24.04.2024, Version 1.1

Security & Privacy Report

Bezahlkarte für Geflüchtete

Auszug aus der Untersuchung derzeit vorliegender technischer Implementierungen zur Bezahlkarte

Autoren: Tim Philipp Schäfers / Niklas Klee

Dokumentenversion

Version	Autor	Datum	Kommentar
0.1	Tim Philipp Schäfers / Niklas Klee	02.04.2024	Initiale Version
0.2	Tim Philipp Schäfers / Niklas Klee	11.04.2024	Funde hinzugefügt
0.3	Tim Philipp Schäfers / Niklas Klee	15.04.2024	Weitere Funde hinzugefügt
0.4	Tim Philipp Schäfers / Niklas Klee	17.04.2024	Weitere Funde hinzugefügt
0.5	Tim Philipp Schäfers / Niklas Klee	19.04.2024	Weitere Funde hinzugefügt
1.0	Tim Philipp Schäfers / Niklas Klee	19.04.2024	Endversion 1.0 erstellt
1.1	Tim Philipp Schäfers / Niklas Klee	24.04.2024	Letzte Anpassung

Inhaltsverzeichnis

1. Einleitung / Zusammenfassung 5
2. Übersicht der Funde 6
3. Ziel, Architektur und Testvorgehen 8
3.1 Ziel der Untersuchung 8
3.2 Architektur von Bezahlkarten-Lösungen 8
3.3 Testparameter / Eingrenzung 9
3.4 Technische Analyse mit Fokus auf IT-Sicherheit 9
4. Funde pro Anbieter 11
4.1 Funde in Bezug auf die Socialcard 11
4.1.1 Nutzung von Funktionen auf der Website ausschließlich nach Einverständnis von Google ReCaptcha möglich (De-facto-Zwang) 12
4.1.2 Links in den Datenschutzbestimmungen teilweise fehlerhaft 14
4.1.3 Datenschutzerklärung auf der Webseite ausschließlich in Deutsch verfügbar 14
4.1.4 Secupay-App (als virtuelle SocialCard) enthält 11 Tracker, welche nach App-Start ohne Einwilligung Daten übermitteln (u.a. an Google und Facebook) 15
4.1.5 Datenschutzbestimmungen der Secupay-App (als virtuelle SocialCard) weisen keine der verwendeten Tracking-Bibliotheken aus 18
4.1.6 Weitreichende Zugriffsmöglichkeiten für die App (secupay-App) 19
4.1.7 Test-Cockpit für Gemeinden/Behörden verwendet Google Fonts 20
4.1.8 „mockCard“ in der HTTP-Response legt personenbezogene Informationen offen 22
4.1.9 Mögliches Subdomain Hijacking von intern.socialcard.de denkbar 23
4.1.10 Unzureichende Informationen über die Behandlung von Transaktionsdaten des Zahlungsdienstleisters Visa 24
4.2 Funde in Bezug auf die Bezahlkarte 25
4.2.1 Klartext Link auf meine.bezahlkarte.eu führt in App zu Fehler 26
4.2.2 Falsch gesetzter Link in der Bezahlkarten-App ermöglicht Anzeige beliebiger Inhalte innerhalb der App 27
4.2.3 Cross-Site-Scripting innerhalb der Anmeldeseite möglich 28
4.2.4 Datenschutzerklärung ausschließlich in Deutsch verfügbar 30
4.2.5 Testumgebung aus verlinkten Assets auslesbar und ermöglicht Informationspreisgaben 30
4.3 Funde in Bezug auf die givve® Card 32
4.3.1 Android App enthält Tracker-Bibliotheken und kontaktiert diese unmittelbar nach App-Start (ohne Einwilligung) 33
4.3.2 Verwendete Tracking-Bibliotheken werden nicht in den Datenschutzbestimmungen genannt 35
4.3.3 Weitreichende Zugriffsmöglichkeiten für die App 35
4.3.4 Datenschutzerklärung auf der Webseite ausschließlich in Deutsch verfügbar 36

Anhang A: Weiterführende Informationen zum Datenschutz in Bezug auf Bezahlkarten 37

1. Einleitung / Zusammenfassung

Nach mehrmonatiger Debatte hat die Ampel-Koalition eine Einigung im Rahmen der sogenannten „Bezahlkarte für Geflüchtete“ erzielt[1] und am 12.04.2024 im Bundestag eine Rechtsgrundlage für die bundeseinheitliche Bezahlkarte für Asylbewerber und Geflüchtete beschlossen[2]. Durch eine Änderung des Asylbewerberleistungsgesetzes soll es zukünftig möglich sein, Leistungen über eine sogenannte Bezahlkarte an Asylbewerber zu vergeben[3]. Die Bezahlkarte ist eine guthabenbasierte Karte mit Debit-Funktion. Einige Gemeinden, Städte und Bundesländer haben bereits vorab Lösungen in dem Bereich eingeführt oder Pilotprojekte durchgeführt, dazu gehören beispielsweise die Thüringer Landkreise Greiz und Eichsfeld, die Landeshauptstadt Hannover, die Stadt Leipzig, der Ortenaukreis, die Freie und Hansestadt Hamburg und folgende Regionen in Bayern: Landkreise Fürstenfeldbruck, Günzburg, Traunstein, kreisfreie Stadt Straubing [4] [5]. Die Lösungen stammen dabei von verschiedenen Anbietern. Neben einer physischen Karte ist für Asylsuchende ebenfalls die Nutzung einer virtuellen Bezahlkarte im Rahmen von Wallet-Apps möglich. Die Bezahlkarte wird dabei innerhalb einer App auf dem Smartphone gespeichert und kann mittels „mobile Payment“ genutzt werden. Die weitverbreitetsten Anbieter und ausgebenden öffentlichen Stellen bewerben aktiv diese Möglichkeit[6].
In der Debatte um die Bezahlkarte für Geflüchtete wurde in den letzten Monaten insbesondere auch das Thema der Diskriminierungsfreiheit diskutiert. Darüber hinaus hat es datenschutzrechtliche Betrachtungen durch verschiedene Stellen gegeben (weitere Details im Anhang A)[7].

„Digital. Bargeldlos. Sicher.“
Quelle: Socialcard Website https://www.socialcard.de/ (Abruf 17.04.2024)

„Nicht alles, was technisch möglich ist, wird vom geltenden Recht auch erlaubt.“
Quelle: Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/240223_Position_HmbBfDI_Bezahlkarte.pdf (Abruf 17.04.2024)

„Wir bieten Ihnen eine kurzfristige und sichere Umsetzung der Bezahlkarte […]“
Quelle: UP givve®
https://givve.com/de/oeffentlicher-sektor/bezahlkarte-fuer-leistungsempfaenger (Abruf 17.04.2024)

Im Rahmen einer Untersuchung konnten die IT-Sicherheitsexperten Tim Philipp Schäfers und Niklas Klee im April 2024 feststellen, dass bisherige technische Implementierungen der Bezahlkarten teils erhebliche Sicherheitslücken und Datenschutzverstöße aufweisen. **Zwei der weitverbreitetsten Anbieter übermittelt, ohne dass dies erkenntlich ist oder in den Datenschutzbestimmungen beschrieben wird, eindeutige, personenbeziehbare Geräte-IDs an Google und Facebook. Das Vorgehen stellt mutmaßlich einen Verstoß gegen die Datenschutzgrundverordnung (DSGVO) dar** und es ist eine zeitnahe Abhilfe erforderlich. Der folgende Bericht führt die Erkenntnisse und Informationen zu Schwachstellen weiter aus.

---

[1] https://www.tagesschau.de/inland/innenpolitik/bezahlkarte-fluechtlinge-einigung-100.html
[2] https://www.tagesschau.de/inland/innenpolitik/bundestag-bezahlkarte-asylbewerber-100.html
[3] https://www.bundesregierung.de/breg-de/service/gesetzesvorhaben/bezahlkarte-fluechtlinge-2263574
[4] https://www.deutschlandfunk.de/die-wichtigsten-fragen-und-antworten-zur-bezahlkarte-fuer-asylbewerber-100.html
[5] https://www.socialcard.de/
[6] Siehe beispielsweise Webseite des Anbieters Socialcard / Publk GmbH https://www.socialcard.de/ & Hinweis auf der Webseite der Stadt Hamburg: https://www.hamburg.de/socialcard
[7] https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/240223_Position_HmbBfDI_Bezahlkarte.pdf & https://www.proasyl.de/news/bezahlkarte-ohne-standards-laender-vereinbaren-diskriminierungskonzept/ & https://www.lto.de/recht/hintergruende/h/bezahlkarte-fluechtlinge-bargeld-taschengeld-asylrecht-hamburg-mindestandards/

2. Übersicht der Funde

Die Angaben zum Status sind gemeinsam mit den Anbietern erfasst worden (Stand: 24.04.2024).

Socialcard (Publk GmbH / secupay AG)

Mängel / Funde	Bereich	Auswirkung	Status
Nutzung von Funktionen auf der Website ausschließlich nach Einverständnis von Google ReCaptcha möglich (De-facto-Zwang)	Datenschutz	Gering	In Prüfung
Links in den Datenschutzbestimmungen teilweise fehlerhaft	Datenschutz	Gering	Geschlossen
Datenschutzerklärung auf der Webseite ausschließlich in Deutsch verfügbar	Datenschutz	Mittel	Geschlossen
Secupay-App (als virtuelle SocialCard) enthält 11 Tracker, welche nach App-Start ohne Einwilligung Daten übermitteln (u.a. an Google und Facebook)	Datenschutz	Sehr hoch	In Prüfung
Datenschutzbestimmungen der Secupay-App (als virtuelle SocialCard) weisen keine der verwendeten Tracking-Bibliotheken aus	Datenschutz	Hoch	In Prüfung
Weitreichende Zugriffsmöglichkeiten für die App (secupay-App)	Datenschutz / IT-Sicherheit	Mittel	In Prüfung
Test-Cockpit für Gemeinden/Behörden verwendet Google Fonts	Datenschutz	Mittel	Geschlossen
„mockCard“ in der HTTP-Response legt personenbezogene Informationen offen	Datenschutz	Gering	Geschlossen
Mögliches Subdomain Hijacking von intern.socialcard.de denkbar	IT-Sicherheit	Mittel	Geschlossen
Unzureichende Informationen über die Behandlung von Transaktionsdaten des Zahlungsdienstleisters Visa	Datenschutz	Mittel	In Prüfung

Bezahlkarte (PayCenter GmbH / petaFuel GmbH)

Mängel / Funde	Bereich	Auswirkung	Status
Klartext Link auf meine.bezahlkarte.eu führt in App zu Fehler	IT-Sicherheit	Gering	Geschlossen
Falsch gesetzter Link in der Bezahlkarten-App ermöglicht Anzeige beliebiger Inhalte innerhalb der App	IT-Sicherheit	Mittel	Geschlossen
Cross-Site-Scripting innerhalb der Anmeldeseite möglich	IT-Sicherheit	Sehr hoch	Geschlossen
Testumgebung aus verlinkten Assets auslesbar und ermöglicht Informationspreisgaben	Datenschutz/IT-Sicherheit	Gering	Geschlossen
Datenschutzerklärung ausschließlich in Deutsch verfügbar	Datenschutz	Mittel	In Prüfung

givve® Card (PL Gutscheinsysteme GmbH / Groupe Up)

Mängel / Funde	Bereich	Auswirkung	Status
Android App enthält Tracker-Bibliotheken und kontaktiert diese unmittelbar nach App-Start (ohne Einwilligung)	Datenschutz	Sehr hoch	In Prüfung
Verwendete Tracking-Bibliotheken werden nicht in den Datenschutzbestimmungen genannt	Datenschutz	Mittel	In Prüfung
Weitreichende Zugriffsmöglichkeiten für die App	Datenschutz/IT-Sicherheit	Mittel	In Prüfung
Datenschutzerklärung auf der Webseite ausschließlich in Deutsch verfügbar	Datenschutz	Mittel	In Prüfung

3. Ziel, Architektur und Testvorgehen

Die vorliegende Untersuchung bezieht sich auf konkrete technische Implementierungen, welche in der Form bereits bei den Pilotprojekten und Anbietern vorliegen. Diese Architektur wird im Regelbetrieb der Bezahlkarte für Asylsuchende in ähnlicher Form ebenfalls zum Einsatz kommen.

3.1 Ziel der Untersuchung

Ziel der vorliegenden Untersuchung ist es verbreitete Lösungen (insbesondere mobile Apps und Webapplikationen) zum Thema Bezahlkarte für Geflüchtete auf Mängel im Bereich IT-Sicherheit und Datenschutz zu prüfen und entsprechende Mängel festzuhalten. Die Mängel sollen nachvollziehbar protokolliert und dargestellt werden.

Die Mängel werden zudem nach Fund an die Betreiber bzw. Anbieter und möglicherweise Aufsichtsbehörden weitergeleitet, damit diese gemeinschaftlich auf eine Behebung der Mängel hinwirken und mögliche Betroffene informieren können. **Ziel ist es zu einer Stärkung des Schutzes von Daten (Datenschutz) beizutragen und für das Thema zu sensibilisieren.** Es ist nicht Ziel der vorliegenden Analyse eine politische Einordnung vorzunehmen.

3.2 Architektur von Bezahlkarten-Lösungen

Alle in diesem Bericht untersuchten Lösungen arbeiten folgendermaßen:

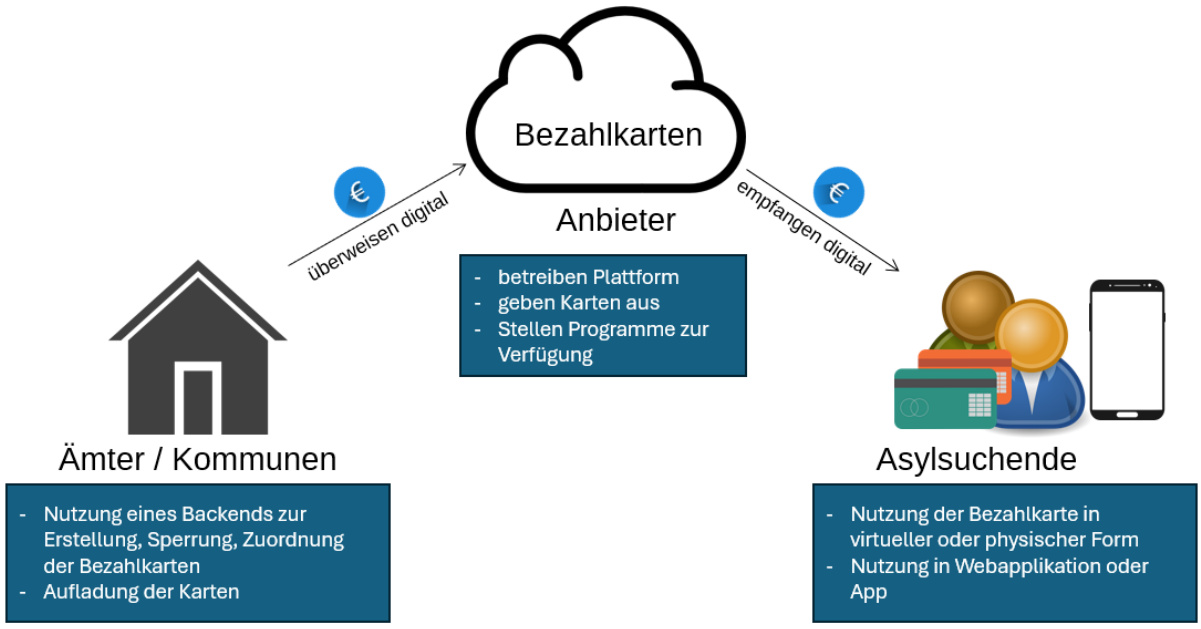


Abbildung 1: Schematische Darstellung der Architektur

Es gibt – der Architektur folgend – folgende Nutzergruppen, welche verschiedene Funktionen nutzen:

1.) Behörden (Sozialamt, etc.)

