White Paper
„Vivy: Sicherheit und Datenschutz“

Erstellt am 16. Oktober 2018 | Version 1.0

in Zusammenarbeit mit

Inhalt

1 Einleitung

Gesundheitsdaten sind hoch sensible Daten. Daher ist der wichtigste Faktor für uns die Sicherheit der Nutzerdaten. Dieses Dokument dient dazu, kompakt und verständlich zu erläutern, wie Vivy den Schutz der Gesundheitsdaten der Nutzer nach höchsten Sicherheitsstandards gewährleistet.

Sie finden darin Informationen zu den Funktionen der Vivy-App und deren Umsetzung auf der Vivy-Infrastruktur. Dazu erläutern wir in diesem Whitepaper alle von uns umgesetzten Maßnahmen zur Informationssicherheit und den Datenschutz, von technischen und infrastrukturellen bis hin zu organisatorischen und personellen Maßnahmen.

Für weitere Fragen zu Betreibermodell, Infrastruktur, Anwenderarchitektur oder Datenschutz stehen wir gerne zur Verfügung.

2 Vivy

Die Vivy GmbH ist das Berliner Unternehmen hinter der gleichnamigen App zur Verwaltung der elektronischen Patientenakte. Die Firmenphilosophie lautet: „Ein gesünderes Leben ist ein glücklicheres Leben". Zu diesem Zweck befähigt Vivy Nutzer dazu, ihr physisches und psychisches Wohlbefinden besser zu verstehen und aktiv zu verbessern. Dazu führt die App die persönlichen Gesundheitsdaten an einem Punkt zusammen und bereitet sie anschaulich auf. Dies gibt dem Nutzer mehr Kontrolle über seine medizinischen Dokumente.

Modular und freiwillig ergänzt um zusätzliche Daten liefert Vivy ein ganzheitliches Bild und wertvolle Erkenntnisse: Vivy versteht sich als Plattform für Gesundheitsdienstleistungen und bietet die Möglichkeit, Daten von Ärzten, Laboren, Anbietern von Health-Apps, Wearables uvm., sowie kooperierender Versicherungsanbieter, zu integrieren. Die Kerndienstleistung von Vivy ist die Aufbereitung medizinischer Daten und somit die Verarbeitung hoch sensibler persönlicher Informationen. Deshalb setzt Vivy auf bewährte Maßnahmen und anerkannten Standards in den Bereichen Informationssicherheit und Datenschutz.

Funktionen von Vivy

Die digitale Gesundheitsassistentin Vivy bietet dem Nutzer eine Reihe von Diensten an. Die grundlegende Funktionalität ist die Verwaltung Gesundheitsdaten im Rahmen einer elektronischen Gesundheitsakte (eGA). Die Sicherheit dieser Funktionen wird in diesem Whitepaper ausführlich betrachtet.

Registrierung

Nutzer können Vivy-Dienste (z.B. Hinterlegen und Teilen von Gesundheitsdaten) einfach und sicher mit der Vivy-App über ihr Smartphone nutzen. Dafür registrieren sich Nutzer mit der App und ihren persönlichen Daten auf der Vivy-Plattform. Hierzu gehören Name, Vorname, Geburtsdatum, E-Mail-Adresse, Telefonnummer, Krankenkasse und Versicherungsnummer des Nutzers. Im Rahmen der Registrierung wird für den Nutzer direkt auf dem Smartphone ein Schlüsselpaar generiert, mit dem zukünftig alle Gesundheitsdaten sicher verschlüsselt werden.

Registrierte Nutzer können Ihre Identität darüber hinaus anhand eines amtlichen Lichtbildausweises (z.B. Personalausweis oder Reisepass) und einem Video-Selfie bestätigen.

Einsehen von Leistungsdaten

Unterstützt die Krankenkasse des Nutzers die elektronische Übermittlung von Leistungsdaten (z.B. Abrechnungsdaten von Arzt, Zahnarzt und Apotheker), können diese Daten ebenfalls mit der

Vivy-App eingesehen werden. Dabei werden Daten wie Name und Anschrift des Arztes, Zahnarztes oder Apothekers, das Datum der Abrechnung und die gestellte Diagnose von der Krankenkasse übertragen und in der App angezeigt. Diese Daten werden aber weder im Backend von Vivy noch in der App dauerhaft gespeichert.

Gesundheitsdaten hinterlegen

Nach erfolgreicher Anmeldung kann der Nutzer über die Vivy-App Gesundheitsdaten verschlüsselt in seinem Vivy-Nutzerkonto hinterlegen. Dazu gehören insbesondere Impfungen, Medikationen, Notfalldaten sowie medizinische Dokumente (z.B. Blutbilder und andere Diagnosen).

Nutzer können über die Vivy-App ebenso medizinische Dokumente von einem Arzt anfordern. Dafür stellt Vivy eine Liste der im Verzeichnis registrierten Ärzte bereit. Nach Auswahl des richtigen Arztes und der Angabe von Informationen hinsichtlich des gewünschten Dokumentes (z.B. Typ des Dokumentes oder Datum der Untersuchung) unterschreibt der Nutzer die Anfrage direkt auf dem Display des Smartphones. Vivy sendet daraufhin diese Anfrage signiert an den Arzt. Der Arzt entscheidet, wie er Daten an den Patienten übermitteln möchte. Die signierte E-Mail enthält einen Link, mit dem der Arzt die gewünschten Dokumente verschlüsselt im Vivy-Konto des Nutzers bereitstellen kann. Alternativ kann der Arzt den Patienten in die Praxis einladen, damit diese Dokumente direkt vor Ort geteilt werden können.

Gesundheitsdaten teilen

Über die Vivy-App kann der Nutzer für einzelne Gesundheitsdaten einen im Internet, zeitlich begrenzt, erreichbaren Shortlink und eine PIN erstellen. Unter Angabe der PIN können diese Gesundheitsdaten dann mit einem Webbrowser heruntergeladen werden. So kann der Nutzer in seinem Vivy-Benutzerkonto hinterlegte Gesundheitsdaten zum Beispiel mit seinem Arzt teilen. Um Gesundheitsdaten mit anderen Vivy-Nutzern (z.B. Familienmitglieder) zu teilen, genügt die Angabe der E-Mail-Adresse des anderen Vivy-Nutzers in der Vivy-App. Das Gesundheitsdokument ist dann für 24 Stunden in der App des anderen Nutzers einsehbar. Die Übertragung der Gesundheitsdaten an andere erfolgt jederzeit in verschlüsselter Form.

Notfalldaten

Nutzer können darüber hinaus über die Vivy-App Notfalldaten (z.B. Blutgruppe, Erkrankungen, Allergien, Notfallkontakt) in Ihrem Vivy-Benutzerkonto verschlüsselt hinterlegen und diese über einen QR-Code Dritten zugänglich machen. Dafür erhält der Nutzer von Vivy einen Notfalldaten-Sticker den dieser z.B. auf seine Krankenkassenkarte kleben kann. Im Falle eines Notfalls können von Rettungskräften sämtliche relevanten medizinischen Daten über den Nutzer durch einen Scan des QR-Codes abgerufen werden. Werden die Notfalldaten abgerufen, wird der Nutzer darüber per Push-Benachrichtigung sofort informiert. Der Nutzer kann den Zugriff auf den Notfalldatensatz jederzeit deaktivieren.

