Leap fitness group)	6	0	1
Period and Ovulation Tracker (SMSROBOT LTD)	6	1	0
Google Fit Activity Tracking (Google)	2	1	0
Ladytimer Ovulation Calendar (Vipos Apps)	2	1	0
30 days sixpack (Leap fitness group)	5	0	0
Prozentanteil		60%	40%

Untersuchte Apps	**Über 10 Empfänger pro Kategorie**	**Mehr Kategorien als festgestellte Empfänger**	**Große Unternehmen namentlich gennant?**
Pregnancy & Baby Tracker (Amma)	1	1	1
Sweatcoin (Sweatco Ltd)	1	1	0
Samsung Health (Samsung)	1	1	1
Zepp Life (Anhui Huami Information Technology Co. Ltd)	1	1	1
Ovia Pregnancy & Baby Tracker	0	1	1
MyTherapy (SmartPatient)	1	0	1
My Calendar (SimpleInnovation)	0	0	1
Medscape(WebMD,LLC)	1	1	0
MyFitnessPal (MyFitnessPal, Inc.)	1	0	0
My Calendar - Period Tracker (Simple Design Ltd.)	1	1	1
Lose Weight App for Men (Leap fitness)	1	1	1
Pregnany Tracker (Amila)	1	0	1
Flo Ovulation & Period Tracker (Flo Health Inc.)	1	0	1
Blood Pressure (K. Szymon)	0	0	0
Health (Ada)	0	0	1
Home Workout - No Equipment (Leap fitness group)	0	1	1
Period and Ovulation Tracker (SMSROBOT LTD)	0	1	1
Google Fit Activity Tracking (Google)	0	0	1
Ladytimer Ovulation Calendar (Vipos Apps)	0	1	0
30 days sixpack (Leap fitness group)	0	0	1
Prozentanteil	55%	55%	75%

Untersuchte Apps	**AD ID**	**Hardware Information**	**Country/Language/Timezone**
30 days sixpack (Leap fitness group)	1	1	0
Blood Pressure (K. Szymon)	1	1	1
Flo Ovulation & Period Tracker (Flo Health Inc.)	1	1	0
Google Fit Activity Tracking (Google)	0	0	0
Health (Ada)	1	1	1
Home Workout - No Equipment (Leap fitness group)	1	0	1
Ladytimer Ovulation Calendar (Vipos Apps)	0	0	0
Medscape (WebMD)	1	1	1
My Calendar - Period Tracker (Simple Design Ltd.)	0	0	0
My Calendar (SimpleInnovation)	1	1	1
Ovia Pregnancy & Baby Tracker (Ovia)	0	0	0
MyFitnessPal (MyFitnessPal, Inc.)	1	1	0
MyTherapy (SmartPatient)	0	0	0
Period and Ovulation Tracker (SMSROBOT LTD)	0	0	0
Pregnancy & Baby Tracker (Amma)	1	1	0
Pregnany Tracker (Amila)	1	1	1
Samsung Health (Samsung)	0	1	0
Lose Weight App for Men (Leap fitness Group)	1	1	1
Sweatcoin(Sweatco Ltd)	1	1	1
Zepp Life (Anhui Huami Information Technology Co. Ltd)	1	1	1
Summe	13	13	9