Mitarbeitende des Sozialamtes bzw. einer Behörde sind in der Lage über eine Webapplikation LeistungsempfängerInnen anzulegen, deren Stammdaten zu bearbeiten und Karten zuzuordnen, zu sperren und aufzuladen. Darüber hinaus gibt es die Möglichkeit administrative Accounts zu verwalten oder Restriktionen für die Karten zu konfigurieren (bspw. Beschränkung der Abhebungen, Eingrenzung auf Postleitzahlen oder ähnliches). Es handelt sich insoweit um die administrativen Funktionen für die jeweils zuständige Behörde.

2.) Anbieter / Betreiber

Die Anbieter der Bezahlkarten stellen die Plattform zur Verfügung, entwickeln diese weiter und geben (meist in Kooperation mit weiteren Unternehmen) die physischen und virtuellen Bezahlkarten aus. Darüber hinaus werden IBANs und Konten verwaltet.

3.) Asylsuchende (Leistungsbeziehende)

Die Asylsuchenden können nach Erhalt einer Karte durch eine Behörde diese zum Einkauf von Waren nutzen (es handelt sich um eine Prepaid Kreditkarte). Zudem gibt es die Möglichkeit per Webapplikation oder mobile App Zugriff auf Informationen zur Bezahlkarte zu nehmen (bspw. Einsicht des Kontostands, Übersicht über die Umsätze, etc.). Darüber hinaus können Nutzende in der Regel ihre Karten auch selbst sperren.

3.3 Testparameter / Eingrenzung

Die entsprechenden Tests wurden im März und April 2024 durchgeführt. Der vorliegende Test ist als Blackbox-Test zu betrachten, da kein Zugriff auf den Quellcode oder weitere Informationen des Systems vorlagen (vgl. Vorgehensweisen des BSI [8]). Während des Tests konnte zudem kein authentifizierter Zugriff erfolgen (da keine Logindaten vorlagen). Trotzdem waren bereits Datenschutzmängel und Sicherheitslücken feststellbar (bspw. nach Start der Apps / Abruf von Webapplikationen).

Untersuchungen sind nach den aktuellen Testing-Guides des Open Webapplication Security Projects (OWASP)[9] erfolgt.

3.4 Technische Analyse mit Fokus auf IT-Sicherheit

Neben einer statischen Analyse der App-Pakete (APK-Dateien) wurde auch eine Beobachtung am Smartphone und in Bezug auf die Netzwerkverbindungen und Anbieteranbindungen vorgenommen.

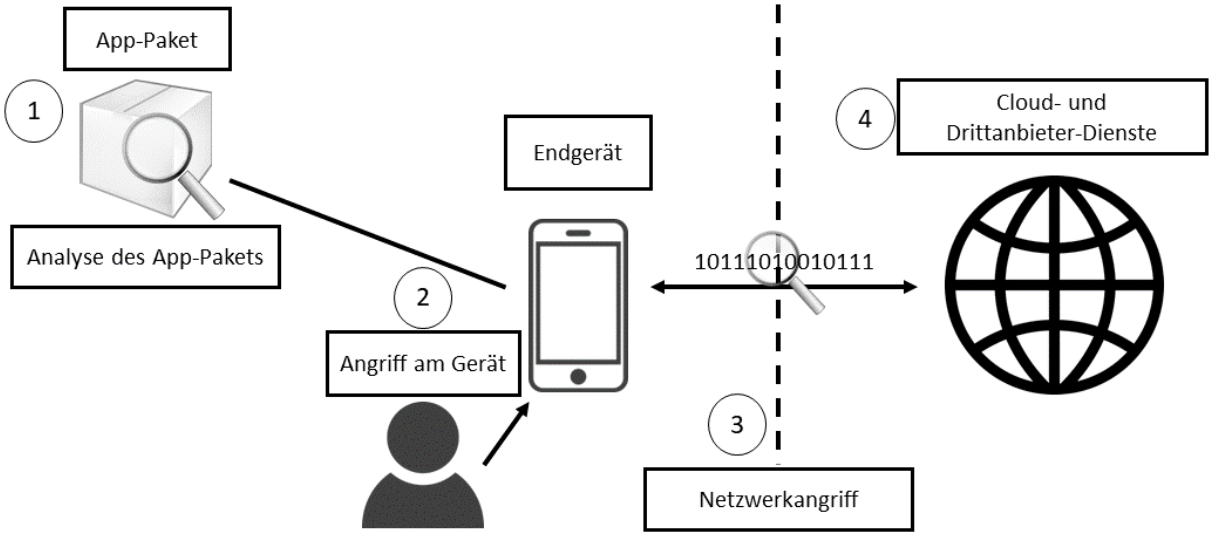


Abbildung 2: Angriffsmöglichkeiten bei der Nutzung von Apps (eigene Darstellung in Anlehnung an: Bundesamt für Sicherheit in der Informationstechnik (BSI), 2021, S. 39 [10])

[8] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/Penetrationstest/penetrationstest.pdf?__blob=publicationFile&v=3

[9] https://owasp.org/www-project-web-security-testing-guide/assets/archive/OWASP_Testing_Guide_v4.pdf & https://github.com/OWASP/owasp-mastg/releases/download/v1.7.0/OWASP_MASTG.pdf

[10] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/DVS-Berichte/gesundheitsapps.pdf?__blob=publicationFile&v=2

Die vorliegende Analyse stützt sich überwiegend auf die im Google Playstore verfügbaren Android Apps (auf die von den Anbieterwebsites oder von öffentlichen Stellen verwiesen wird). Eine Analyse der iOS (Apple) Apps ist in Planung, allerdings voraussichtlich aufwendiger. Es ist davon auszugehen, dass die Probleme auf Grund einer Cross-Plattform-Kompatibilität in ähnlicher Form auf bei iOS-Geräten vorliegen. Die Findings in Bezug auf Webserver / Webapplikationen sind zudem als plattformunabhängig zu betrachten.

3.5 Analyse in Bezug auf den Datenschutz

Zur Betrachtung des Bereiches Datenschutz wurden Erkenntnisse aus der technischen Analyse herangezogen, beispielsweise die kontaktierten URLs oder verwendete Tracking Bibliotheken. Anschließend wurde anhand der vorliegenden Datenschutzbestimmungen (innerhalb der Apps oder Verlinkung im Google Play Store) geprüft, ob dieses Verhalten in der vorliegenden Form beschrieben wird oder ob es Abweichungen gibt.

Darüber wurde innerhalb der Apps, beispielsweise mit Hilfe der sogenannten App-Manifest-Datei, geprüft welche Berechtigungen und Konfigurationen vorliegen und wie diese unter dem Gesichtspunkt des Datenschutzes zu bewerten sind.

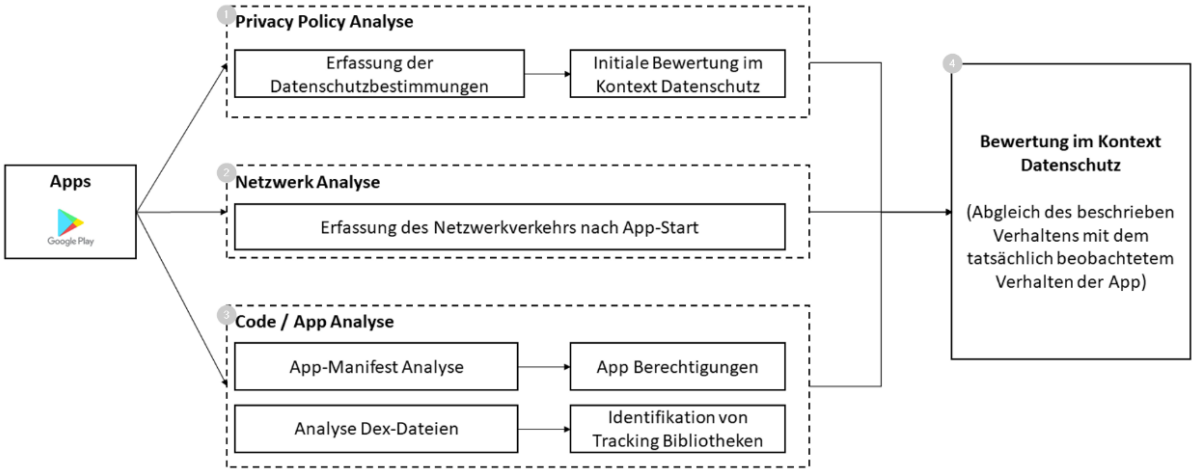


Abbildung 3: Vorgehensweise zur Analyse des Datenschutzes (eigene Darstellung in Anlehnung an Kollnig, et al., 2021 [11])

[11] Kollnig, K., Dewitte, P., Van Kleek, M., Wang, G., Omeiza, D., Webb, H., & Shadbolt, N. (9. August 2021). A Fait Accompli? An Empirical Study into the Absence of Consent to Third-Party Tracking in Android Apps. USENIX - SOUPS 2021, S. 181-196.

4. Funde pro Anbieter

Im Folgenden werden alle Funde pro Anbieter aufgeführt (siehe unter anderem Limitierungen im Rahmen des Testings im Kapitel zuvor).

4.1 Funde in Bezug auf die Socialcard

Nachfolgend werden Funde in Bezug auf die Socialcard von den Anbietern Publk GmbH / secupay AG detailliert beschrieben. Die Kenntnisse stützen sich dabei auf die aktuelle Version der Webapplikation (17.04.2024) und die neuste Version der Android-App (9.27.00 vom 07.02.2024, neuste Version zum Zeitpunkt des initialen Berichtes).

Lösungsname	SocialCard
Logo des Anbieters / App	(entnommen von: https://www.socialcard.de/) (entnommen von: https://play.google.com/store/apps/details?id=com.secupay)
Anbieter	Publk GmbH / secupay AG
Kreditkarten-Anbieter	Visa
Website	https://www.socialcard.de/
Name der App	secupay
URL zur App (Play Store)	https://play.google.com/store/apps/details?id=com.secupay
Version (zum Zeitpunkt des Tests)	9.27.00
APK SHA-256	5BCF9A19E295C616F6023CFE83C4FFE7DE1F0DBAE12F4D3DDE0F8F91B99582DA
URL zur App (App Store)	https://apps.apple.com/de/app/6443697026
Privacy Policy im App-Store	https://secupay.com/agb/secupay-app-datenschutzbestimmungen
Pilotprojekte (Stand 15.04.2024, laut öffentlich zugänglichen Informationen)	Landeshauptstadt Hannover, Stadt Leipzig, Der Ortenaukreis, Freie und Hansestadt Hamburg, Landkreis Schmalkalden-Meiningen, Ortennau Kreis, Landkreis Nordhausen, Landkreis Konstanz, Magdeburg, Kyffhäuserkreis, Landkreis Erzgebirge, Landkreis Göttingen, Landkreis Sömmerda, Landkreis Waldshut, Rhein-Pfalz-Kreis, Zollernalbkreis, Altenburger Land, Hildburghausen, Ilm Kreis

4.1.1 Nutzung von Funktionen auf der Website ausschließlich nach Einverständnis von Google ReCaptcha möglich (De-facto-Zwang)

Klasse	Datenschutz
Auswirkung	Gering

Zur Nutzung der Website bzw. wichtigen Funktionen der Socialcard (bspw. Ablesen des Guthabens) ist es erforderlich, dass Besuchende Cookies von dem Drittanbieter „Google Ireland Limited“ akzeptieren.

Es handelt sich dabei um Cookies zur Nutzung des Dienstes „ReCaptcha“ (von Google), welcher Zugriffe durch Bots auf die Seite einschränken soll.

Durch die vorliegende Umsetzung liegt ein **De-facto-Zwang** vor: Nutzenden ist es nicht möglich wichtige Funktionen der Website bzw. Bezahlkarte zu nutzen, ohne, dass Daten an Dritte übermittelt werden.

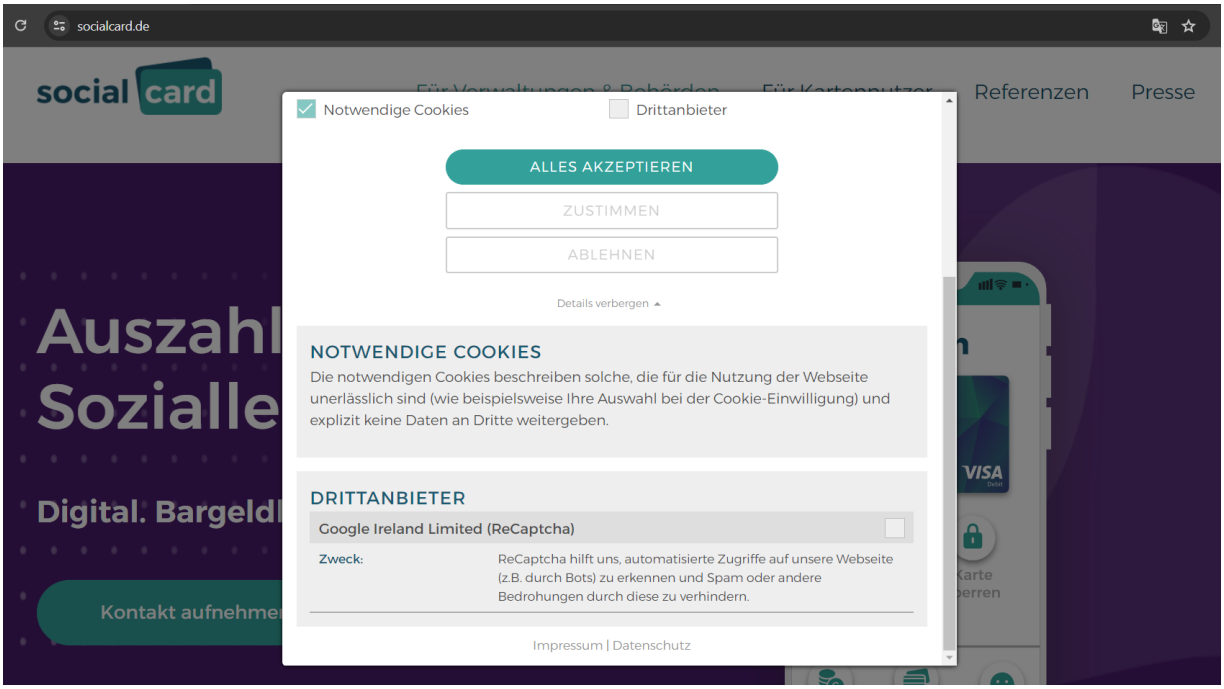


Abbildung 4: Aufforderung in Form eines Cookie-Banners bei Erstbesuch

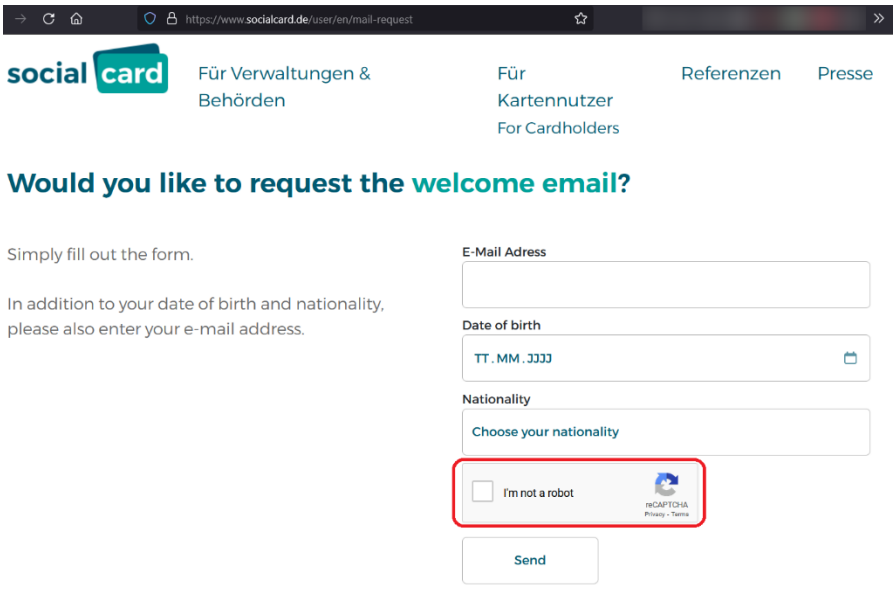
Besuchende von socialcard.de haben die Möglichkeit auszuwählen, ob sie „Alles akzeptieren“ (damit alle Cookies annehmen), ausschließlich ausgewählten Cookies zustimmen mittels „Zustimmen“ oder „Ablehnen“.