Systemmodell

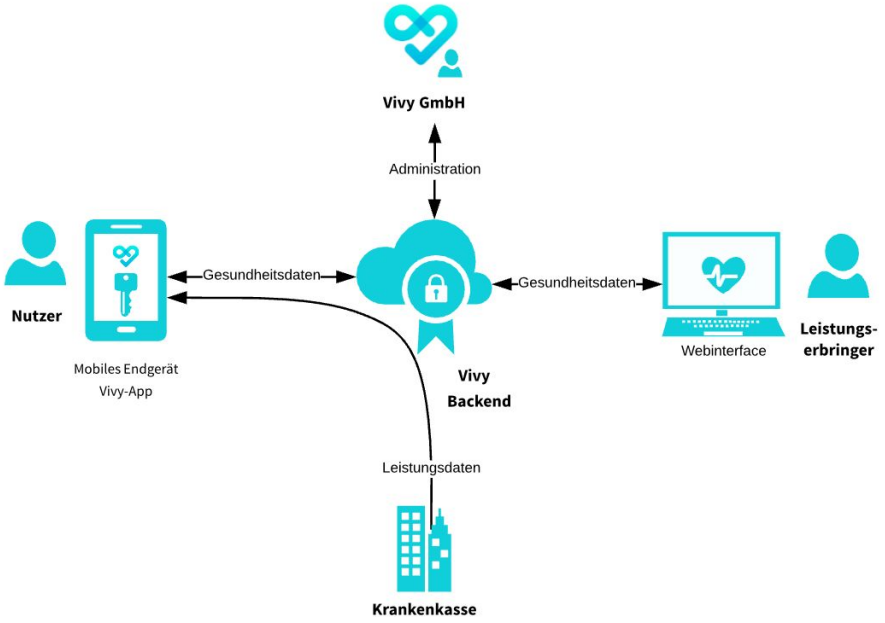

Abbildung 1: Systemmodell der Vivy Infrastruktur

Die technische Infrastruktur von Vivy ist in Abbildung 1 dargestellt und basiert auf den folgenden wesentlichen Komponenten:

- Die **Vivy-App** ist eine für iOS und Android verfügbare App, welche der Nutzer auf seinem Smartphone installiert. Sie ermöglicht dem Nutzer den sicheren Zugriff auf sein Vivy-Benutzerkonto sowie das Hinzufügen, Teilen und Anzeigen von Gesundheitsdaten. In der Vivy-App selbst werden keine Gesundheitsdaten gespeichert, sondern nur in verschlüsselter Form im Vivy-Backend.
- Das **Vivy-Backend** ist in Form einer Cloud-Lösung realisiert. Dort werden die Gesundheitsdaten in verschlüsselter Form mit dem Konto des Nutzers verknüpft gespeichert. Für den Up- und Download von Gesundheitsdaten durch Dritte generiert das Vivy-Backend jeweils eine transaktionsabhängige URL, welche über ein Webinterface genutzt werden kann. Insbesondere für die Anfrage von Gesundheitsdaten stellt Vivy einen verifizierten Satz von Kontaktdaten (Ärzte und Leistungserbringer) zur Verfügung.
- Die **Vivy GmbH** administriert das Vivy-Backend und die Nutzerverwaltung. Dazu speichert Vivy die im Rahmen des Registrierungsprozesses vom Nutzer angegebenen personenbezogenen Daten (Name, Vorname, Geburtsdatum, E-Mail-Adresse, Telefonnummer, Krankenkasse und Versicherungsnummer). Gesundheitsdaten der Nutzer werden so im Vivy-Backend verschlüsselt gespeichert, dass nur der Nutzer und von diesem autorisierte Dritte (Ärzte und Familienmitglieder) diese Daten entschlüsseln können. Dadurch ist technisch sichergestellt, dass Vivy die Gesundheitsdaten nicht einsehen kann.
- Die **Krankenkasse** als externe Kooperationspartner kann den Zugriff auf die Leistungsdaten des Nutzers ermöglichen.

Geschäftsmodell

Die Basis unseres Angebots ist die Bereitstellung einer elektronischen Gesundheitsakte (eGA), mit der Impfungen, Medikationen und weitere medizinische Dokumente verwaltet und mit Ärzten und Apothekern geteilt werden können. Das Ziel von Vivy ist es, möglichst vielen Menschen einen

kostenfreien Zugang zu ermöglichen. Das erreicht Vivy durch die Kooperation mit Krankenkassen und Krankenversicherungen. Die Krankenkassen und Krankenversicherungen im Kooperationsverbund von Vivy übernehmen für ihre Kunden die im Rahmen der Nutzung von Vivy entstehenden Kosten.

Regulatorisch steht dieses Finanzierungsmodell auf sicheren Beinen. Mit §68 des SGB V eröffnet der Gesetzgeber den gesetzlichen Krankenkassen ausdrücklich die Finanzierung einer persönlichen eGA. Gesetzliche Krankenkassen haben damit die Möglichkeit, ihren Versicherten die Vorteile der eGA kostenfrei zur Verfügung zu stellen. Für Kunden nicht teilnehmender Kassen besteht die Möglichkeit, Vivy zu einem jährlichen Beitrag zu nutzen.

Sowohl technisch als auch organisatorisch ist sichergestellt, dass die Krankenversicherungen keinen Zugriff auf persönliche Gesundheitsdaten der Nutzer erhalten. Allein die Identifikationsdaten sowie die Versicherungsnummer des Nutzers werden für Abrechnungszwecke mit der Krankenversicherung regelmäßig abgeglichen.

3 Verschlüsselung und Datensicherheit

Dieser Abschnitt erläutert den Einsatz der in Vivy genutzten kryptografischen Methoden. Für den Schutz der Gesundheitsdaten werden nur kryptographische Verfahren eingesetzt, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlen werden. Dabei kommen die vom BSI veröffentlichten Technischen Richtlinien BSI TR-02102-1[1] und BSI TR-02102-2[2] zur Anwendung.

Es wird zunächst das Konzept der persistenten Speicherung der verschlüsselten Gesundheitsdaten in der Vivy Infrastruktur beschrieben. Darauf aufbauend wird erklärt, wie Gesundheitsdaten hinzugefügt und mit anderen geteilt werden. Abschließend wird die Verschlüsselung des Notfalldatensatzes erläutert.

Speichern von Gesundheitsdaten

Alle Daten, die auf Vivy-Servern gespeichert werden, liegen nur in verschlüsselter Form vor. Sie sind mit einem nutzerspezifischen Schlüssel verschlüsselt. Dies bedeutet, dass nur der zugehörige Nutzer mit seinem Smartphone diese Daten wieder entschlüsseln kann.