Untersuchte Apps	**Local IP (GPS?)**	**Summe**	**Länder**
30 days sixpack (Leap fitness group)	0	2	USA
Blood Pressure (K. Szymon)	0	3	USA
Flo Ovulation & Period Tracker (Flo Health Inc.)	0	2	USA
Google Fit Activity Tracking (Google)	0	0	
Health (Ada)	0	3	USA, Ger
Home Workout - No Equipment (Leap fitness group)	0	2	USA
Ladytimer Ovulation Calendar (Vipos Apps)	1	1	USA
Medscape (WebMD)	0	3	USA
My Calendar - Period Tracker (Simple Design Ltd.)	0	0	USA, Kanada
My Calendar (SimpleInnovation)	0	3	USA
Ovia Pregnancy & Baby Tracker (Ovia)	0	0	
MyFitnessPal (MyFitnessPal, Inc.)	1	3	USA
MyTherapy (SmartPatient)	0	0	
Period and Ovulation Tracker (SMSROBOT LTD)	0	0	
Pregnancy & Baby Tracker (Amma)	0	2	USA, RU
Pregnany Tracker (Amila)	0	3	USA
Samsung Health (Samsung)	0	1	USA
Lose Weight App for Men (Leap fitness Group)	0	3	USA
Sweatcoin(Sweatco Ltd)	0	3	USA
Zepp Life (Anhui Huami Information Technology Co. Ltd)	0	3	USA
Summe	2	37	

Untersuchung auf Dark Patterns

Untersuchte Apps	Misdirection	Forced Action	Obfuscation
Pregnancy & Baby Tracker (Amma)	1	1	1
Sweatcoin (Sweatco Ltd)	1	1	1
Samsung Health (Samsung)	1	1	1
Zepp Life (Anhui Huami Information Technology Co. Ltd)	0	0	0
Ovia Pregnancy & Baby Tracker	0	0	0
My Calendar (SimpleInnovation)	1	0	0
Medscape(WebMD,LLC)	1	0	0
MyTherapy (SmartPatient)	1	1	1
MyFitnessPal (MyFitnessPal, Inc.)	1	1	1
My Calendar - Period Tracker (Simple Design Ltd.)	0	1	1
Lose Weight App for Men (Leap fitness)	1	0	1
Pregnany Tracker (Amila)	0	0	1
Blood Pressure (K. Szymon)	Keine Angaben	Keine Angaben	Keine Angaben
Flo Ovulation & Period Tracker (Flo Health Inc.)	1	0	0
Health (Ada)	1	0	0
Home Workout - No Equipment (Leap fitness group)	0	1	1
Google Fit Activity Tracking (Google)	1	1	0
Period and Ovulation Tracker (SMSROBOT LTD)	0	1	1
Ladytimer Ovulation Calendar (Vipos Apps)	Keine Angaben	Keine Angaben	Keine Angaben
30 days sixpack (Leap fitness group)	1	0	1
Summe	12	9	11

Untersuchte Apps	**Disguised Data Collection**	**Missing Consent Notices, Consent Checkboxes, or Settings Options**	**Forced Registration**
Pregnancy & Baby Tracker (Amma)	0	0	0
Sweatcoin (Sweatco Ltd)	1	1	1
Samsung Health (Samsung)	0	1	1
Zepp Life (Anhui Huami Information Technology Co. Ltd)	0	0	1
Ovia Pregnancy & Baby Tracker	0	0	1
My Calendar (SimpleInnovation)	0	1	0
Medscape(WebMD,LLC)	0	1	1
MyTherapy (SmartPatient)	1	1	0
MyFitnessPal (MyFitnessPal, Inc.)	0	0	1
My Calendar - Period Tracker (Simple Design Ltd.)	0	1	0
Lose Weight App for Men (Leap fitness)	0	0	0
Pregnany Tracker (Amila)	0	0	0
Blood Pressure (K. Szymon)	Keine Angaben	Keine Angaben	Keine Angaben
Flo Ovulation & Period Tracker (Flo Health Inc.)	0	0	0
Health (Ada)	0	0	0
Home Workout - No Equipment (Leap fitness group)	0	1	0
Google Fit Activity Tracking (Google)	1	1	1
Period and Ovulation Tracker (SMSROBOT LTD)	0	0	0
Ladytimer Ovulation Calendar (Vipos Apps)	Keine Angaben	Keine Angaben	Keine Angaben
30 days sixpack (Leap fitness group)	0	0	0
Summe	3	8	7