Es ist positiv hervorzuheben, dass genau erläutert wird welchen Zweck die Cookies haben, es wird allerdings keine Laufzeit ausgewiesen (dies könnte eine informierte Entscheidung begünstigen).

Alle der folgenden Funktionen erfordern eine Akzeptanz des „Google Ireland Limited (ReCaptcha)“-Cookie:

Abbildung 5: Kartenfunktionen, welche Zustimmung benötigen

Eine Einbettung von ReCaptcha sieht folgendermaßen aus. Bei dieser Verwendung werden Daten zu Google geschickt. In diesem Beispiel erfolgt auch die Erfassung der Nationalität eines Karteninhabers.



Anmerkung / Empfehlung

Eine Einwilligung muss nach Artikel 7 der DSGVO informiert, freiwillig, aktiv und vor der eigentlichen Übermittlung von Daten erfolgen[12]. Die Freiwilligkeit könnte im vorliegenden Fall bezweifelt werden, da sonst keine Nutzbarkeit vorliegt (und auch mittels App Datenschutz-Probleme vorliegen, siehe unten). Auch die Informiertheit könnte verbessert werden (bspw. durch Nennung der Cookie Laufzeit). Das Blockieren mittels CAPTCHA ist sinnvoll (unter Betrachtung der IT-Sicherheit), allerdings sollte ein self-hosted CAPTCHA betrieben werden, um keinen Zwang zur Übertragung an Dritte zu implementieren, wenn Funktionen genutzt werden (im Bereich Schriftarten wurde dies berücksichtigt).

[12] Vgl. https://www.baden-wuerttemberg.datenschutz.de/faq-zu-cookies-und-tracking-2/

4.1.2 Links in den Datenschutzbestimmungen teilweise fehlerhaft

Klasse	Datenschutz
Auswirkung	Gering

Auf der Webseite von socialcard.de werden in der Datenschutzerklärung (verfügbar über https://www.socialcard.de/datenschutz) Links verwendet. Mindestens zwei dieser Links sind fehlerhaft bzw. nicht korrekt angegeben und erschweren es somit Besuchende weitere Informationen zur Verarbeitung ihrer Daten zu erhalten.

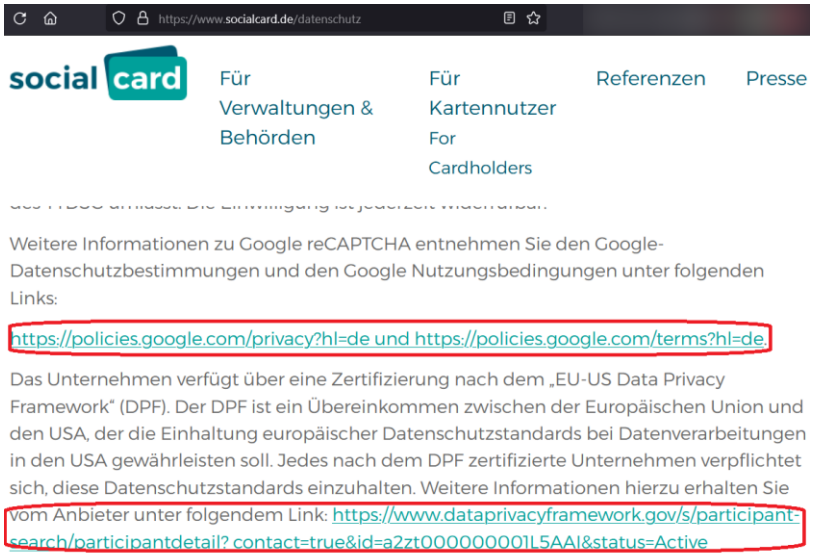


Abbildung 6: Fehlerhafte Links in der Datenschutzerklärung

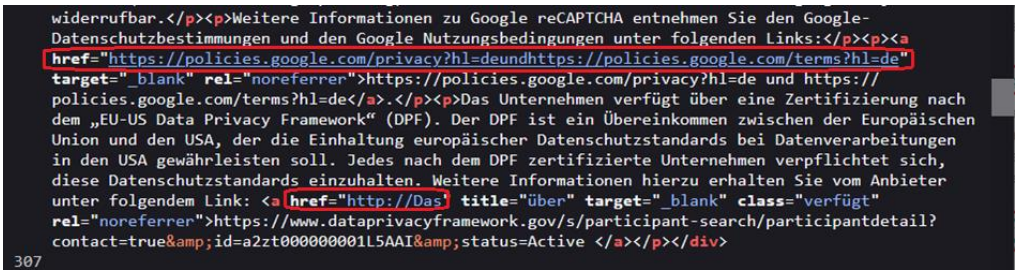


Abbildung 7: Fehlerhafte Link in der HTML-Ansicht

Anmerkung / Empfehlung

Die entsprechenden Links sollten neu gesetzt werden und auf die jeweils gewünscht Seite führen. Darüber hinaus sollten Links regelmäßig geprüft werden, um eine korrekte Verlinkung sicherzustellen.

4.1.3 Datenschutzerklärung auf der Webseite ausschließlich in Deutsch verfügbar

Klasse	Datenschutz
Auswirkung	Mittel

Die Datenschutzerklärung auf der Website (verfügbar über https://www.socialcard.de/datenschutz) ist ausschließlich in Deutsch verfügbar. Es gibt keine Möglichkeiten auf der Webseite eine übersetzte Version der Datenschutzerklärung einzusehen, was eine informierte Entscheidung für Betroffene erschwert.

Anmerkung / Empfehlung

Insbesondere unter Berücksichtigung des Nutzendenkreises empfiehlt es sich zumindest auch eine englischsprachige Version der Datenschutzerklärung anzubieten.

4.1.4 Secupay-App (als virtuelle SocialCard) enthält 11 Tracker, welche nach App-Start ohne Einwilligung Daten übermitteln (u.a. an Google und Facebook)

Klasse	Datenschutz
Auswirkung	Sehr hoch

Die Secupay-App wird vom Anbieter selbst[13] und öffentlichen Stellen (bspw. der Stadt Hamburg[14]) als zu nutzendes Wallet beschrieben.

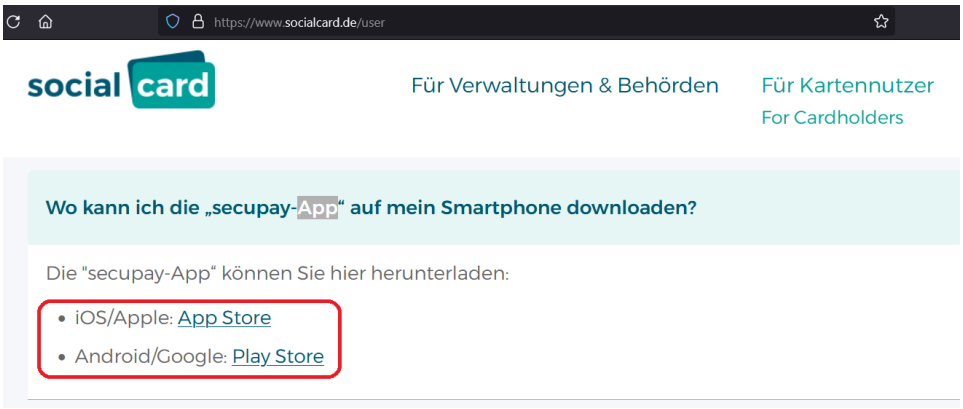


Abbildung 8: Verweis des Anbieters SocialCard auf die "secupay-App"

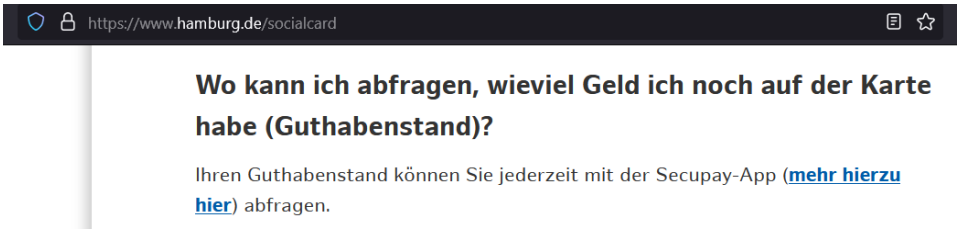
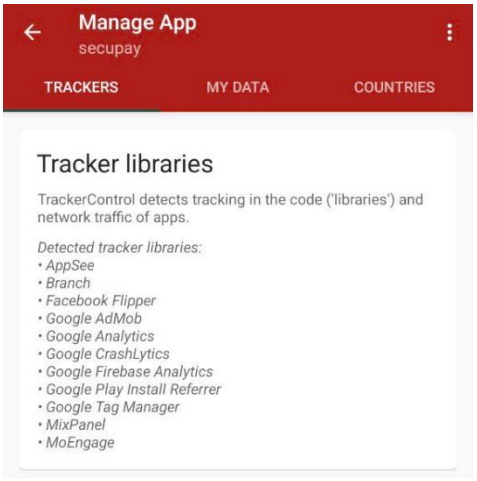


Abbildung 9: Hinweis auf die secupay-App auf hamburg.de

Die App enthält mindestens folgende Tracking-Bibliotheken[15]:

- **AppSee**
- **Branch**
- **Facebook Flipper**
- **Google AdMob**
- **Google Analytics**
- **Google CrashLytics**
- **Google Firebase Analytics**
- **Google Play Install Referrer**
- **Google Tag Manager**
- **Mix Panel**
- **MoEngage**



Keine dieser Tracking-Bibliotheken wird in den Datenschutzbestimmungen zur secupay-App[16] transparent genannt (siehe dazu nächstes Finding).

---

[13] https://www.socialcard.de/user
[14] https://www.hamburg.de/socialcard
[15] Die Analyse wurde mit dem Tool „Tracker Control“ (https://trackercontrol.org/) durchgeführt und manuell durch Analyse der APK-Datei verifiziert.
[16] https://secupay.com/agb/secupay-app-datenschutzbestimmungen (Stand: 15.04.2024)

Nach einer Installation auf einem Android Gerät[17] kann die App gestartet werden, unmittelbar nach App-Start (ohne weitere Einwilligungen) werden Verbindungen zu zahlreichen Servern hergestellt und Daten übermittelt:

Kategorie	Tracker	Kontaktierte URLs
Advertising	Branch	api.branch.io / cdn.branch.io
Analytics	Mixpanel	api.mixpanel.com
Analytics	Google	firebase-settings.crashlytics.com
Analytics	Google	www.googletagmanager.com
E-Mail	MoEngage	sdk-02.moengage.com
Essential	Google	firebaseappmessaging.googleapis.com
Fingerprinting	Google	www.google-analytics.com
Social	Facebook	graph.facebook.com

Durch verschiedene Tracker innerhalb der secupay-App werden eindeutige personenbeziehbare Merkmale (beispielsweise die Google Advertising-ID oder eindeutige Gerätekennungen) an dritte Stellen übermittelt (diese Stellen werden an keiner Stelle erwähnt / noch wurde eingewilligt). Das beschriebene Verhalten kann dazu dienen Nutzende eindeutig zu identifizieren und Profile zu Anwendenden zu erstellen. Das Vorgehen dazu wird im folgenden Schaubild exemplarisch dargestellt:

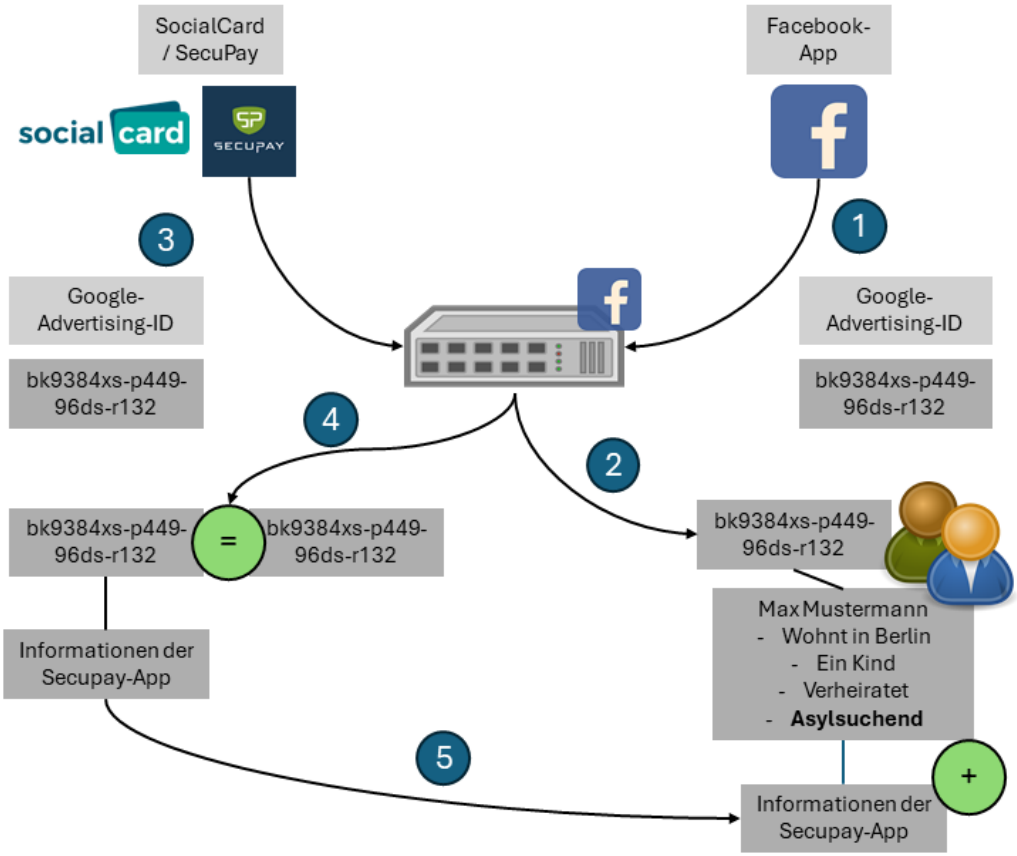


Abbildung 10: Exemplarische Darstellung zur Bildung von Profilen mittels Tracking über Google Advertising-IDs[18]

[17] Es ist naheliegend, dass dieses Verhalten auch auf iOS-Geräten vorliegt, da in Teilen plattformübergreifend gearbeitet wird. Aktuell wird dies noch verifiziert. (Stand: 15.04.2024).