Bei der Registrierung wird auf dem Smartphone des Nutzers zunächst ein asymmetrisches RSA-Schlüsselpaar[3] erstellt. Ein Schlüsselpaar besteht aus einem privaten und einem öffentlichen Schlüssel, die in einer mathematischen Beziehung stehen. Aus der Kenntnis des öffentlichen Schlüssels lässt sich der Private nicht ableiten. Der private Schlüssel verbleibt dabei auf dem Smartphone. Die Sicherheit des privaten Schlüssels auf dem Smartphone ist Betriebssystem-spezifisch. Es werden die dort vorhandenen Schlüsselspeichermechanismen benutzt (Android – Keystore, iOS – Keychain). Ein Zugriff auf den privaten Schlüssel ist damit nur möglich, wenn sich der Nutzer auf seinem Smartphone authentifiziert. Der öffentliche Schlüssel wird zusätzlich auch im Vivy Backend gespeichert. Die Verschlüsselung von Daten mit RSA funktioniert mithilfe des öffentlichen Schlüssels. Jeder, der im Besitz des öffentlichen Schlüssels ist, kann Daten damit verschlüsseln. Die Entschlüsselung ist dagegen nur mit dem privaten Schlüssel möglich.

---

[1] BSI: TR 02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 1 – Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 2018-02, Bundesamt für Sicherheit in der Informationstechnik

[2] BSI: TR 02102-2, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 – Verwendung von Transport Layer Security (TLS), Version 2018-02, Bundesamt für Sicherheit in der Informationstechnik.

[3] RFC 8017, "PKCS #1: RSA Cryptography Specifications Version 2.2", November 2016

Zur praktischen Umsetzung der Verschlüsselung der Gesundheitsdaten kommt eine hybride Verschlüsselung zum Einsatz. D.h. die Gesundheitsdaten werden mit einem symmetrischen Verschlüsselungsverfahren (AES[4] im Betriebsmodus GCM[5] mit einer Schlüssellänge von 256 Bit) verschlüsselt. Der hierbei eingesetzte AES-Schlüssel wird mit dem asymmetrischen Verschlüsselungsverfahren RSA (Padding OAEP[6] und einer Schlüssellänge von 4096 Bit) verschlüsselt. Dabei wird für jedes Gesundheitsdatum ein individueller AES-Schlüssel verwendet. Die verschlüsselten Gesundheitsdaten zusammen mit den verschlüsselten symmetrischen AES-Schlüsseln (im folgenden Kryptogramm genannt) werden im Vivy-Backend abgelegt.

Beim Abruf der Gesundheitsdaten aus dem Vivy-Backend bekommt der Nutzer das Kryptogramm (verschlüsselter AES-Schlüssel und verschlüsselte Gesundheitsdaten). Sein Smartphone entschlüsselt mit dem privaten RSA-Schlüssel den AES Schlüssel, der wiederum zur Entschlüsselung der Gesundheitsdaten verwendet wird. Erst jetzt liegen die Gesundheitsdaten wieder im Klartext auf dem Smartphone des Nutzers vor.

Gesundheitsdaten hinterlegen

Entsprechend dem bereits beschriebenen Verfahren zur Speicherung von Gesundheitsdaten, wird zum Hinzufügen von Daten zu einem Nutzerkonto der öffentliche Schlüssel des Nutzers benötigt. Diesen stellt Vivy auf Anfrage bereit. Das neue Gesundheitsdatum wird nun mit einem individuellen AES-Schlüssel symmetrisch verschlüsselt und als Kryptogramm mit dem durch den öffentlichen RSA-Schlüssel des Nutzers verschlüsselten AES-Schlüssel an die Vivy-Infrastruktur übergeben. Dort wird das Kryptogramm im Konto des Nutzers abgespeichert und steht diesem nun zum Abruf zur Verfügung. Das Hinzufügen von Gesundheitsdaten kann vom Nutzer selbst oder Dritten (Arzt, Apotheker, Labore) erfolgen. Dieser Vorgang wird jedoch in jedem Fall vom Nutzer ausgelöst.

Gesundheitsdaten teilen

Zum Teilen von Gesundheitsdaten müssen diese zunächst entschlüsselt werden. Dies geschieht auf dem Smartphone des Nutzers mit seinem privaten Schlüssel: Das Kryptogramm wird heruntergeladen, der verschlüsselte AES-Schlüssel entschlüsselt und mit diesem AES-Schlüssel dann die Gesundheitsdaten entschlüsselt. Der Empfänger benötigt ein eigenes asymmetrisches Schlüsselpaar, dessen öffentlicher Teil dem Nutzer von Vivy zur Verfügung gestellt wird. Somit verschlüsselt der Nutzer seine Gesundheitsdaten (wieder über das oben beschriebene hybride Verfahren), die er teilen will, so dass nur der Besitzer des privaten Schlüssels, passend zu diesem bereitgestellten öffentlichen Schlüssel, die Daten entschlüsseln kann. Die so geschützten Daten werden über die Vivy-Plattform dem Empfänger übermittelt.

Je nach Empfänger gibt es aber technische Unterschiede bei der Art der Bereitstellung (z.B. Dauer der Gültigkeit, Optionen zum Export der Daten sowie die Art der Bereitstellung über eine Website oder in der App). Wir unterscheiden im Folgenden zwei Fälle:

1) Teilen von Gesundheitsdaten mit anderen Vivy-Nutzern (z.B. Familienmitglieder)
2) Teilen von Gesundheitsdaten mit Leistungserbringern (z.B. Ärzte, Apotheker, Labore)

Zum Teilen von Daten mit anderen Vivy-Nutzern muss die registrierte E-Mail-Adresse des Empfängers bekannt sein. Anhand dieser wird er als Vivy-Nutzer identifiziert und über Vivy sein

[4] FIPS PUB 197, Advanced Encryption Standard (AES), National Institute of Standards and Technology, U.S. Department of Commerce, November 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf
[5] Morris J. Dworkin. 2007. SP 800-38d. Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (Gcm) and GMAC. Technical Report. NIST, Gaithersburg, MD, United States.
[6] RFC 8017, "PKCS #1: RSA Cryptography Specifications Version 2.2", November 2016

öffentlicher Schlüssel bereitgestellt. Die so geteilten Gesundheitsdaten werden auf dem Smartphone des Empfängers zwar dargestellt, die Vivy-App bietet aber nicht die Möglichkeit zur persistenten Speicherung oder zum Export. Nach 24 Stunden sind die Daten auch nicht mehr einsehbar, da Vivy sie aus dem Benutzerkonto des Empfängers wieder entfernt.