Sprache der Datenschutzerklärung und Möglichkeiten zum Widerruf

Untersuchte Apps	**Privacy Policy auf Deutsch?**	**Möglichkeit zum Widerruf**
Pregnancy & Baby Tracker (Amma)	0	0
Sweatcoin (Sweatco Ltd)	0	0
Samsung Health (Samsung)	1	1
Zepp Life (Anhui Huami Information Technology Co. Ltd)	1	1
Ovia Pregnancy & Baby Tracker	App nur auf Englisch	1
My Calendar (SimpleInnovation)	0	0
Medscape(WebMD,LLC)	0	1
MyTherapy (SmartPatient)	1	0
MyFitnessPal (MyFitnessPal, Inc.)	1	1
My Calendar - Period Tracker (Simple Design Ltd.)	0	0
Lose Weight App for Men (Leap fitness)	0	0
Pregnany Tracker (Amila)	App nur auf Englisch	0
Blood Pressure (K. Szymon)	Keine Angaben	Keine Angaben
Flo Ovulation & Period Tracker (Flo Health Inc.)	1	0
Health (Ada)	1	1
Home Workout - No Equipment (Leap fitness group)	0	0
Google Fit Activity Tracking (Google)	1	1
Period and Ovulation Tracker (SMSROBOT LTD)	0	0
Ladytimer Ovulation Calendar (Vipos Apps)	Keine Angaben	Keine Angaben
30 days sixpack (Leap fitness group)	0	0
Summe/Prozentsatz	7	0,388888889

Übermittlung an Drittländer

Untersuchte Apps	**Australien**	**Brazilien**	**China**	**Finnland**	**Frankreich**
Pregnancy & Baby Tracker (Amma)	0	0	0	1	0
Sweatcoin (Sweatco Ltd)	0	0	0	0	0
Samsung Health (Samsung)	0	0	1	0	0
Zepp Life (Anhui Huami Information Technology Co. Ltd)	1	0	1	0	1
My Calendar (SimpleInnovation)	0	0	0	0	0
Medscape(WebMD,LLC)	1	0	0	0	1
MyTherapy (SmartPatient)	0	0	0	0	0
MyFitnessPal (MyFitnessPal, Inc.)	0	0	1	0	1
My Calendar - Period Tracker (Simple Design Ltd.)	0	0	0	0	0
Pregnany Tracker (Amila)	0	0	0	0	0
Blood Pressure (K. Szymon)	0	0	0	0	0
Flo Ovulation & Period Tracker (Flo Health Inc.)	0	0	0	0	0
Health (Ada)	0	0	0	0	0
Home Workout - No Equipment (Leap fitness group)	0	0	0	0	0
Google Fit Activity Tracking (Google)	0	0	0	0	0
Ladytimer Ovulation Calendar (Vipos Apps)	0	0	0	0	0
Period and Ovulation Tracker (SMSROBOT LTD)	0	0	0	0	0
Ovia Pregnancy & Baby Tracker (Ovia)	1	1	1	0	1
Lose Weight App for Men (Leap fitness group)	0	0	0	0	0
30 days sixpack (Leap fitness group)	0	0	0	0	0
Summe	3	1	4	1	4

Untersuchte Apps	**Indien**	**Irland**	**Japan**	**Kanada**	**Niederlande**
Pregnancy & Baby Tracker (Amma)	0	1	0	0	1
Sweatcoin (Sweatco Ltd)	0	1	0	0	0
Samsung Health (Samsung)	0	1	1	0	0
Zepp Life (Anhui Huami Information Technology Co. Ltd)	0	1	0	0	1
My Calendar (SimpleInnovation)	0	0	0	0	0
Medscape(WebMD,LLC)	0	0	0	0	0
MyTherapy (SmartPatient)	0	0	0	0	0
MyFitnessPal (MyFitnessPal, Inc.)	0	1	0	0	0
My Calendar - Period Tracker (Simple Design Ltd.)	0	0	1	0	1
Pregnany Tracker (Amila)	0	0	0	0	0
Blood Pressure (K. Szymon)	0	0	0	0	0
Flo Ovulation & Period Tracker (Flo Health Inc.)	0	0	0	0	0
Health (Ada)	0	0	0	0	0
Home Workout - No Equipment (Leap fitness group)	0	0	0	0	0
Google Fit Activity Tracking (Google)	0	0	0	0	0
Ladytimer Ovulation Calendar (Vipos Apps)	0	0	0	0	0
Period and Ovulation Tracker (SMSROBOT LTD)	0	1	0	0	0
Ovia Pregnancy & Baby Tracker (Ovia)	1	1	1	1	0
Lose Weight App for Men (Leap fitness group)	0	0	0	0	0
30 days sixpack (Leap fitness group)	0	0	0	0	0
Summe	1	7	3	1	3