[18] In Anlehnung an: https://www.kuketz-blog.de/wie-tracking-in-apps-die-sicherheit-und-den-datenschutz-unnoetig-gefaehrdet/ Es wurden Anpassungen für den vorliegenden Fall vorgenommen.

Die Übermittlung der Google-Advertising-ID genügt, dass Facebook eine Verknüpfung zwischen Facebook-NutzerIn und den übermittelten Daten herstellen kann. Der Grund: Auch die Facebook-App (sofern installiert) oder andere Apps lesen die Google-Advertising-ID ebenfalls aus. Damit hat Facebook anschließend einen Identifier, den sie einer Person exakt zuordnen können. Mit dem Server „graph.facebook.com“ kommuniziert die App im Verlauf der App-Nutzung regelmäßig – auch wenn man überhaupt kein Facebook-Konto hat. Facebook erfährt also unter anderem, in welcher View (Ansicht in der App) sich die Nutzerin gerade befindet [19].

Die Permissions der App ermöglichen darüber hinaus Trackern Zugriff auf viele Informationen/Schnittstellen:

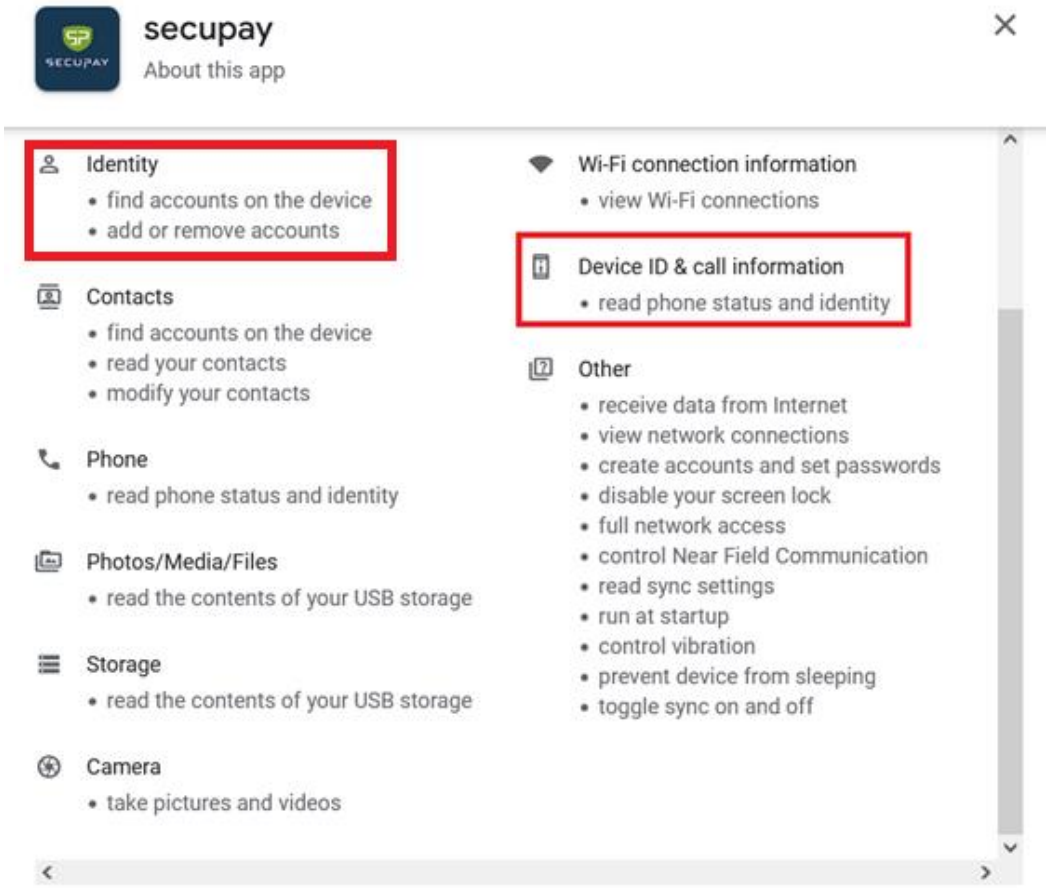


Abbildung 11: Zugriffsmöglichkeiten laut Play Store (Quelle: https://play.google.com/store/apps/details?id=com.secupay)

Anmerkung / Empfehlung

Es empfiehlt sich eingebaute Tracking-Bibliotheken auf das absolute Minimum zu beschränken und innerhalb der Tracking-Bibliotheken zudem stark zu regulieren welche Daten erfasst werden. Im vorliegenden Fall sind überdurchschnittlich viele Tracking-Bibliotheken eingebaut und senden aktiv personenbeziehbare Daten an Dritte ohne Einwilligung oder Information, dies stellt mutmaßlich einen Verstoß gegen die DSGVO dar.

Darüber hinaus ist zumindest über Tracking und die dabei verwendeten Dienst zu informieren (bspw. durch ein Pop-Up bei Erstnutzung oder in den Datenschutzbestimmungen). Darüber hinaus sollte eine eindeutige Einwilligung vorliegen – das ist in den letzten Fällen eindeutig nicht der Fall.

[19] Die Vorgehensweise wird auch hier beschrieben (Quelle des Vorgehens / Formulierung): https://www.kuketz-blog.de/wie-tracking-in-apps-die-sicherheit-und-den-datenschutz-unnoetig-gefaehrdet/

4.1.5 Datenschutzbestimmungen der Secupay-App (als virtuelle SocialCard) weisen keine der verwendeten Tracking-Bibliotheken aus

Klasse	Datenschutz
Auswirkung	Hoch

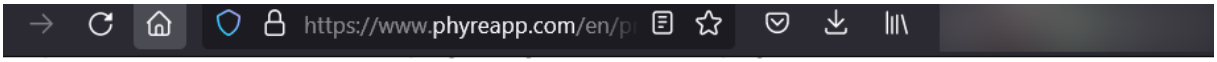
Wie im Fund zuvor beschrieben weist die secupay-App zahlreiche Tracking-Bibliotheken auf:

- **AppSee**
- **Branch**
- **Facebook Flipper**
- **Google AdMob**
- **Google Analytics**
- **Google CrashLytics**
- **Google Firebase Analytics**
- **Google Play Install Referrer**
- **Google Tag Manager**
- **Mix Panel**
- **MoEngage**

Keine dieser Tracking-Bibliotheken wird in den Datenschutzbestimmungen zur secupay-App[20] oder auf socialcard.de transparent genannt. Durch die Nichtnennung kann keine informierte Entscheidung erfolgen, darüber hinaus findet eine ungewollte Weiterleitung von Informationen an Dritte statt.

Die secupay-App scheint auf der sogenannten „phyreapp“-App eines bulgarischen Unternehmens aufzubauen[21], dies ist erkennbar anhand von Informationen in der AndroidManifest.xml-Datei und weiteren Informationen aus der APK-Datei.

Bei der ursprünglichen App werden die Verbindungen und Tracking-Bibliotheken erwähnt (auch wenn die Informationen unzureichend sind)[22]:



- Phyre app use Firebase, Google Analytics, Crashlytics, Mixpanel, MoEngage and Intercom to collect information regarding the use of the mobile application by the users in order to improve the user experience.

Anmerkung / Empfehlung

Es empfiehlt sich Tracking-Bibliotheken in den Datenschutzbestimmungen zu erwähnen und ausführlich zu beschreiben (Welche Tracking-Bibliotheken gibt es? Welchen Zweck verfolgen sie? Welche Daten werden dabei erfasst und übermittelt? Kann man der Erfassung widersprechen und welche Folgen hat das? etc.). Alternativ sollte man einen Großteil der Tracking-Bibliotheken ausbauen.

[20] https://secupay.com/agb/secupay-app-datenschutzbestimmungen
[21] Siehe: https://www.phyreapp.com/ des bulgarischen Unternehmens: Paynetics AD bzw. phyre JSC
[22] https://www.phyreapp.com/en/privacy-policy (Abruf: 15.04.2024)

4.1.6 Weitreichende Zugriffsmöglichkeiten für die App (secupay-App)

Klasse	Datenschutz / IT-Sicherheit
Auswirkung	Mittel

Mittels Analyse der AndroidManifest.xml Informationen aus der APK-Datei lässt sich ermitteln welche Berechtigungen (Permission) der App auf einen Android Smartphone eingeräumt wird.

AndroidManifest.xml

```
<?xml version="1.0" encoding="utf-8"?>
<manifest
    xmlns:android="http://schemas.android.com/apk/res/android"
    android:versionCode="9270003"
    android:versionName="9.27.00"
    android:compileSdkVersion="33"
    android:compileSdkVersionCodename="13"
    package="com.secupay"
    platformBuildVersionCode="33"
    platformBuildVersionName="13">
```

Abbildung 12: Beginn der AndroidManifest.xml-Datei

Auch nach der Installation der App auf einem Android Telefon lassen sich die Permissions (Berechtigungen) einsehen.

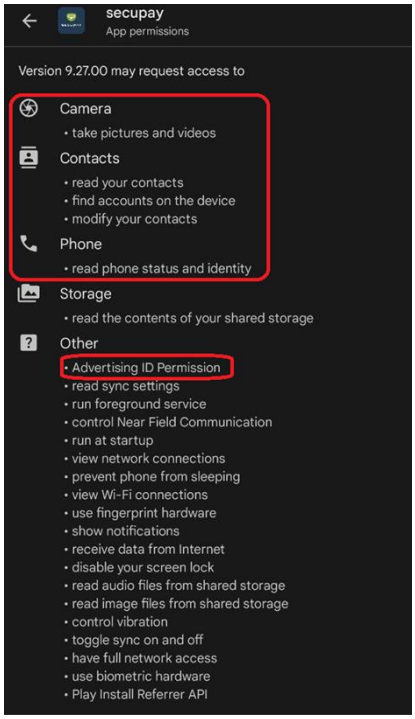


Abbildung 13: Permissions nach der Installation auf einem Android-Smartphone

Insbesondere bei den rot markierten Permissions (bspw. Kamera-Funktion, Advertising ID Permission oder Kontakte auslesen) ist unklar, weshalb diese überhaupt für die App und ihren Nutzungszweck erteilt werden müssen. Auch die sonstigen Permissions legen den Eindruck nahe, dass diese für den engeren Nutzungszweck der App nicht erforderlich sind.

Anmerkung / Empfehlung

Es sollte geprüft werden, welche Permissions tatsächlich benötigt werden. Die Permissions sollten sich auf das notwendige Minimum (Datenminimierung nach DSGVO) beschränken und genau zugewiesen werden.

4.1.7 Test-Cockpit für Gemeinden/Behörden verwendet Google Fonts

Klasse	Datenschutz
Auswirkung	Mittel

Über die sogenannten Certificate Transparency Logs[23] lassen sich ausgestellte Zertifikate für Domains prüfen. Prüft man diese Domains für socialcard.de[24], so lassen sich einige Subdomains herausfinden.

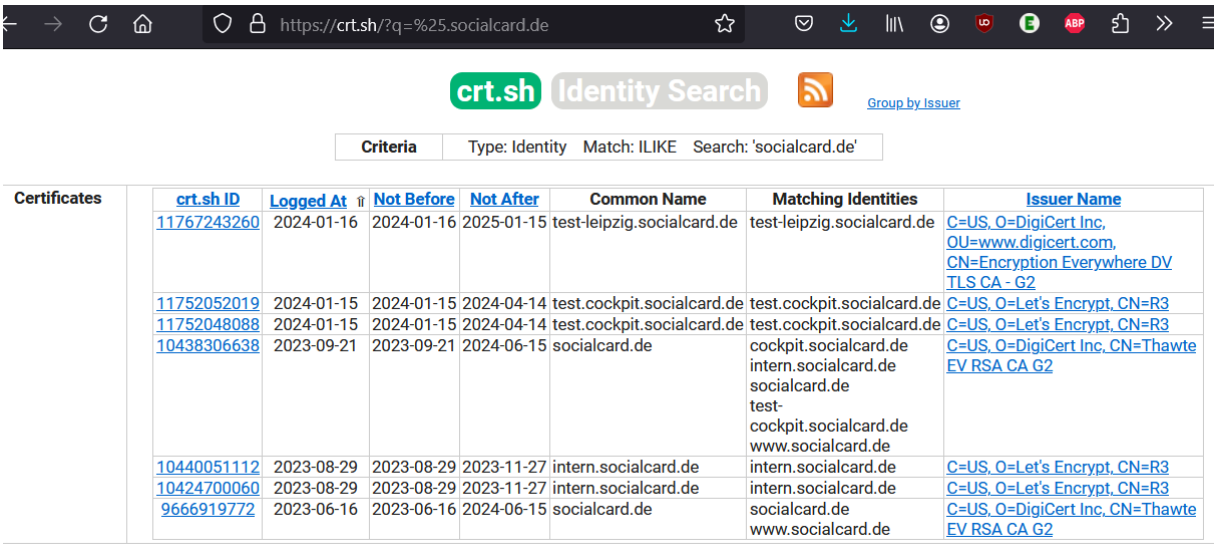


Abbildung 14: Subdomains für socialcard.de

Anhand der gefundenen URLs lässt sich feststellen, dass u.a. das sogenannte Cockpit ausgewiesen wird. Dabei handelt es sich um die Backend-Funktionen, die von den öffentlichen Stellen (Gemeinden/Kommunen bzw. den zuständigen Sozialämtern) genutzt werden kann.

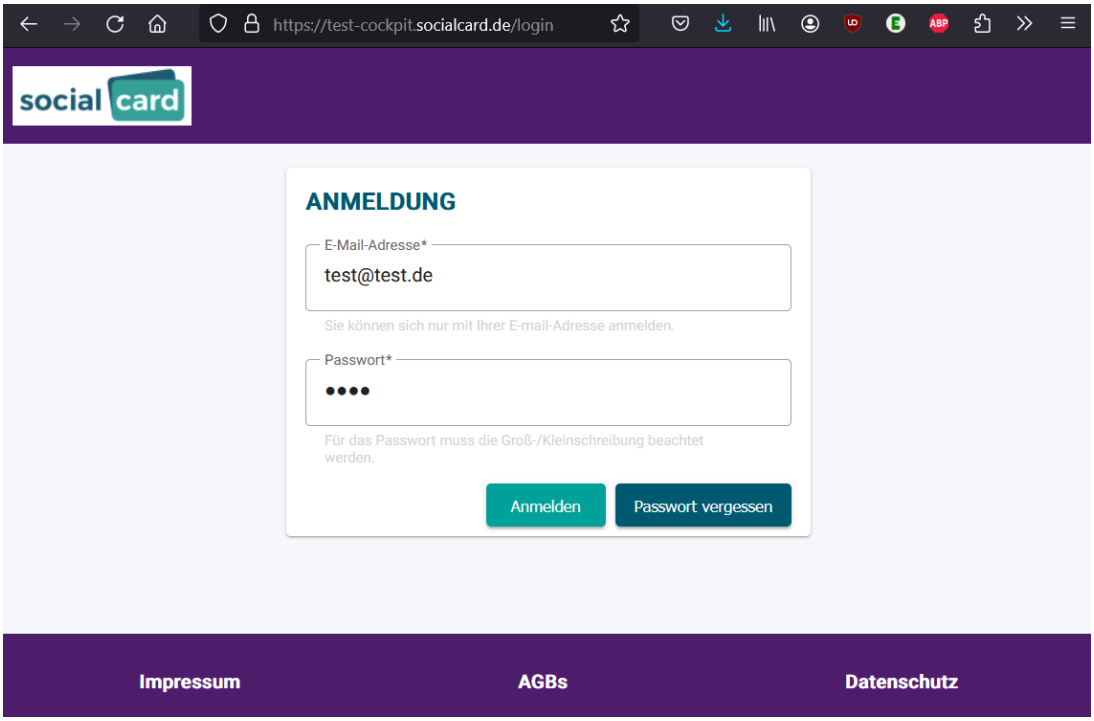


Abbildung 15: Test Cockpit von Socialcard

[23] https://de.wikipedia.org/wiki/Certificate_Transparency
[24] Dies ist bspw. hier möglich: https://crt.sh/?q=%25.socialcard.de

Wie erkennbar ist, liegt an der betreffenden Stelle eine Loginmöglichkeit vor (offensichtlich handelt es sich um ein test-System, da Test in der URL steht). Schaut man sich den Quelltext der betreffenden Seite an, so ist erkennbar, dass Google Fonts geladen werden.