Für das Teilen der Gesundheitsdaten mit Leistungserbringern wird angenommen, dass diese nicht über ein Vivy-Benutzerkonto verfügen. Ein RSA-Schlüsselpaar muss also temporär erzeugt werden. Der Nutzer muss durch die Angabe der E-Mail-Adresse des Leistungserbringers den Vorgang starten. Dabei bestimmt er auch die Dauer, wie lange seine zu teilenden Gesundheitsdaten abrufbar sein sollen. Zur Auswahl stehen hier 24 Stunden oder dauerhaft, was aber jederzeit widerrufen werden kann. Der Teilungsvorgang erfolgt über eine URL, die im Vivy-Backend erzeugt wird. Diese URL wird auf dem Smartphone des Nutzers angezeigt. Dazu wird auch auf dem Smartphone eine PIN erzeugt und mit der URL dargestellt. Diese Daten zeigt der Nutzer dem Leistungserbringer. Der Leistungserbringer gibt die URL in seinen Webbrowser ein. Dabei wird lokal im Browser eine Anwendung ausgeführt, die ein temporäres RSA-Schlüsselpaar erzeugt, die PIN abfragt und den öffentlichen Schlüssel zusammen mit der PIN an das Vivy-Backend sendet. Dieser Vorgang sowie der öffentliche Schlüssel und die PIN werden der Vivy-App auf dem Smartphone des Nutzers übermittelt, die so Zugriff auf den öffentlichen Schlüssel des Leistungserbringers erhält und die PIN abgleicht. Die zu teilenden Gesundheitsdaten werden nun nach der beschriebenen Methode verschlüsselt und über das Vivy Backend unter der eingangs generierten URL dem Leistungserbringer zur Verfügung gestellt. Da Vivy keine Kontrolle über den Rechner des Leistungserbringers ausübt, geht die Verantwortung im Umgang mit diese Daten zum Leistungserbringer über, der sie in seiner Infrastruktur/Praxis-IT speichern kann. Zukünftig ist anvisiert, dass auch Leistungserbringer ein Vivy Benutzerkonto besitzen. Dann wird das Teilen der Gesundheitsdaten mit Leistungserbringern technisch wie mit anderen Nutzern umgesetzt.

Notfalldatensatz

Der Notfalldatensatz (z.B. Blutgruppe, Erkrankungen, Allergien, Notfallkontakt) kann für den Notfall verfügbar gemacht werden. Dieser wird auf eine andere Art gespeichert als die bisher behandelten Gesundheitsdaten. Da ein potentieller Retter, der Zugriff auf den Datensatz benötigt, nicht erst mit einem asymmetrischen Schlüsselpaar ausgestattet werden kann, und auch der Nutzer keine Interaktion zur Einwilligung a posteriori geben kann, wird hier auf ein anderes Verfahren zurückgegriffen. Dazu wird in den Ressourcen der Vivy GmbH eine URL erstellt. Diese beinhaltet als Pfad zwei Teile, die Code und PIN genannt werden. Diese URL wird in Form eines QR-Codes an den Nutzer geliefert.

Der Nutzer erstellt anhand eines festen Schemas aus dem Code und der PIN einen AES Schlüssel mittels der Schlüsselableitungsfunktion scrypt[7]. Dieser Schlüssel dient zur symmetrischen Verschlüsselung der Gesundheitsdaten im Notfalldatensatz, der unter der URL in den Ressourcen der Vivy GmbH hinterlegt wird.

Ein Retter, der Zugriff auf den Notfalldatensatz benötigt, scannt den QR-Code und erhält so die URL inklusive Code und PIN. Bei Aufruf der URL wird in seinem Browser aus Code und PIN wieder derselbe AES Schlüssel abgeleitet und zur Entschlüsselung des Notfalldatensatzes verwendet. Gleichzeitig wird der Nutzer über den Aufruf des Datensatzes informiert. Sollte der QR-Code unabsichtlich seine Vertraulichkeit verloren haben, kann der Nutzer die URL sperren.

[7] C. Percival, S. Josefsson: The scrypt Password-Based Key Derivation Function, August 2016, IETF, RFC 7914

4 Identitätsmanagement

Datensicherheit beginnt mit der eindeutigen Verifizierung des Nutzers. Schon bei der Registrierung und Anmeldung in der App stellt Vivy daher sicher, dass persönliche Informationen nie in die falschen Hände gelangen.

Registrierung

Damit Nutzer die Dienste von Vivy verwenden können, müssen sie sich einmalig registrieren. Wie bereits oben beschrieben, werden dabei Name und Vorname, Geburtsdatum, E-Mail-Adresse und Telefonnummer, die Krankenversicherung und die Versicherungsnummer des Nutzers von Vivy aufgenommen.

Darüber hinaus werden weitere Daten erzeugt, die bei jeder Verwendung der Vivy App zur Identifikation des Nutzers und der Bindung an das Smartphone verwendet werden. Zunächst muss der Nutzer ein Passwort vergeben, das sicher in der Vivy-Plattform gespeichert wird. Hier kommt das Verfahren PBKDF2-HMAC-SHA-512[8] zum Einsatz, d.h. die Passwörter werden nicht im Klartext gespeichert. Weiter wird ein Geheimnis „S“ für die Authentisierung des Nutzers gegenüber Vivy benötigt. Dieses Geheimnis wird bei jedem Zugriff auf das Vivy-Backend verifiziert, da es als Basis für die Berechnung von Einmal-Passwörtern dient, siehe Abschnitt „Authentisierung“. Daher wird es nach der Erstellung auch an das Vivy Backend übertragen.

Weiter wird im Rahmen des Registrierungsprozesses das Smartphone des Nutzers an den Vivy-Account über die Telefonnummer gebunden. Dazu wird von Seiten des Vivy Backends eine SMS mit einer One-Time-TAN erzeugt und an die vom Nutzer angegebene Nummer versendet. Auf dem Smartphone wird an dieser Stelle das Geheimnis „S“ erzeugt und zusammen mit der empfangenen One-Time-TAN an das Vivy Backend übertragen. Dies muss innerhalb von 30 Sekunden geschehen. Damit ist sichergestellt, dass Nutzer nur über ihr registriertes Smartphone Vivy nutzen können.

Um zu verhindern, dass Gesundheitsdaten von z.B. Ärzten an nicht berechtigte Personen gehen, müssen Nutzer, die diesen Dienst verwenden wollen, zusätzlich ihre bei der Registrierung angegebenen Daten verifizieren. Dies geschieht über ein sogenanntes Videolegitimationsverfahren. Dabei wird der Nutzer aufgefordert, ein kurzes Video von sich und ein Foto des amtlichen Lichtbildausweises (z.B. Personalausweis oder Reisepass) hochzuladen. Danach werden Video und Foto von geschultem Personal abgeglichen.

Authentisierung

Zur Authentisierung des Nutzers gegenüber der Vivy-Infrastruktur kommt, neben der Eingabe des Passwortes, das Verfahren Time-based-One-Time-Passwords (TOTP[9]) zum Einsatz. Dieses generiert auf der Basis eines Geheimnisses Passwörter. Das zugrunde liegende Geheimnis muss auf beiden Seiten der Verifikation bekannt sein, so dass beide dieselben Passwörter berechnen können. Dieses Geheimnis wurde zuvor als „S“ bezeichnet und ist nach der Registrierung auf dem Smartphone und im Vivy Backend verfügbar. Bei jedem Zugriff wird die aktuelle Zeit in einem Intervall von 30 Sekunden zusammen mit „S“ als Eingangswerte für eine Hashfunktion (PBKDF2-HMAC-SHA-256) verwendet, die wiederum in das TOTP-Verfahren eingeht, und so ein Einmalpasswort berechnet. Dies passiert sowohl auf dem Smartphone als auch im Backend. Die Vivy-App überträgt das Passwort mit der Anfrage an das Backend. Nur wenn die Passwörter auf beiden Seiten gleich berechnet wurden, wird der Zugriff erlaubt.