Untersuchte Apps	Nordmazedonien	Russland	Singapore	Spanien	Sweden
Pregnancy & Baby Tracker (Amma)	0	1	1	0	0
Sweatcoin (Sweatco Ltd)	0	0	0	0	1
Samsung Health (Samsung)	0	0	1	0	1
Zepp Life (Anhui Huami Information Technology Co. Ltd)	0	0	1	0	0
My Calendar (SimpleInnovation)	0	0	0	0	0
Medscape(WebMD,LLC)	0	0	0	1	1
MyTherapy (SmartPatient)	1	0	0	0	0
MyFitnessPal (MyFitnessPal, Inc.)	0	0	0	1	0
My Calendar - Period Tracker (Simple Design Ltd.)	0	1	0	0	0
Pregnany Tracker (Amila)	0	0	0	0	0
Blood Pressure (K. Szymon)	0	0	0	0	0
Flo Ovulation & Period Tracker (Flo Health Inc.)	0	0	0	0	1
Health (Ada)	0	0	0	0	1
Home Workout - No Equipment (Leap fitness group)	0	0	0	0	0
Google Fit Activity Tracking (Google)	0	0	0	0	0
Ladytimer Ovulation Calendar (Vipos Apps)	0	0	0	0	0
Period and Ovulation Tracker (SMSROBOT LTD)	0	0	0	0	0
Ovia Pregnancy & Baby Tracker (Ovia)	0	0	1	1	1
Lose Weight App for Men (Leap fitness group)	0	1	0	0	0
30 days sixpack (Leap fitness group)	0	0	0	0	0
Summe	1	3	4	3	6

Untersuchte Apps	**Schweiz**	**Türkei**	**USA**	**Vereinigtes Königreich**
Pregnancy & Baby Tracker (Amma)	0	0	1	0
Sweatcoin (Sweatco Ltd)	0	0	1	0
Samsung Health (Samsung)	0	0	1	0
Zepp Life (Anhui Huami Information Technology Co. Ltd)	1	0	1	0
My Calendar (SimpleInnovation)	0	0	1	1
Medscape(WebMD,LLC)	1	0	1	0
MyTherapy (SmartPatient)	0	0	1	0
MyFitnessPal (MyFitnessPal, Inc.)	0	0	1	1
My Calendar - Period Tracker (Simple Design Ltd.)	0	0	1	0
Pregnany Tracker (Amila)	0	0	1	0
Blood Pressure (K. Szymon)	0	0	1	0
Flo Ovulation & Period Tracker (Flo Health Inc.)	0	0	1	0
Health (Ada)	0	1	1	0
Home Workout - No Equipment (Leap fitness group)	0	0	1	0
Google Fit Activity Tracking (Google)	0	0	1	0
Ladytimer Ovulation Calendar (Vipos Apps)	0	0	1	0
Period and Ovulation Tracker (SMSROBOT LTD)	0	0	1	0
Ovia Pregnancy & Baby Tracker (Ovia)	0	1	1	1
Lose Weight App for Men (Leap fitness group)	0	0	1	0
30 days sixpack (Leap fitness group)	0	0	1	0
Summe	2	2	20	3