Abbildung 16: Google Fonts innerhalb der Cockpit-Test Webseite

Bei jedem Aufruf der Seite wird (sofern die Schriftarten nicht im Cache enthalten sind) eine Verbindung zu Google Servern eröffnet und Schriftarten nachgeladen. In den Datenschutzbestimmungen der Socialard[25] wird erwähnt, dass dies explizit nicht der Fall ist:

Weitere Hinweise zu Verarbeitungsprozessen, Verfahren und Diensten:

- **Google Fonts (Bereitstellung auf eigenem Server):** Bereitstellung von Schriftarten-Dateien zwecks einer nutzerfreundlichen Darstellung unseres Onlineangebotes
- **Dienstanbieter:** Die Google Fonts werden auf unserem Server gehostet, es werden keine Daten an Google übermittelt

Abbildung 17: Auszug aus den Datenschutzbestimmungen zu Google Fonts

Auch in möglichen Datenschutzbestimmungen zum Cockpit selbst findet keine Erwähnung der Google Fonts und den Verbindungen zu Google statt. Da es sich um ein Testsystem für das Cockpit handelt ist naheliegend, dass in den produktiven Systemen für das Cockpit (die offenbar durch zusätzliche Maßnahmen abgeschirmt sind) ebenfalls Google Fonts von Google Systemen verwendet werden. In einem solchen Fall würde bei jedem Abruf durch ein Amt/Behörde auch eine Verbindung an Google erfolgen.

Bei den geladenen Daten handelt es sich um Schriftart-Dateien, welche von einem Server des Unternehmen Google (Alphabet Inc.) geladen werden. Bei Abruf dieser Schriftarten werden Nutzerdaten, darunter auch die IP-Adresse, an Google übertragen. Nach dem Urteil des Landgericht München I, Urteil vom 20.01.2022, Az. 3 O 17493/20 stellt dies (ohne Einwilligung) einen Verstoß gegen die Datenschutzgrundverordnung (DSGVO) dar[26].

Anmerkung / Empfehlung

Die Google Fonts sollten – wie auf der generellen socialcard.de-Applikation – direkt von den eigenen Servern geladen werden und nicht von Google Systemen. Sofern dies nicht möglich ist, sollte mittels Cookie-Banner eine Information erfolgen und eine Einwilligung eingeholt werden. Die betroffenen Personen sollten darüber stets informiert werden (u.a. per Cookie-Banner und innerhalb der Datenschutzbestimmungen).

[25] https://www.socialcard.de/datenschutz
[26] https://rewis.io/urteile/urteil/lhm-20-01-2022-3-o-1749320/

4.1.8 „mockCard“ in der HTTP-Response legt personenbezogene Informationen offen

Klasse	Datenschutz / IT-Sicherheit
Auswirkung	Gering

Bei Abruf des Testcockpits unter „test-cockpit.socialcard.de“ wird eine Datei mit dem Namen „main.5f0794d6ad371033.js“ geladen (Abruf unter: https://test-cockpit.socialcard.de/main.5f0794d6ad371033.js). Diese Datei weist eine sogenannte „mockCard“ aus, durch welche gut nachvollziehbar ist welche Dateien verarbeitet werden. Die Daten enthalten Echtdaten des mutmaßlichen Entwicklers (bei Suche nach dem Namen innerhalb von LinkedIn findet man einen Angular Developer). Dass die Applikation in Angular geschrieben ist, lässt sich unter anderem am Favicon erkennen.

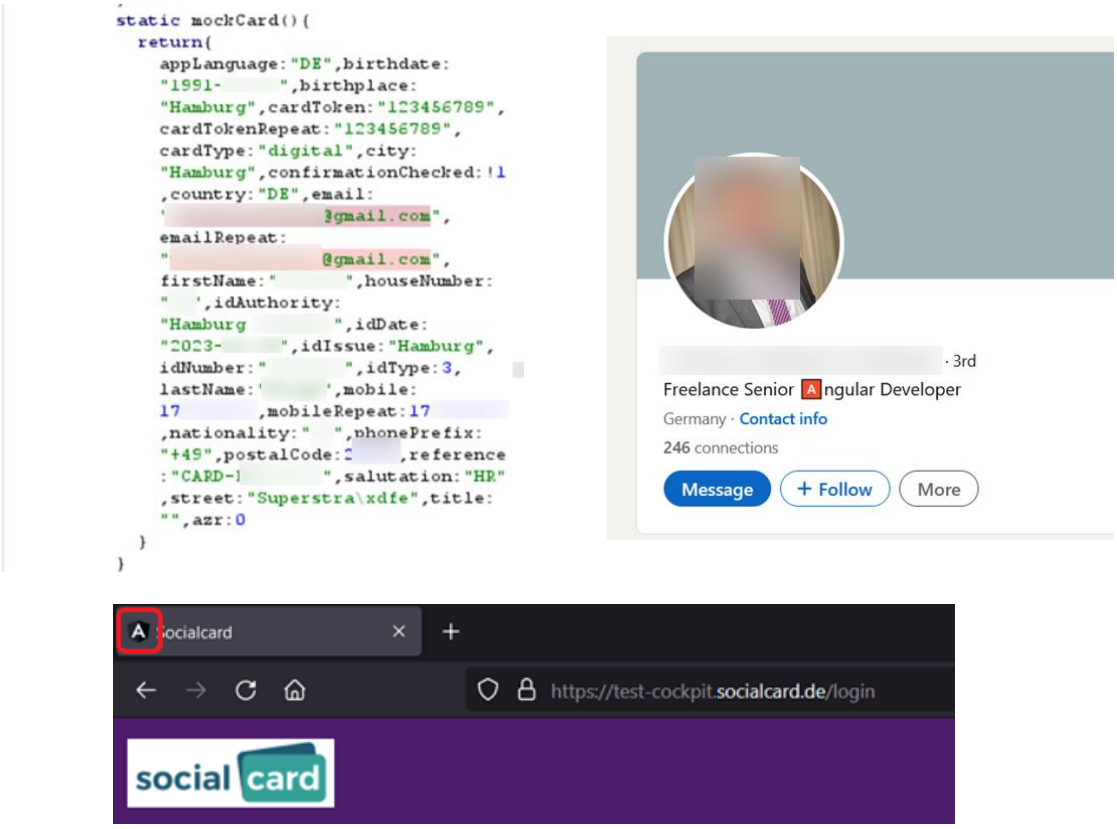


Abbildung 18: Informationen zur mockCard, dem Entwickler und dem Favicon mit Angular Icon

Anmerkung / Empfehlung

Personenbezogene Informationen und Testdaten sollten nicht ohne Authentifizierung abrufbar sein. Es empfiehlt sich diese Testdaten zu entfernen und den Eingriff auf das Test-Cockpit (wie auf die produktiven Cockpits) zu begrenzen, bspw. durch Allow-Listing.

4.1.9 Mögliches Subdomain Hijacking von intern.socialcard.de denkbar

Klasse	IT-Sicherheit
Auswirkung	Mittel

Über die sogenannten Certificate Transparency Logs[27] lassen sich ausgestellte Zertifikate für Domains prüfen. Prüft man diese Domains für socialcard.de[28], so lassen sich einige Subdomains herausfinden, u.a. auch die Subdomain intern.socialcard.de. Diese verweist – mittels DNS-Eintrag - auf eine Applikation des Dienstleisters Freshdesk (podeucentral1route.freshdesk.com [18.193.167.198]).

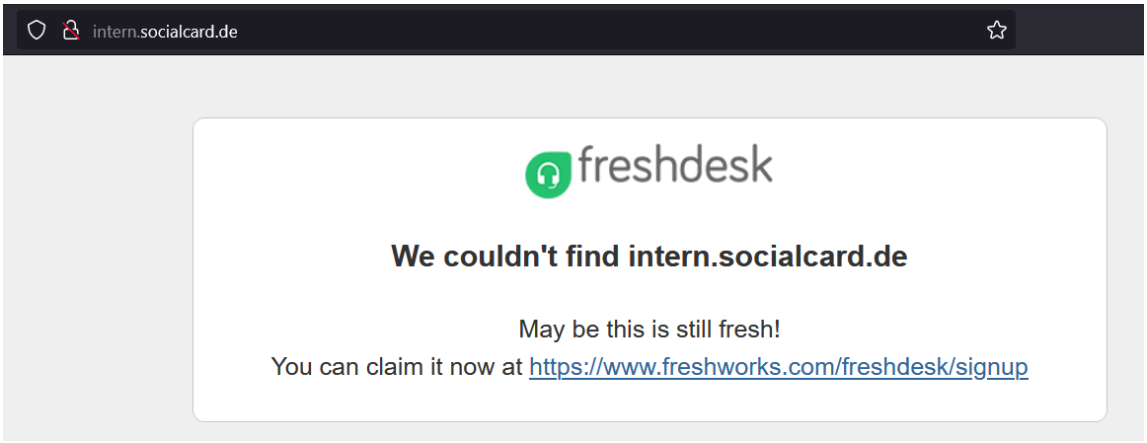


Abbildung 19: Freshdesk Seite unter intern.socialcard.de

Offensichtlich werden Supportmaßnahmen über Freshdesk abgebildet. Hinweise darauf finden sich auch in den Datenschutzbestimmungen[29].

Abbildung 20: Informationen zu Freshdesk in den Datenschutzbestimmungen

Im Text der Seite steht „We couldn't find intern.socialcard.de" was darauf hindeutet, dass die Domain innerhalb von Freshdesk nicht „geclaimt" wurde. Es gibt Berichte und Videos dazu, in denen Dritte darstellen, wie man nicht „geclaimte" URLs von Freshdesk übernehmen kann[30].

Anmerkung / Empfehlung

Es sollte geprüft werden, ob ein Claim vorliegt. Ist dies nicht der Fall, sollte dieser entweder vorgenommen werden oder der DNS-Eintrag bereinigt werden (sofern dies nicht notwendig ist).

---

[27] https://de.wikipedia.org/wiki/Certificate_Transparency
[28] Dies ist bspw. hier möglich: https://crt.sh/?q=%25.socialcard.de
[29] https://www.socialcard.de/datenschutz
[30] Vgl. https://www.youtube.com/watch?v=eph0PaccRP0 / https://github.com/EdOverflow/can-i-take-over-xyz/issues/71

4.1.10 Unzureichende Informationen über die Behandlung von Transaktionsdaten des Zahlungsdienstleisters Visa

Klasse	Datenschutz
Auswirkung	Mittel

Im Rahmen der Analyse konnte festgestellt werden, dass innerhalb der Datenschutzbestimmungen auf der Webseite von Socialcard[31] und innerhalb der aktuellen Nutzungsbedingungen zur Socialcard[32] keine Informationen zur Datenverarbeitung bei der Durchführung von Transaktionen gemacht werden.

Der in diesem Fall verwendete Anbieter Visa stellt dazu umfangreiche Informationen bereit[33], so werden bei Zahlung mittels Visa Card zahlreiche Daten durch verschiedene Stellen verarbeitet, dies ist aktuell nicht transparent für die Nutzenden.

Warum wir personenbezogene Daten erfassen und wie wir sie verwenden:

Zweck der Erfassung und des Teilens	**Kategorien personenbezogener Daten**	**Rechtsgrundlage für die Verarbeitung (soweit nach geltendem Recht erforderlich)**
Betrieb der elektronischen Zahlungsnetzwerke von Visa (einschließlich Autorisierung, Freischaltung und Abwicklung von Transaktionen und Tokenisierung), Bearbeitung Ihrer Zahlungstransaktionen sowie für verwandte Zwecke wie Authentifizierung, Streitbeilegung, Schutzmaßnahmen gegen Betrug und Sicherheit.	• Kontaktdaten • Transaktions- und Finanzinformationen • Informationen zu unserer Beziehung • Informationen aus Interaktionen • Biometrische Kennungen • Geschäftskundendaten • Schlussfolgerungen und abgeleitete Informationen • Online- und technische Informationen • Audio- und visuelle Informationen • Staatlich ausgestellte Identifikationsnummern • Geolokalisierungsinformationen • Compliance-Daten	• Zur Erfüllung eines Vertrags mit Ihnen oder zur Erfüllung eines Vertrags zwischen Ihnen und Händlern oder zwischen Ihnen und dem Finanzinstitut oder einer anderen Einrichtung, die Ihre Karte ausgestellt hat, wenn Visa Zahlungsdienste anbietet oder als Datenverarbeiter fungiert; • Zur Einhaltung der für uns weltweit geltenden Gesetze und Vorschriften; • Zum Zwecke unserer eigenen berechtigten Interessen oder der berechtigten Interessen anderer, wie etwa zum Schutz von Ihnen, uns oder anderen vor Bedrohungen (wie Sicherheitsbedrohungen oder Betrug), zur Abwicklung und Verwaltung unserer Geschäftstätigkeiten, wie z. B. für Qualitätskontrolle, Compliance,

Abbildung 21: Auszug aus den Datenschutzbestimmungen von Visa

Anmerkung / Empfehlung

Es sollte auf die Datenschutzbestimmungen von Visa hingewiesen werden, u.a. empfiehlt es sich Visa innerhalb der Datenschutzbestimmungen auf socialcard.de aufzuführen und weitere Informationen im Kontext von Visa-Zahlungen bereitzustellen.

[31] https://www.socialcard.de/datenschutz
[32] https://www.socialcard.de/fileadmin/user_upload/socialcard_kartennutzervereinbarung_1.2.pdf
[33] https://www.visa.de/nutzungsbedingungen/visa-globale-datenschutzmitteilung.html

4.2 Funde in Bezug auf die Bezahlkarte

Nachfolgend werden Funde in Bezug auf die Bezahlkarte von den Anbietern PayCenter GmbH / petaFuel GmbH detailliert beschrieben. Die Kenntnisse stützen sich dabei auf die aktuelle Version der Webapplikation (21.04.2024) und die neuste Version der Android-App (1.1 vom 02.04.2024, neuste Version zum Zeitpunkt des Berichtes).