[8] RFC 8018, "PKCS #5: Password-Based Cryptography Specification Version 2.1", January 2017
[9] RFC 6238, "TOTP: Time-Based One-Time Password Algorithm", May 2011

Account-Sperrung und Wiederaufnahme

Bei Verlust seines Smartphones kann der Nutzer seinen Vivy-Account über eine telefonische Hotline sperren. In diesem Fall wird der Account zunächst gesperrt, so dass niemand die Gesundheitsdaten herunterladen oder manipulieren kann.

Key-Recovery

Die medizinischen Daten eines Benutzers sind ausschließlich in Kombination mit dessen privaten RSA-Schlüssel einsehbar, weshalb sämtliche medizinischen Informationen, die in der Vivy-App gespeichert wurden, permanent verloren gehen, wenn ein Benutzer den Zugriff auf seinen privaten RSA-Schlüssel verlieren sollte. Daher werden die Benutzer der Vivy-App bereits bei der Registrierung aufgefordert, ihren privaten RSA-Schlüssel zu exportieren und außerhalb ihres Smartphones zu speichern. Der private RSA-Schlüssel kann in Form von vier QR-Codes[10], beispielsweise als Ausdruck auf Papier oder über eine andere Anwendung wie einer Cloud-Speicherlösung extern gespeichert werden. Wäre diese Möglichkeit der Extraktion nicht gegeben, würde ein Benutzer seine medizinischen Daten in den folgenden Szenarien verlieren:

- bei Verlust des Smartphones
- bei Wechsel des Smartphones

Die einzige andere Möglichkeit, die Daten eines Benutzers über den Wechsel seines Smartphones ohne eine Migration des privaten Schlüssels zu erhalten, wäre ein unverschlüsseltes Backup aller medizinischer Daten, die nicht mehr nur durch den Benutzer selbst entschlüsselt werden können. Folglich ist es im starken Interesse des Benutzers, dass er seinen eigenen privaten RSA-Schlüssel exportieren kann.

Der Backup-Prozess muss auf eine sichere Art und Weise geschehen, da der auf diese Weise extrahierte private RSA-Schlüssel in Kombination mit dem durch die 2-Faktor-Authentifizierung registrierten Smartphones und dem Passwort des Benutzerkontos uneingeschränkten Zugriff auf die medizinischen Daten des Benutzers gewähren. Daher wird das Backup über die Share-Funktion des Betriebssystems des Smartphones realisiert und der Benutzer wird vor dem Backup explizit dazu aufgefordert, den Export über eine sichere, andere Anwendung vorzunehmen und den privaten Schlüssel nicht nur im Download-Verzeichnis des Smartphones zu speichern, da dort andere Anwendungen auf den privaten Schlüssel zugreifen können.

5 Netzwerksicherheit

Für eine sichere Umsetzung des Datenabrufes müssen nicht nur die einzelnen Systeme, wie z.B. die Vivy-App und die Vivy-Server, abgesichert sein, sondern im besonderen Maße auch die Kommunikation zwischen den einzelnen Systemen. Hierzu gehört, neben der Verschlüsselung der Kommunikation über TLS, auch die Authentisierung der Kommunikationspartner. Die von Vivy verwendete Version ist ELBSecurityPolicy-TLS-1-2-2017-01. Sie erlaubt ausschließlich TLS v1.2[11].

Alle Kommunikationswege werden mittels Transport Layer Security (TLS v1.2) gesichert. Diese sind:

- Kommunikationsweg zwischen Nutzer und der Vivy Plattform
- Kommunikationsweg zwischen Leistungserbringern und der Vivy Plattform

[10] ISO/IEC 18004:2015 Information technology -- Automatic identification and data capture techniques -- QR Code bar code symbology specification

[11] RFC 5246, "The Transport Layer Security (TLS) Protocol Version 1.2", August 2008

Alle Daten werden also sowohl verschlüsselt als auch authentisiert übertragen. Zum Einsatz kommen ausschließlich Cipher Suites, die vom BSI in BSI-TR 02102-2[12] empfohlen sind.

Nutzer authentisieren sich gegenüber der Vivy Plattform mittels Passwort und durch Nachweises des Besitzes des Geheimnisses „S“, welches bei der Registrierung an das Smartphone gebunden wurde. Die anderen Kommunikationspartner authentisieren sich mittels TLS-Server-Zertifikate. Es findet also immer eine gegenseitige Authentisierung statt.

6 Plattformsicherheit

Alle Systeme wurden von Anfang an in Hinblick auf die sichere Umsetzung entworfen. Hierzu zählen nicht nur die verwendeten kryptographischen Verfahren, sondern auch die in diesem Abschnitt beschriebenen technischen Maßnahmen zur Absicherung der Plattform.

Technische Sicherheit

Die Vivy GmbH nutzt die Cloud-Computing-Umgebung der Amazon Web Services, Inc. (AWS) Region Frankfurt. Diese erfüllt die Standards ISO-27001 (Informationssicherheitsmanagement), ISO-9001 (Qualitätsmanagement), wie auch die BSI-Standards 200-1 (Managementsysteme für Informationssicherheit) und BSI 200-2 (IT-Grundschutz-Methodik), was durch entsprechende Zertifikate bestätigt wurde. Zudem verfügt AWS über ein Testat unabhängiger Wirtschaftsprüfer, das die Entsprechung des „Anforderungskatalog Cloud Computing (C5)“ vom BSI bestätigt. Die Nutzung der AWS Cloud-Computing-Umgebung erfüllt ebenso die technischen Anforderungen unserer Partner BITMARCK Holding GmbH sowie Allianz SE. Beide haben dies in gesonderten Prüfverfahren verifiziert und bestätigt. Die Datenspeicherung wird mit Hilfe der “Simple Storage Service” (kurz S3) Cloud-Speicher-Plattform realisiert.

Damit ist die Wahrscheinlichkeit, dass Angreifer in das System eindringen können, extrem gering. Weiter ist sichergestellt, dass unser Service hochverfügbar ist.

Softwarequalität und Penetrationstest

Wir legen bei der Entwicklung großen Wert auf die Qualität der Software. Unsere Software durchläuft deshalb einen definierten Qualitätssicherungsprozess, welcher sowohl automatisierte als auch manuelle Tests enthält.

Aber selbst mit intensiven Tests und klaren Spezifikationen können Fehler nicht vollständig ausgeschlossen werden. Aus diesem Grund lassen wir regelmäßig Penetrationstests durchführen, um Sicherheitslücken frühzeitig erkennen und beheben zu können.

Des Weiteren wurde ein öffentliches Sicherheitsprogramm aufgesetzt. Bei diesem Programm können sich unabhängige Fremdpersonen beteiligen und werden für das Finden und Bekanntgeben von Fehlern, welche die Sicherheit unserer Software betreffen, belohnt.

Systemzugang

Die Systemwartung und -pflege erfolgt durch Administratoren der Vivy.

7 Datenschutz

Konform zur neuen Datenschutz-Grundverordnung der Europäischen Kommission hat Vivy einen Datenschutzbeauftragten bestellt. Der Datenschutzbeauftragte wird von einem Team aus

[12] BSI: TR 02102-2, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 – Verwendung von Transport Layer Security (TLS), Version 2018-02, Bundesamt für Sicherheit in der Informationstechnik.

qualifizierten Mitarbeiterinnen und Mitarbeitern unterstützt. Hinsichtlich Datensicherheit arbeitet das Datenschutzteam eng mit dem Sicherheitsteam von Vivy zusammen.