Lösungsname	Bezahlkarte
Logo des Anbieters / App	 (entnommen von: https://play.google.com/store/apps/details?id=net.petafuel.mobile.bezahlkarte)
Anbieter	PayCenter GmbH / petaFuel GmbH
Kreditkarten-Anbieter	Mastercard
Website	Nutzungsseite: https://bezahlkarte.eu/ / https://meine.bezahlkarte.eu/ Informationsseite: https://bezahlkarte.info/
Name der App	Bezahlkarte
URL zur App (Play Store)	https://play.google.com/store/apps/details?id=net.petafuel.mobile.bezahlkarte
Version (zum Zeitpunkt des Tests)	1.1
APK SHA-256	4B106AE2F1AD8DB4CCF56470E2A32B4926A326AAB85C378B78CBDDDEF93388F0
URL zur App (App Store)	https://apps.apple.com/de/app/bezahlkarte/id6478606321
Privacy Policy im App-Store	https://bezahlkarte.eu/datenschutzerklaerung/
Pilotprojekte (Stand 15.04.2024, laut öffentlich zugänglichen Informationen)	Landkreis Günzburg, Landkreis Fürstenfeldbruck, der Landkreis Traunstein, kreisfreie Stadt Straubing

4.2.1 Klartext Link auf meine.bezahlkarte.eu führt in App zu Fehler

Klasse	IT-Sicherheit
Auswirkung	Gering

Bei Aufruf des Buttons „meine.bezahlkarte.eu“ innerhalb des Impressums und der Datenschutzbestimmungen wird versucht unverschlüsselt auf http://meine.bezahlkarte.eu/ zuzugreifen. Der finale Zugriff wird von dem Betriebssystem Android mit einer Fehlermeldung unterbunden, da Klartext Protokolle nicht erlaubt sind (ERR_CLEARTEXT_NOT_PERMITTED).

Abbildung 22: Button führt zu Klartext-URL

Abbildung 23: Fehler innerhalb der Android App

Durch den Fehler kann kein Login erfolgen und die App muss neu gestartet oder auf den Homebutton gedrückt werden. Dies erschwert die Bedienung.

Anmerkung / Empfehlung

Es ist begrüßenswert, dass HTTPS erzwungen werden soll, allerdings sollten dann alle Links innerhalb der Android-App HTTPS verwenden, andernfalls ist ein Abruf der Informationen oder eine Verlinkung zum Login nicht möglich und beeinträchtigt die Verwendung der App. Es wird empfohlen die beschriebene http-Verlinkung durch eine verschlüsselte https-Verlinkung auszutauschen.

4.2.2 Falsch gesetzter Link in der Bezahlkarten-App ermöglicht Anzeige beliebiger Inhalte innerhalb der App

Klasse	IT-Sicherheit
Auswirkung	Mittel

Nachdem man auf Login geklickt hat, erscheint eine Login-Maske. Klickt man innerhalb dieser Maske auf „Datenschutz“, so wird eine fehlerhafte URL geöffnet (ERR_NAME_NOT_RESOLVED).

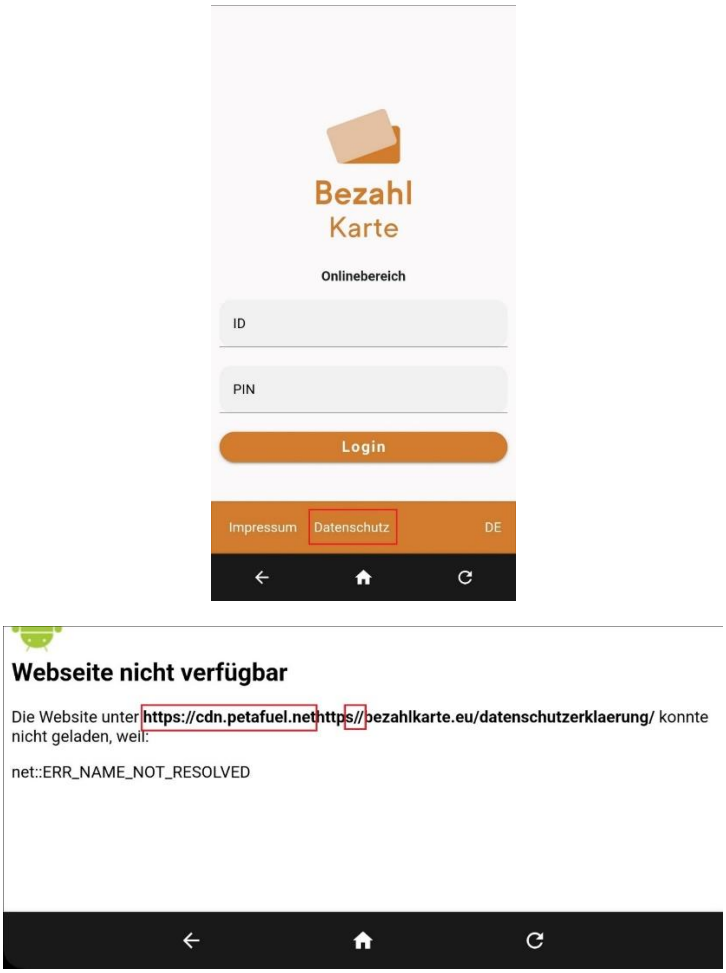


Abbildung 24: Nach Klick auf den Link öffnet sich eine fehlerhafte URL

Wie erkennbar ist, wird eine fehlerhafte URL geladen. Browser interpretieren den Link folgendermaßen:

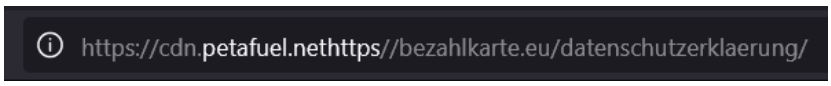


Abbildung 25: Interpretierte URL im Browser

Es wäre denkbar, dass Angreifer – sofern Sie DNS-Einträge für das abrufende Gerät beeinflussen können[34] – einen DNS-Eintrag für „cdn.petafuel.nethttps“ erstellen. Ist dies der Fall, so könnten beliebige Inhalte innerhalb der App angezeigt werden[35].

[34] Das wäre beispielsweise denkbar, wenn ein Man-in-The-Middle-Angriff erfolgt oder Angreifer Geräte von Opfern in ihrem Netzwerk (Evil Twin Angriff, etc.).
[35] Möglicherweise kommt es zu Fehlern durch fehlende TLS-Zertifikate (es handelt sich nicht um einen validen Hostnamen für den von einer public CA ein Zertifikat erstellt werden könnte).

Das Vorgehen wird in folgender Grafik schematisch dargestellt:

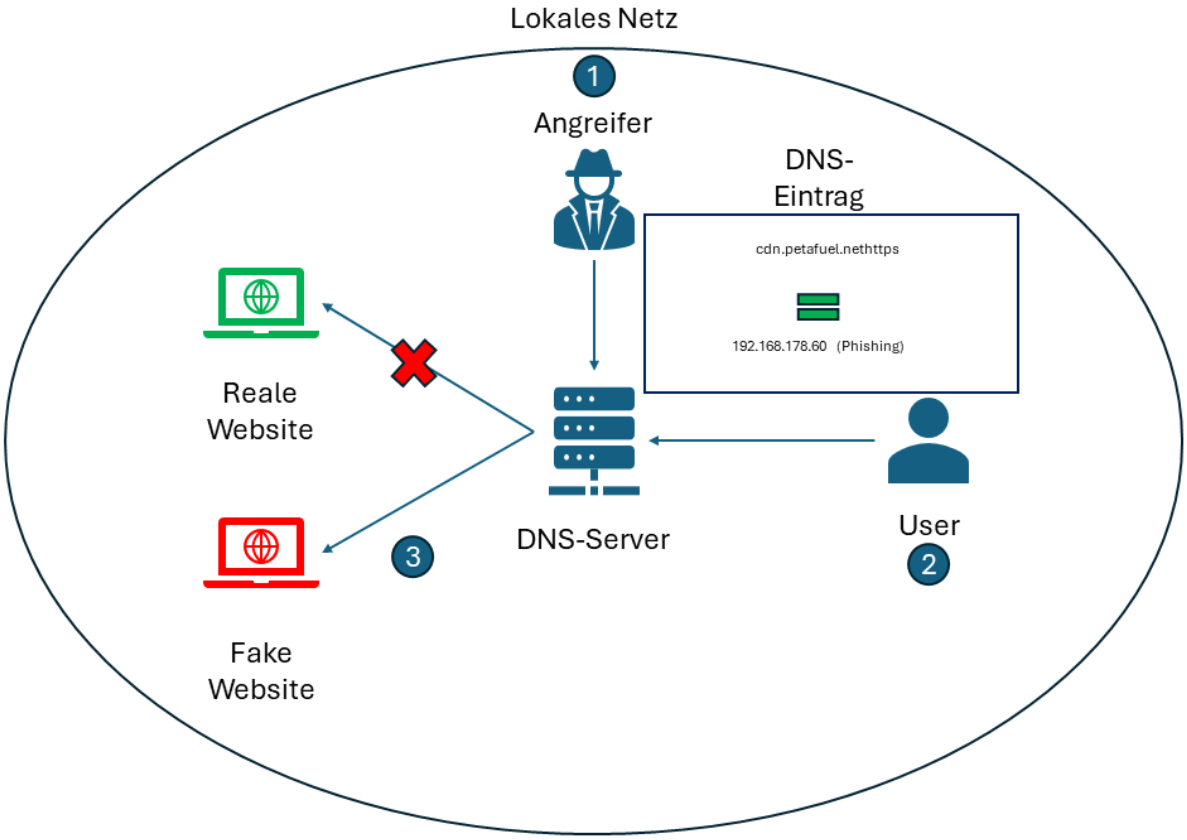


Abbildung 26: Übernahme der URL durch lokalen DNS-Eintrag

Anmerkung / Empfehlung

Da ein spezielles Szenario vorliegen muss (Man-in-The-Middle) und eine Aktion durch Benutzende vorliegen muss (Klick auf die Datenschutz-Informationen) wird das geschilderte Vorgehen als unwahrscheinlich, jedoch nicht unmöglich betrachtet. Neben der Ausnutzung durch Angreifer führt dies zudem zu einer Nicht-Nutzbarkeit bestimmter Funktionen (in diesem Fall Betrachtung der Datenschutzbestimmungen aus der Login-Maske heraus).

Es wird empfohlen den Link zu überabreiten, sodass eine korrekte Auflösung des Links und der Zugriff auf die Datenschutzerklärung möglich ist.

4.2.3 Cross-Site-Scripting innerhalb der Anmeldeseite möglich

Klasse	IT-Sicherheit
Auswirkung	Sehr Hoch

Nach einem Klick auf Login innerhalb von https://meine.bezahlkarte.eu/ bzw. der App wird folgende Seite geladen: https://login.petafuel.net/

Auf der Website befindet sich eine schwerwiegende Schwachstelle, die es ermöglicht JavaScript mit in die Website einzuschleusen. Diese Schwachstelle ist als XSS (Cross-Site-Scripting[36]) bekannt und gehört zu den OWASP Top Ten Schwachstellen (https://owasp.org/Top10/A03_2021-Injection/).

[36] Weitere Informationen zu XSS: https://owasp.org/www-community/attacks/xss/

Auf diesem Weg können z.B. Cookies von Usern gestohlen werden[37] und auf dem eigenen Gerät eingefügt werden. Das kann bedeuten, dass es einem nicht eingeloggten User möglich ist die Login Session eines anderen Users zu stehlen und sich als dieser einzuloggen (Session Hijacking). Statt einer Sitzungsübernahme ist es auch möglich, dass andere Inhalte eingebunden werden, etwa zu Phishing-Zwecken.

In folgendem Beispiel wird eine Ausgabe der Domain vorgenommen (statt einem JavaScript Alert würden Angreifer tiefgreifendere Änderungen vornehmen): https://login.petafuel.net/?redirectUrl=javascript:alert(document.domain)

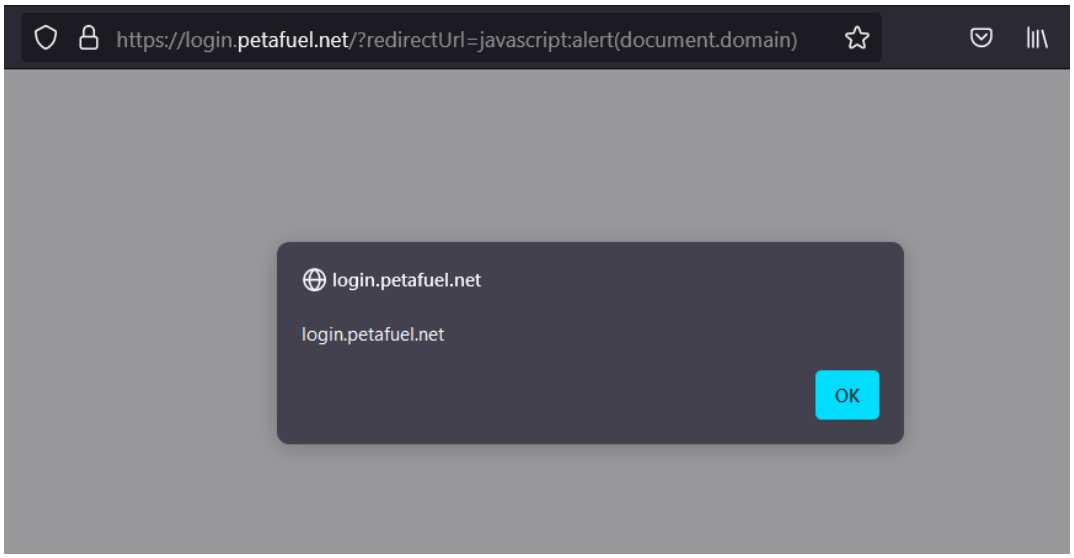


Abbildung 27: Durch eine XSS platzierter JavaScript Code wird ausgeführt

Ein HTTP-Request zur Ausnutzung sieht folgendermaßen aus:

```
GET /?redirectUrl=javascript:alert(document.domain) HTTP/1.1
Host: login.petafuel.net
Sec-Ch-Ua: "Chromium";v="123", "Not:A-Brand";v="8"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Windows"
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/123.0.6312.122 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Accept-Language: en-US,en;q=0.9
Priority: u=0, i
Connection: close
```

Anmerkung / Empfehlung

Ein Schutz vor XSS ist möglich, indem man eine strikte Eingabenvalidierung durchführt. Im vorliegenden Fall sollten nur Weiterleitungen auf valide URLs vorgenommen werden dürfen (bspw. Umsetzung mittels Allow-Listing). Weitere Informationen zum Schutz vor XSS finden sich hier: https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html

[37] Sofern entsprechende Cookies nicht mittels httpOnly-Flag geschützt sind: https://owasp.org/www-community/HttpOnly

4.2.4 Datenschutzerklärung ausschließlich in Deutsch verfügbar

Klasse	Datenschutz
Auswirkung	Mittel

Die Datenschutzerklärung auf der Website (verfügbar über https://bezahlkarte.eu/datenschutzerklaerung/) ist ausschließlich in Deutsch verfügbar. Es gibt keine Möglichkeiten auf der Webseite eine übersetzte Version der Datenschutzerklärung einzusehen, was eine informierte Entscheidung für Betroffene erschwert. Auch innerhalb der App ist keine andere Sprache einsehbar.

Anmerkung / Empfehlung

Insbesondere unter Berücksichtigung des Nutzendenkreises empfiehlt es sich zumindest auch eine englischsprachige Version der Datenschutzerklärung anzubieten.

4.2.5 Testumgebung aus verlinkten Assets auslesbar und ermöglicht Informationspreisgaben

Klasse	Datenschutz / IT-Sicherheit
Auswirkung	Gering

Innerhalb verschiedener Webseiten sind Assets von „wozutesten.de“ eingebunden, bspw. wird das Favicon von meine.bezahlkarte.eu von dieser Quelle geladen.

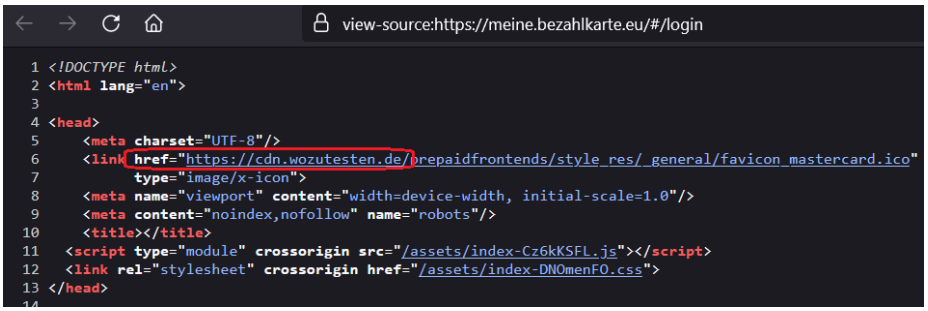


Abbildung 28: Favicon wird von wozutesten.de geladen

Durch das Certificate Transparency Project[38] lassen sich weitere Subdomains ermitteln:

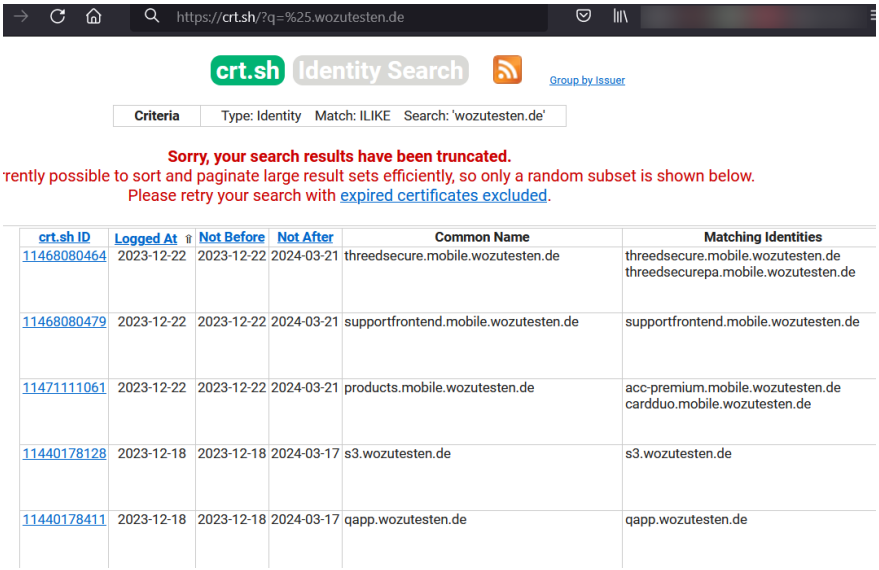
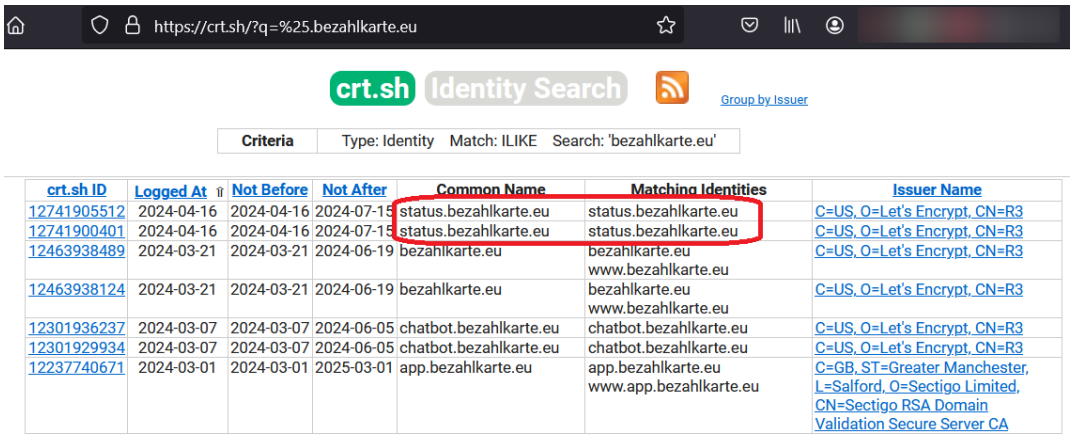


Abbildung 29: Subdomains von wozutesten.de

[38] https://de.wikipedia.org/wiki/Certificate_Transparency

Auch von bezahlkarte.eu lassen sich Subdomains finden[39], darunter status.bezahlkarte.eu:



crt.sh ID	Logged At	Not Before	Not After	Common Name	Matching Identities	Issuer Name
12741905512	2024-04-16	2024-04-16	2024-07-15	status.bezahlkarte.eu	status.bezahlkarte.eu	C=US, O=Let's Encrypt, CN=R3
12741900401	2024-04-16	2024-04-16	2024-07-15	status.bezahlkarte.eu	status.bezahlkarte.eu	C=US, O=Let's Encrypt, CN=R3
12463938489	2024-03-21	2024-03-21	2024-06-19	bezahlkarte.eu	bezahlkarte.eu www.bezahlkarte.eu	C=US, O=Let's Encrypt, CN=R3
12463938124	2024-03-21	2024-03-21	2024-06-19	bezahlkarte.eu	bezahlkarte.eu www.bezahlkarte.eu	C=US, O=Let's Encrypt, CN=R3
12301936237	2024-03-07	2024-03-07	2024-06-05	chatbot.bezahlkarte.eu	chatbot.bezahlkarte.eu	C=US, O=Let's Encrypt, CN=R3
12301929934	2024-03-07	2024-03-07	2024-06-05	chatbot.bezahlkarte.eu	chatbot.bezahlkarte.eu	C=US, O=Let's Encrypt, CN=R3
12237740671	2024-03-01	2024-03-01	2025-03-01	app.bezahlkarte.eu	app.bezahlkarte.eu www.app.bezahlkarte.eu	C=GB, ST=Greater Manchester, L=Salford, O=Sectigo Limited, CN=Sectigo RSA Domain Validation Secure Server CA

Abbildung 30: Subdomains von Bezahlkarte.eu

Unter status.bezahlkarte.eu läuft ein Status-Tracking Service. Einzelne der Meldungen beinhalten sensible Daten (u.a. Serverfehler oder Informationen zu Krankheitsständen der Mitarbeitenden). Einzelne Informationen waren ausschließlich zum Zeitpunkt des Screenshots temporär einsehbar, wurden später entfernt.

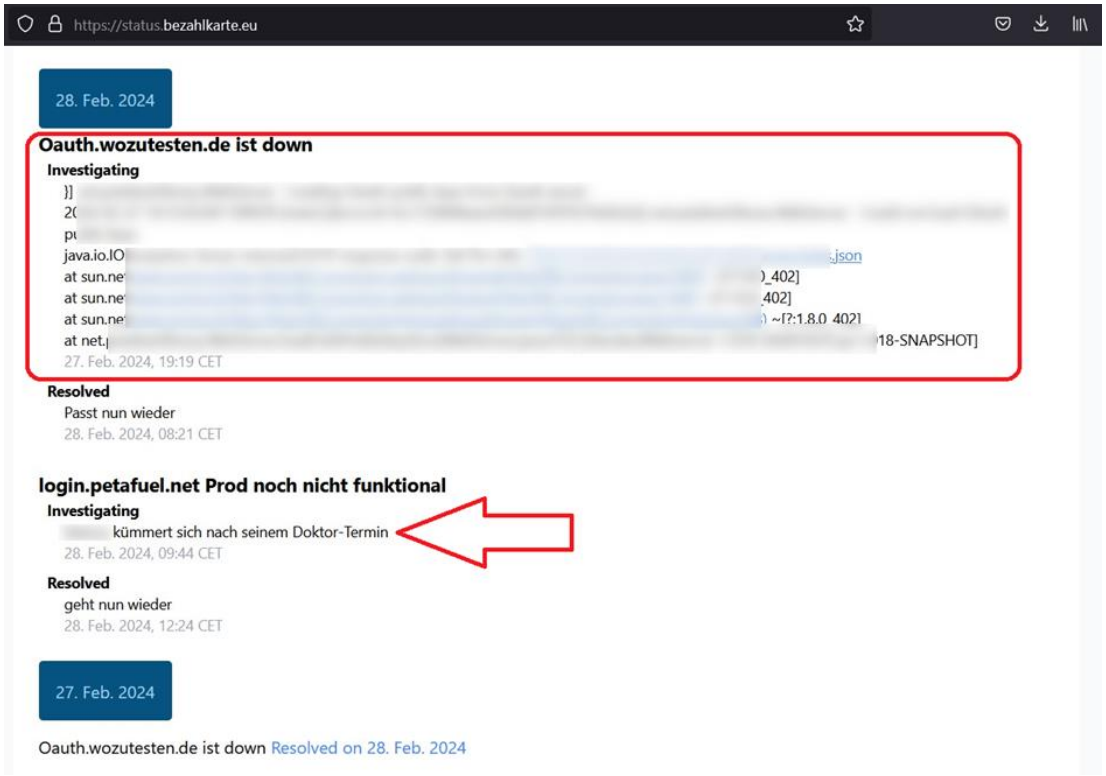


Abbildung 31: Serverinformationen und Information zu Krankheitsstand eines Mitarbeitenden

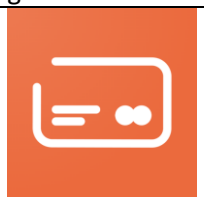
Anmerkung / Empfehlung

Testumgebungen sollten im Idealfall nicht aus dem Internet erreichbar sein. Darüber hinaus sollte aus Produktivumgebungen keine Verlinkungen auf Testdateien oder Assets vorgenommen werden. Zudem sollte ein Status-Tracking entweder nicht frei verfügbar sein oder keine sensiblen Daten beinhalten.

[39] https://crt.sh/?q=%25.bezahlkarte.eu

4.3 Funde in Bezug auf die givve® Card

Nachfolgend werden Funde in Bezug auf die givve® Card von den Anbietern PL Gutscheinsysteme GmbH / Groupe Up detailliert beschrieben. Die Kenntnisse stützen sich dabei auf die aktuelle Version der Android-App (5.4.1 vom 12.04.2024, neuste Version zum Zeitpunkt des Berichtes).

Lösungsname	givve® Card
Logo des Anbieters / App	 (entnommen von: https://play.google.com/store/apps/details?id=com.givve.cardsuite.app)  (entnommen von: https://givve.com/de/karriere)
Anbieter	givve®/PL Gutscheinsysteme GmbH
Kreditkarten-Anbieter	Mastercard
Website	Informationsseite: https://givve.com/de/ Informationsseite zur Bezahlkarte: https://givve.com/de/oeffentlicher-sektor/bezahlkarte-fuer-leistungsempfaenger
Name der App	givve® Card
URL zur App (Play Store)	https://play.google.com/store/apps/details?id=com.givve.cardsuite.app
Version (zum Zeitpunkt des Tests)	5.4.1
APK SHA-256	A2688482D40A1612EB1B9812BFC4533FA32B3199ED043 9185B086BBFF70165F8
URL zur App (App Store)	https://apps.apple.com/de/app/givve/id1449954897
Privacy Policy im App-Store	https://givve.com/de/datenschutz-fuer-kartenhalter#c8037
Pilotprojekte (Stand 15.04.2024, laut öffentlich zugänglichen Informationen)	Landkreis Greiz, Wartburgkreis, Saale-Orla-Kreis

4.3.1 Android App enthält Tracker-Bibliotheken und kontaktiert diese unmittelbar nach App-Start (ohne Einwilligung)

Klasse	Datenschutz
Auswirkung	Sehr hoch

Die App (com.givve.cardsuite.app) enthält unter anderem folgende 2 Tracker-Bibliotheken:

- **Google Firebase Analytics**
- **Sentry**

Die entsprechenden Tracking-Bibliotheken werden unmittelbar nach erstmaligem App-Start kontaktiert:

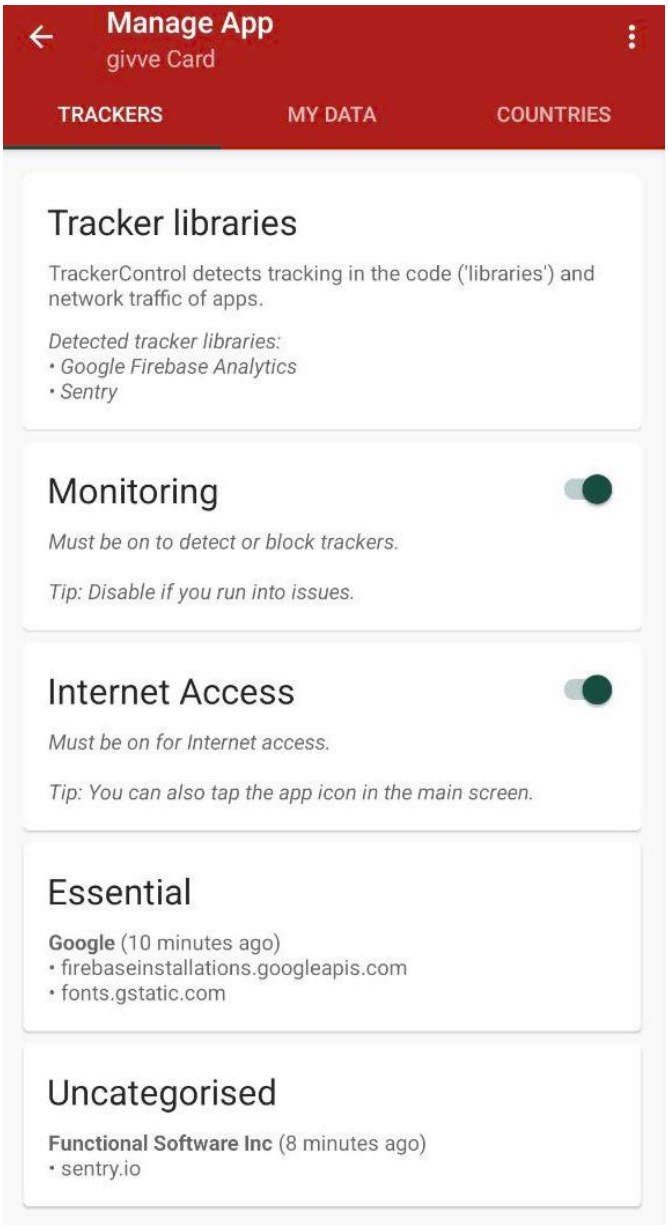


Abbildung 32: Kontakt zu Tracking-Servern

Darüber hinaus wird neben dem Tracking offensichtlich auch eine Schriftart über Google Fonts geladen. Bei den geladenen Daten handelt es sich um Schriftart-Dateien, welche von einem Server des Unternehmen Google (Alphabet Inc.) geladen werden. Bei Abruf dieser Schriftarten werden Nutzerdaten, darunter auch die IP-Adresse, an Google übertragen. Nach dem Urteil des Landgericht

München I, Urteil vom 20.01.2022, Az. 3 O 17493/20 stellt dies (ohne Einwilligung) einen Verstoß gegen die Datenschutzgrundverordnung (DSGVO) dar[40].