Im Rahmen der Vivy-App werden ausschließlich Daten erhoben, die für die Funktionalitäten von Vivy erforderlich sind. Welche Daten zu welchem Zweck erhoben werden, ist in der Datenschutzerklärung der Vivy-Webseite und der Datenschutzerklärung der Vivy-App ersichtlich.

Durch das Design der Systemarchitektur entscheidet ausschließlich der Nutzer von Vivy darüber, welche Daten in seinem Vivy-Nutzerkonto erfasst werden, mit wem er diese Daten teilen möchte und wann diese wieder gelöscht werden. Andere Teilnehmer der Plattform können keine Änderungen an den Gesundheitsdaten des Nutzers vornehmen und können ausschließlich durch eine Einladung des Nutzers Gesundheitsdaten im Vivy-Konto des Nutzers ablegen.

Die Gesundheitsdaten des Nutzers werden ausschließlich verschlüsselt im Nutzerkonto der Vivy-Plattform gespeichert. Der private Schlüssel zum Entschlüsseln der Gesundheitsdaten ist nur dem Nutzer selbst zugänglich und sicher auf dem Smartphone des Nutzers hinterlegt.

Die Gesundheitsdaten sind sowohl im Datenspeicher des Vivy-Backend als auch während der Übertragung durch Verschlüsselung vor unbefugtem Zugriff geschützt. Auch Mitarbeiter der Vivy GmbH oder Betreiber des Rechenzentrums können die verschlüsselten Daten nicht einsehen. Dritte könnten diese, selbst wenn sie in deren Besitz kommen sollten, ebenfalls nicht einsehen.

8 Sicherheitsmanagement

Neben dem Einsatz kryptographischer Algorithmen zur Absicherung der Daten müssen auch weitere technische sowie organisatorische und personelle Maßnahmen für den sicheren Betrieb von Vivy umgesetzt werden.

Die notwendigen Sicherheitsmaßnahmen werden nicht nur von unseren kompetenten Mitarbeiterinnen und Mitarbeitern entwickelt und umgesetzt, sondern auch von externen Unternehmen auf Vollständigkeit und Wirksamkeit evaluiert. Die Erarbeitung der notwendigen umzusetzenden Sicherheitsmaßnahmen erfolgt nach etablierten Vorgehensmodellen. Hierzu gehören, neben der Umsetzung und dem regelmäßigen Audit aktueller Sicherheitsmaßnahmen auch Aktivitäten zur Aufrechterhaltung im laufenden Betrieb (z.B. Notfallmanagement, Vorgehen bei Sicherheitsvorfällen und Anpassungen der Maßnahmen hinsichtlich der aktuellen Sicherheitslage). Darüber hinaus betreiben wir ein Bug-Bounty-Programm.

Sicherheitsteam

Unser Sicherheitsteam besteht aus einem Informationssicherheitsbeauftragten, welcher die Sicherheitsprozesse steuert und weiteren Sicherheitsexpertinnen und –experten. Das Sicherheitsteam erarbeitet die organisatorischen technischen und infrastrukturellen Sicherheitsmaßnahmen und überwacht die Umsetzung dieser Maßnahmen und deren Aufrechterhaltung im laufenden Betrieb. In diesem Zusammenhang führt das Sicherheitsteam regelmäßig interne Audits durch, steuert das Schulungsprogramm unserer Mitarbeiter und führt Anpassungen der Sicherheitsmaßnahmen in Abhängigkeit von der aktuellen Sicherheitslage durch.

Zuverlässigkeitsüberprüfungen der Mitarbeiterinnen und Mitarbeitern

Vor der Einstellung neuer Mitarbeiter prüfen wir eingehend deren Qualifikation hinsichtlich der zu verantwortenden Aufgaben. Dabei berücksichtigen wir unter anderem die Ausbildung aber auch die vorangehenden Anstellungen und prüfen diese anhand der Ausbildungs- und Arbeitszeugnisse. Jedes neue Teammitglied verpflichte sich zudem zur Einhaltung unserer Sicherheitsvorschriften und wird

im Rahmen seiner Einstellung hinsichtlich der IT-Sicherheit und des Datenschutzes geschult. Darüber hinaus werden alle zukünftigen Mitarbeiterinnen und Mitarbeiter ein polizeiliches Führungszeugnis vorlegen.

Sicherheitsschulungen

Mitarbeiter müssen für relevante Gefährdungen sensibilisiert werden und wissen, wie sich diese auf ihre Institution auswirken können. Wir führen aus diesem Grund regelmäßig Sicherheitsschulungen für die Themen IT-Sicherheit und Datenschutz durch, um die Wahrnehmung der Mitarbeiter für sicherheitskritische Situationen und ihre Auswirkungen zu schärfen und die notwendigen Kenntnisse und Kompetenzen für sicherheitsbewusstes Verhalten sicher zu stellen. Dabei berücksichtigt unser Schulungsprogramm unterschiedliche Zielgruppen mit deren Fähigkeiten und Arbeitsabläufen und ist sowohl für das technische Personal (z.B. Systemadministratoren und Entwickler) als auch für Mitarbeiter der Verwaltung verpflichtend. So weiß jeder aus unserem Team, was von ihm im Hinblick auf Informationssicherheit erwartet wird und wie er in sicherheitskritischen Situationen reagieren sollte.

Schwachstellenmanagement und Vorgehen bei Sicherheitsvorfällen

Software kann Fehler enthalten, welche im Zweifel auch zu Sicherheitslücken führen können. Typischerweise ergibt sich im laufenden Anwendungsbetrieb daher die Notwendigkeit, die Anwendung funktional anzupassen, Fehler zu beheben oder Sicherheitslücken zu schließen. Ebenso gilt dies für personelle, organisatorische, technische oder infrastrukturelle Sicherheitsmaßnahmen. Trotz der Evaluierung dieser Maßnahmen hinsichtlich ihrer Sicherheitsfunktion können sich Sicherheitslücken ergeben, die im Rahmen der Evaluierung nicht erkannt wurden.

Unser Sicherheitsteam prüft aus diesem Grund regelmäßig die Wirksamkeit der umgesetzten Maßnahmen. Neben regelmäßigen internen Audits simulieren wir auch eigene Angriffe (z.B. Hacking oder Phishing-Angriffe) um die Wirksamkeit unserer Sicherheitsmaßnahmen und -schulungen zu testen.

Werden uns Sicherheitslücken bekannt, z.B. durch eigene Beobachtungen oder aus tatsächlichen Angriffen, sind wir hierauf vorbereitet.

Unser Sicherheitsteam hat im Rahmen seiner Funktion bereits mögliche Angriffsszenarien durchgespielt und entsprechende Gegenmaßnahmen vorbereitet. Dazu gehört z.B. die kurzfristige Abschaltung sicherheitskritischer Dienste aber auch Abschaltung der gesamten Plattform, bis die Sicherheit wieder hergestellt ist.