Kategorie	Tracker	Kontaktierte URLs
Essential	Google	firebaseinstallations.googleapis.com / fonts.gstatic.com
Uncategorised	Functional Software Inc	sentry.io

Auch das Senden von Daten an Google Firebase und Sentry stellt mutmaßlich einen Verstoß gegen die DSGVO dar, da dort personenbeziehbare Informationen (Advertising ID und Geräte-ID) übermittelt werden.

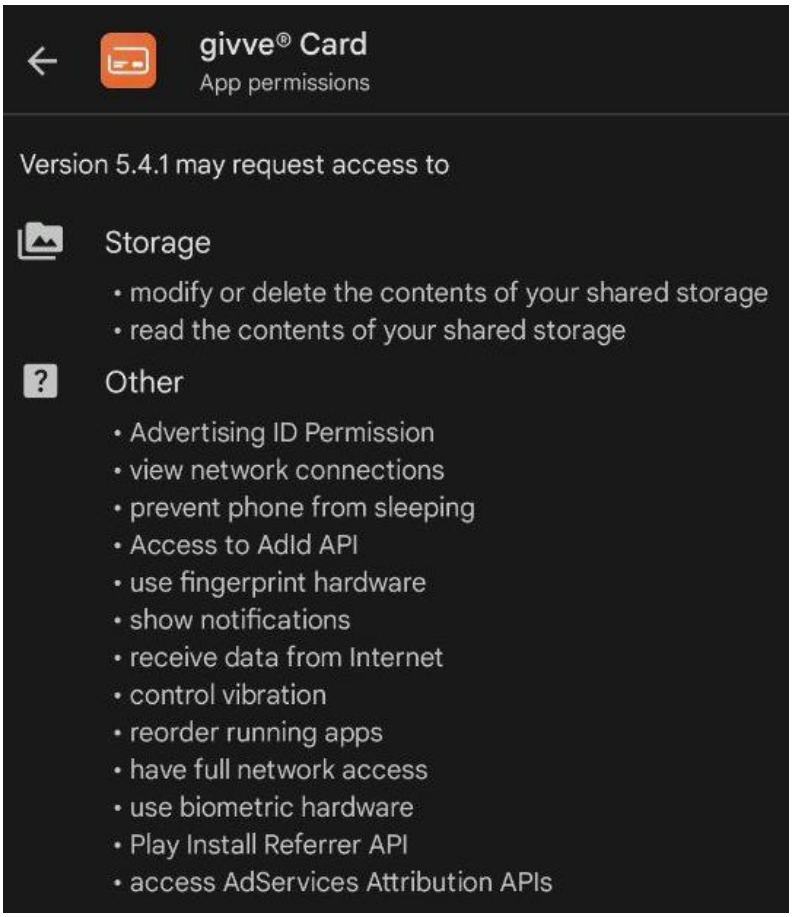


Abbildung 33: Permissions der App erlauben Auslesen der Advertising-ID

Anmerkung / Empfehlung

Die Verwendung von Tracking-Bibliotheken ohne Rechtsgrundlage (bspw. durch eine Einwilligung) stellt mutmaßlich einen Verstoß gegen die DSGVO dar. Die genannten Tracking-Bibliotheken sollten entweder aus der App entfernt werden oder es sollte eine – vor der Übermittlung von Daten - informierte, freiwillige und aktive Einwilligung über ein Banner eingeholt werden.

[40] https://rewis.io/urteile/urteil/lhm-20-01-2022-3-o-1749320/

4.3.2 Verwendete Tracking-Bibliotheken werden nicht in den Datenschutzbestimmungen genannt

Klasse	Datenschutz
Auswirkung	Mittel

Wie im Fund zuvor bereits beschrieben wird Kontakt zu mindestens 2 Tracking-Anbietern aufgenommen (Google Firebase, Sentry). Beide Tracking Dienstleister sind nicht in den Datenschutzbestimmungen[41] angeführt, dies bedeutet, dass das vorliegende Verhalten der App von dem beschriebenen Verhalten der Datenschutzbestimmung abweicht.

Nutzende können sich so nicht ausreichend über die App und ihre Rechte informieren.

Anmerkung / Empfehlung

Es wird empfohlen die Datenschutzbestimmungen zu aktualisieren und Drittanbieter (sofern sie weiterhin verwendet werden) dort aufzuführen.

4.3.3 Weitreichende Zugriffsmöglichkeiten für die App

Klasse	Datenschutz / IT-Sicherheit
Auswirkung	Mittel

Mittels Analyse der AndroidManifest.xml Informationen aus der APK-Datei lässt sich ermitteln welche Berechtigungen (Permission) der App auf einen Android Smartphone eingeräumt wird.

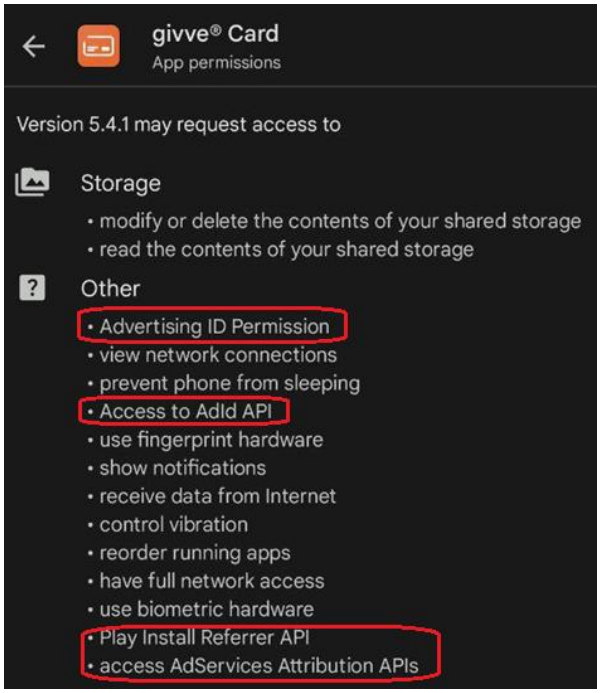


Abbildung 34: App-Permissions

Insbesondere bei den rot markierten Permissions (bspw. Advertising ID Permission oder AdId API) ist unklar, weshalb diese überhaupt für die App und ihren Nutzungszweck erteilt werden müssen. Auch die sonstigen Permissions legen den Eindruck nahe, dass diese für den engeren Nutzungszweck der App nicht erforderlich sind.

[41] Verlinkte Datenschutzbestimmungen aus dem Google Play Store, Datenschutzbestimmungen zum 23.04.2024: https://givve.com/de/datenschutz-fuer-kartenhalter

Anmerkung / Empfehlung

Es sollte geprüft werden, welche Permissions tatsächlich benötigt werden. Die Permissions sollten sich auf das notwendige Minimum (Datenminimierung nach DSGVO) beschränken und genau zugewiesen werden.

4.3.4 Datenschutzerklärung auf der Webseite ausschließlich in Deutsch verfügbar

Klasse	Datenschutz
Auswirkung	Mittel

Die Datenschutzerklärung auf der Website (verfügbar über https://givve.com/de/datenschutz-fuer-kartenhalter) ist ausschließlich in Deutsch verfügbar. Es gibt keine Möglichkeiten auf der Webseite eine übersetzte Version der Datenschutzerklärung einzusehen, was eine informierte Entscheidung für Betroffene erschwert.

Anmerkung / Empfehlung

Insbesondere unter Berücksichtigung des Nutzendenkreises empfiehlt es sich zumindest auch eine englischsprachige Version der Datenschutzerklärung anzubieten.

Anhang A: Weiterführende Informationen zum Datenschutz in Bezug auf Bezahlkarten

In der Europäischen Union ist seit dem 24. Mai 2016 die Datenschutz-Grundverordnung (DSGVO) in Kraft. Ab dem 25. Mai 2018 ist diese verbindlich von Mitgliedsstaaten der Europäischen Union und damit auch Deutschland anzuwenden (vgl. Bauer, Eickmeier, & Eckard, 2018, S. 52 f.[42]). Datenschutz hat in Deutschland einen sehr hohen Stellenwert. So hat das Land Hessen beispielsweise 1970 mit dem Hessischen Datenschutzgesetz (HDSG 1970) das erste Datenschutzgesetz der Welt eingeführt und in einem Aufsatz von Ulrich Seidel mit dem Titel „Persönlichkeitsrechtliche Probleme der elektronischen Speicherung privater Daten“ (vgl. Seidel, 1970[43]) wurde ebenfalls 1970 erstmals der Begriff „Datenschutz“ definiert (vgl. Schäfers, Die Datenschutz-Grundverordnung (DSGVO) – eine neue Zeitrechnung im Bereich des Datenschutzes?, 2018, S. 16[44]).

Wie Hamburgs Datenschutzbeauftragter Thomas Fuchs zudem beschrieben hat, gilt: „Das Recht auf Schutz der personenbezogenen Daten […] für deutsche und ausländische Staatsangehörige, die sich in der Bundesrepublik Deutschland oder in der Europäischen Union aufhalten, gleichermaßen“[45].

Die DSGVO (und damit das geltende Datenschutzrecht) dient nach Artikel 1 DSGVO dazu natürliche Personen, ihre Grundrechte und insbesondere das Recht auf den Schutz personenbezogener Daten zu schützen. Personenbezogene Informationen sind nach Artikel 4 DSGVO:

> „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person […] beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann […]“ (Auszug aus Artikel 4 DSGVO).

Wie an der Beschreibung deutlich wird ist ein Personenbezug in recht abstrakten Formen (etwa über eindeutige Kennungen) denkbar. Auch in Betriebssystemen von Smartphones gibt es personenbezogene Kennzeichen, dies können beispielsweise **eindeutige Gerätekennungen oder Werbe-IDs** sein.

Eine Verarbeitung von personenbezogenen Daten ist darüber hinaus nach Artikel 6 DSGVO nur dann zulässig, wenn eine Rechtmäßigkeit der Verarbeitung vorhanden ist (vgl. Bauer, Eickmeier, & Eckard, 2018, S. 70 [46]), letzteres kann beispielsweise in folgenden Fällen vorliegen:

> „a.) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

[42] Bauer, C., Eickmeier, F., & Eckard, M. (2018). E-Health: Datenschutz und Datensicherheit. Wiesbaden: Springer Fachmedien Wiesbaden GmbH.
[43] Seidel, U. (1970). Persönlichkeitsrechtliche Probleme der elektronischen Speicherung privater Daten. Neuen Juristischen Wochenschrift, S. 1581-1583.
[44] Schäfers, T. P. (2018). Die Datenschutz-Grundverordnung (DSGVO) – eine neue Zeitrechnung im Bereich des Datenschutzes? Freilaw - Freiburg Law Students Journal Nr. 01/2018, S. 16-23.
[45] https://www.zeit.de/news/2024-02/23/datenschutzbeauftragter-sieht-keine-verstoesse-bei-bezahlkarte
[46] Bauer, C., Eickmeier, F., & Eckard, M. (2018). E-Health: Datenschutz und Datensicherheit. Wiesbaden: Springer Fachmedien Wiesbaden GmbH.

> b.) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;
>
> c.) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;
>
> d.) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
>
> e.) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt" (Auszug aus Artikel 6 DSGVO).

In der Praxis liegt meist die Einwilligung der Betroffenen (a) als Grund für die Rechtmäßigkeit der Verarbeitung vor. Die meisten Menschen neigen laut Angaben des „European Data Protection Boards" (EDPB) offenbar dazu Einwilligungen ohne genauere Recherche zu erteilen und bezeichnen dies als eine Art Gewöhnungseffekt:

> „In the digital context, many services need personal data to function, hence, data subjects receive multiple consent requests that need answers through clicks and swipes every day. This may result in a certain degree of click fatigue: when encountered too many times, the actual warning effect of consent mechanisms is diminishing." (European Data Protection Board (EDPB), 2020, S. 19 [47]).

Der Gesetzgeber hat in Artikel 7 DSGVO definiert, wie genau eine Einwilligung erfolgen muss, damit sie zulässig ist. Eine **Einwilligung muss demnach informiert, freiwillig, aktiv und vor der eigentlichen Übermittlung von Daten erfolgen** (vgl. Landesbeauftragten für den Datenschutz und die Informationsfreiheit, 2022[48]).

In einem Bericht der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 20. Dezember 2021 wird in Bezug auf Einwilligungen kritisiert, dass häufig fehlende Informationen oder Intransparenz vorliegt:

> „Im Zusammenhang mit Webseiten und Apps besteht oftmals ein Defizit darin, dass die Banner, mit denen eine Einwilligung eingeholt werden soll, intransparent gestaltet sind, sodass u. a. die Zwecke des Zugriffs auf ein Endgerät und die beteiligten Akteure nicht ausreichend erkennbar sind. Intransparenz kann sich auch daraus ergeben, dass unklar ist, mit welcher Schaltfläche welcher Effekt erreicht werden kann und wie oder mit welchem Aufwand eine Ablehnung von einwilligungsbedürftigen Prozessen möglich ist." (Konferenz der unabhängigen Datenschutzaufsichtsbehörden, 2021[49])

Neben der Notwendigkeit einer Einwilligung gibt es (sofern kein sonstiger Aspekt eine Rechtmäßigkeit der Verarbeitung gewährleistet) weitere Kernprinzipien des Datenschutzes, welche folgend dargestellt werden sollen. Nach Artikel 5 DSGVO dürfen personenbezogene Daten nur für den Zweck verwendet werden für den eine Einwilligung vorliegt (***Zweckbindung***). Darüber hinaus ist eine ***Datenminimierung*** anzustreben, es sollen nur solche Daten verarbeitet oder erfasst werden, welche auch tatsächlich notwendig für das Erbringen eines Service sind.

---

[47] European Data Protection Board (EDPB). (2020). Guidelines 05/2020 on consent under Regulation 2016/679. Brüssel: European Data Protection Board (EDPB).

[48] https://www.baden-wuerttemberg.datenschutz.de/faq-zu-cookies-und-tracking-2/

[49] Konferenz der unabhängigen Datenschutzaufsichtsbehörden. (2021). Orientierungshilfe der Aufsichtsbehörden für Anbieter:innen von Telemedien ab dem 1. Dezember 2021 (OH Telemedien 2021). Berlin: Konferenz der unabhängigen Datenschutzaufsichtsbehörden.

Bei der Nutzung von Bezahlkarten fallen verschiedene Informationen an, neben den Daten, welche für die Ausstellung und Registrierung der Karten notwendig sind, fallen bei der späteren Benutzung auch Transaktionsdaten an. Die Nutzung der Transaktionsdaten ist nach geltendem Recht unzulässig (Datenschutzrechtliche Unzulässigkeit der Kontoeinsicht)[50].

Wie sich zeigt, gibt es eine ganze Reihe an gesetzlichen Anforderungen im Zusammenhang mit dem Thema Datenschutz die bei dem Einsatz von Bezahlkarten zu berücksichtigen sind.

Die vorliegende Untersuchung hat gezeigt, dass zwei von drei Anbietern Tracking-Bibliotheken in ihren Bezahlkarten-Apps integriert hatten, welche unmittelbar nach App-Start personenbezogene Informationen übermitteln und keine Einwilligung der Nutzenden eingeholt haben.

Zudem haben alle drei Anbieter ausschließlich deutschsprachige Datenschutzbestimmungen zur Verfügung gestellt, wodurch eine informierte Entscheidung teils beeinträchtigt wird.

[50] https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/240223_Position_HmbBfDI_Bezahlkarte.pdf