Darüber hinaus beobachten wir regelmäßig sowohl mit unserem Sicherheitsteam als auch automatisiert die aktuelle Sicherheitslage und informieren uns, z.B. über das Computer Emergency Response Team des Bundesamtes für Sicherheit in der Informationstechnik, über aktuelle Sicherheitslücken und Angriffe und leiten entsprechende Gegenmaßnahmen ein.

Bug-Bounty-Programm

Für ein professionelles Sicherheitsmanagement ist ein Prozess für die Reaktion auf das Bekanntwerden oder das Auftreten von Sicherheitsvorfällen notwendig. Noch einen Schritt weiter gehen sogenannte Bug-Bounty-Programme. Diese institutionalisieren nicht nur den Umgang mit Sicherheitslücken, sie geben Sicherheitsforschern auch konkrete Anreize verantwortungsvoll mit gefundenen Problemen umzugehen.

Ein Bug-Bounty-Programm ist ein klares Zeichen, dass ein Verständnis für den souveränen Umgang mit Sicherheitslücken vorhanden ist. Das Aufzeigen von Lücken wird nicht mit juristischen

Maßnahmen unterbunden, sondern durch zumeist monetäre Anreize kanalisiert. Das Melden von Sicherheitslücken wird also belohnt und die Lücken können behoben werden, bevor diese veröffentlicht werden. Nach Absprache kann eine Veröffentlichung nach Beheben der Lücke erfolgen. Gleichzeitig ist so ein Programm auch Teil der gesamten Sicherheitsstrategie. Es werden kontinuierlich die Systeme der Allgemeinheit zum Testen auf Sicherheitslücken zur Verfügung gestellt. Dies kommuniziert, dass der Betreiber sich sicher ist, alles nach dem Stand der Technik abgesichert zu haben und diesen Zustand auch kontinuierlich weiter erhalten wird.

Vivy bietet über die hackerone-Plattform[13] ein Bug-Bounty-Programm an.

9 Sicherheits- und Datenschutzevaluierungen

Die Infrastruktur der Vivy GmbH wird regelmäßig von unabhängigen Unternehmen geprüft und zertifiziert. Sowohl hinsichtlich Anwendungsarchitektur, Verschlüsselungstechnologien als auch gegenüber verschiedener Angriffsszenarien wurden die hohen Standards an Datensicherheit innerhalb der Vivy-App mehrfach bestätigt.

Neben den in Abschnitt Plattformsicherheit aufgeführten Evaluierungen hinsichtlich IT-Sicherheit, die der von Vivy genutzte AWS erfüllt, wird auch die Vivy-App regelmäßig eingehend untersucht. Darüber hinaus werden Sicherheitstests von renommierten Experten durchgeführt.

Zertifikat des TÜV Rheinland

Der TÜV Rheinland hat die Vivy-App (iOS/Android) geprüft und als *Sichere Mobile Applikation* zertifiziert[14]. Nutzer von Smartphones oder Tablets erkennen an diesem Prüfzeichen, dass eine mobile Applikation auf Sicherheitslücken und Schwachstellen geprüft ist. Dazu analysieren die Experten des TÜV Rheinland den Entwicklungsprozess, das Applikations-Design, den Quellcode und die zum Betrieb der Vivy-App notwendige Backend-Infrastruktur. Die Zertifizierungsstelle der TÜV Rheinland i-sec GmbH bescheinigt der Vivy-App folgende Eigenschaften:

- Die Integrität, Authentizität und die Vertraulichkeit von sensiblen Daten ist durch eine verschlüsselte Kommunikation gemäß dem Stand der Technik geschützt.
- Die Integrität, Authentizität und die Vertraulichkeit von sensiblen Daten ist durch eine verschlüsselte Speicherung gemäß dem Stand der Technik geschützt.
- Die App nutzt im Rahmen Ihrer Funktionalität angemessene Berechtigungen.

Die Wirksamkeit der Schutzmaßnahmen wird durch die TÜV Rheinland i-sec GmbH regelmäßig überwacht.

Penetrationstests

Für die Vivy-App (iOS und Android) und das Vivy-Backend wurden durch externe Dienstleister Penetrationstests aus unterschiedlichen Perspektiven durchgeführt, indem unterschiedliche Angriffsszenarien simuliert wurden:

- durch einen Angreifer, der selbst nicht im Besitz von Zugangsdaten ist und der Schwachstellen zu finden versucht, um sich Zugang zu persönlichen Daten eines Benutzers zu verschaffen
- durch einen Angreifer, der selbst im Besitz von Zugangsdaten ist und der Schwachstellen zu finden versucht, um seine Zugriffsrechte zu erhöhen

[13] https://hackerone.com/vivy

[14] Zertifikat: Sichere Mobile Applikation. [Online] https://www.certipedia.com/quality_marks/0000062427.

Die Penetrationstests der Android-Version, der Vivy-App und des Backends wurden durch ein Security Unternehmen in Frankfurt am Main, Hessen durchgeführt. Die Penetrationstests der iOS-Version wurden durch die ERNW Enno Rey Netzwerke GmbH durchgeführt.

Lokale Auftragsdatenverarbeitung nach deutschen Datenschutzbestimmungen

AWS garantiert die lokale Auftragsdatenverarbeitung nach deutschen Datenschutzbestimmungen in Deutschland selbst (Region Frankfurt). Die genutzten Services befinden sich ausschließlich in Frankfurt und die Daten werden nicht auf ausländischen Servern gespeichert oder verarbeitet.

AWS sichert für die eingesetzte Cloud-Speicher-Plattform S3 umfassende Sicherheits- und Compliance-Funktionen zu:

- Das Unternehmen besitzt mehrere regionale Verfügbarkeitszonen, die den lokalen Datenschutzbestimmungen unterliegen. Dies gewährleistet der Vivy GmbH die Behandlung der Daten gemäß deutscher Datenschutzbestimmungen sowie die Speicherung innerhalb der Landesgrenzen.
- S3 bietet eine ausgefeilte Integration in AWS Cloud Trail zur Protokollierung, Überwachung und Aufbewahrung von Speicher-API-Aufrufen für Auditing-Zwecke.
- S3 unterstützt Standards und Compliance-Zertifizierungen, darunter DSGVO, PCI-DSS, HIPAA/HITECH, FedRAMP und FISMA. Dies unterstützt, die Compliance-Anforderungen für nahezu jede Regulierungsbehörde der Welt zu erfüllen.

Privacy Siegel der Vivy App

Im Rahmen von ePrivacyApp wurde die Vivy-App (iOS und Android) durch die ePrivacyseal GmbH umfassende hinsichtlich des Datenschutzes und der Sicherheit der Daten geprüft und mit dem Datenschutz-Gütesiegel ePrivacyApp Health zertifiziert[15]. Das Prüfergebnis bescheinigt der Vivy App folgende Eigenschaften:

- Die geprüfte App entspricht dem Kriterienkatalog „ePrivacyApp“ der ePrivacyseal GmbH
- Die Daten werden entsprechend des aktuellen Standes der Technik verschlüsselt
- Es kommt zu keinen vom App-Nutzer unerwünschten Datenverarbeitungsvorgang
- Nach Auffassung der ePrivacyseal GmbH sind die Anforderungen an Datensicherheit nach aktuellem Stand der Technik erfüllt.

10 Verwendung von Analytics-Diensten

Mit der Nutzung von Analytics-Diensten kann das Nutzerverhalten analysiert werden und damit der Service sowie die Qualität und Nutzbarkeit der Vivy-App verbessert werden. Dabei ist explizit zu erwähnen, dass keine Gesundheitsdaten davon betroffen sind. Die Verwendung von Analytics-Diensten ist für jeden Nutzer freiwillig: Beim Erstaufruf der App wird gefragt, ob der Nutzer damit einverstanden ist, dass Analyse- und Trackingdienste Daten erheben und diese zur Analyse zur Vivy GmbH schicken. Hier geht es ausschließlich um Daten zur Verbesserung der App-Usability. Im Folgenden beschreiben wir, welche Analytic-Dienste Vivy einsetzt, wozu wir diese konkret nutzen und welche Daten dabei anfallen.

Mixpanel

Mixpanel bietet eine Geschäftslösung für erweiterte Produktanalyse. Es ermöglicht, besser zu verstehen, wie Nutzer sich mit dem Produkt auseinandersetzen. Besonders bei elektronischen

[15] Datenschutz-Gütesiegel ePrivacyApp. [Online] https://www.eprivacy.eu/kunden/vergebene-siegel/firma/uvita-gmbh/.

Produkten bietet sich dies an, da der digitale Fingerabdruck sehr leicht zu verfolgen ist. So kann ersichtlich gemacht werden, was Nutzer ansprechend fanden, was sie dazu bewegt hat das Produkt weiter zu nutzen oder bei welchem Schritt sie aufgehört haben sich mit dem Produkt zu befassen.

Die Produktanalyse teilt sich hierbei in zwei grundlegende Bereiche:

- Datenerhebung: Aufrufe von Seiten, Events und Nutzeraktionen werden aufgezeichnet
- Datenanalyse: Die erhobenen Daten werden analysiert und übersichtlich dargestellt über Dashboards und Reports.

Zusätzlich bietet Mixpanel zusätzliche Funktionen wie z.B. A/B Tests an, um die Nutzerführung weiter zu verbessern.

In Vivy wird Mixpanel hauptsächlich genutzt, um den Anmeldeprozess der Nutzer nachzuvollziehen. Insbesondere von Interesse ist, an welchem Punkt Nutzer den Anmeldeprozess abbrechen. An dieser Stelle könnte der Anmeldeprozess dann angepasst werden z.B. durch klarere Sprache, übersichtlichere Bildschirmführung usw.

Andere Vorgänge werden ebenso erfasst, um die Benutzerführung innerhalb der App zu verbessern oder festzustellen, welche Funktionen besonders gefragt sind.

Mixpanel schickt Daten im JSON-Format. Gesendet werden nicht-sensible Daten über das Telefon, Betriebssystem und App-Version, sowie alle Schritte in den Prozessen der Vivy-App.

Crashlytics

Crashlytics Hauptprodukt ist ein Software Development Kit (SDK) für Crashreports, Anwendungslogging, Onlinereviews und statische Analyse von Anwendungslogs. Crashlytics wurde 2017 von Google erworben. Für einen stabilen Betrieb der Vivy App wird Crashlytics folgendermaßen genutzt: Im Falle eines App-Absturzes sendet Crashlytics Absturz-relevante Daten an die Entwickler, um die Absturzursache zeitnah beheben zu können. In der Vivy-App werden nur die von Crashlytics voreingestellten Daten verschickt: Daten über das Telefon und dessen aktuellen Zustand, das Betriebssystem, App-Status und in welchem Ausführungsschritt die App war. Wenn die App einen Fehler festgestellt hat, wird dieser ebenfalls mitgesendet. Nur durch Beschreibungs-Texte des Fehlers könnten Nutzerdaten mitgesandt werden, wenn die Fehlermeldung sie mitführt. Die Entwickler selbst haben Sorge zu tragen, dass Fehlermeldungen keine Nutzerdaten enthalten.

Crashlytics kann die Daten zu übersichtlichen Reports aufbereiten, um Ursprünge von Abstürzen besser nachzuvollziehen.

Glossar

AES: Advanced Encryption Standard ist ein symmetrisches Verschlüsselungsverfahren, d. h. der Schlüssel zum Ver- und Entschlüsseln ist identisch.

Authentifizierung: ist ein elektronischer Prozess, der die Bestätigung der elektronischen Identifizierung einer natürlichen oder juristischen Person oder die Bestätigung des Ursprungs und der Unversehrtheit von Daten in elektronischer Form ermöglicht.

Authentifizierungsfaktor: ist ein Element, das nachweislich mit einer Person verknüpft ist und (mindestens) einer der folgenden Kategorien angehört:

- besitzabhängiger Authentifizierungsfaktor (Besitz) ist ein Authentifizierungsfaktor, dessen Besitz der Nutzer nachweisen muss;

- kenntnisabhängiger Authentifizierungsfaktor (Wissen) ist ein Authentifizierungsfaktor, dessen Kenntnis der Nutzer nachweisen muss;
- „inhärenter Authentifizierungsfaktor“ (Inhärent) ist ein Authentifizierungsfaktor, der auf ein körperliches Merkmal einer natürlichen Person abstellt und bei dem der Nutzer nachweisen muss, dass er dieses körperliche Merkmal hat

Benutzer/Nutzer: ist eine bei Vivy registrierte Person.

BSI: Das Bundesamt für Sicherheit in der Informationstechnik ist eine in der Bundesstadt Bonn ansässige zivile obere Bundesbehörde im Geschäftsbereich des Bundesministeriums des Innern, die für Fragen der IT-Sicherheit zuständig ist.

Gesundheitsdaten: „personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen“[16]

Leistungserbringer: Arzt, Apotheker, Heilpraktiker. Alle zur Abrechnung von Leistungen gegenüber den Krankenkassen und Versicherungen berechtigten.

RSA: RSA ist ein asymmetrisches kryptographisches Verfahren. Es verwendet ein Schlüsselpaar, bestehend aus einem privaten Schlüssel, der zum Entschlüsseln von Daten verwendet wird, und einem öffentlichen Schlüssel, mit dem man verschlüsselt. Der private Schlüssel wird geheim gehalten und kann nur mit extrem hohem Aufwand aus dem öffentlichen Schlüssel berechnet werden.

TLS: Transport Layer Security ist ein hybrides Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet. Aktuell ist Version 1.2.

Vivy-Benutzerkonto: ist die Zugangsberechtigung eines Benutzers zur Vivy-Plattform.

Vivy-App: ist eine Software für Smartphones, mit der sich Nutzer sowohl mit E-Mail/Passwort als auch mit einer Zwei-Faktor-Authentisierung gegenüber Vivy authentisieren können.

Vivy-Plattform: ist das Gesamtsystem aus Vivy-App, Vivy-Backend und den Ressourcen der Vivy GmbH.

Zwei-Faktor-Authentisierung (2FA): bezeichnet, bezeichnet den Identitätsnachweis eines Nutzers mittels der Kombination zweier unterschiedlicher und insbesondere unabhängiger Authentifizierungsfaktoren.

[16] Art. 4 Z 15 DSGVO 2016/679