



Datenschutzerklärung «UZH Wallet Pilot» App

Die Wirtschaftswissenschaftliche Fakultät (WWF) der Universität Zürich (UZH) freut sich über Ihr Interesse an der «UZH Wallet Pilot» App. Da Datenschutz für die UZH ein wichtiges Anliegen ist, möchten wir Sie im Folgenden darüber unterrichten, welche Daten die UZH im Rahmen der geltenden datenschutzrechtlichen Bestimmungen von Nutzenden der «UZH Wallet Pilot» App zu welchem Zweck erhebt, weiterbearbeitet und bekannt gibt, wie lange die Daten gespeichert werden und welche Massnahmen getroffen worden sind, um für die Sicherheit dieser Daten zu sorgen.

1.1 «UZH Wallet Pilot» App

1.1.1 Ziel und Zweck der «UZH Wallet Pilot» App

Die Vision des Projekts «UZH Wallet» App ist es, in einem Open Innovation Prozess zu testen, wie eine auf der Technologie der «Selbstbestimmten Identität» (engl. Self-Sovereign Identity (SSI)) basierende mobile Brieftasche, die den Besitzenden der Brieftasche (z.B. Studierenden) die vollständige Kontrolle über ihre Daten gibt, aufgebaut sein könnte.

Die App kann sogenannte verifizierbare digitale Nachweise (engl. verifiable credentials (VC)) empfangen, speichern, verwalten und an Dritte präsentieren. Solche VC können beispielsweise ein digitaler Studierendenausweis (nachfolgend «UZH Student ID») sowie Leistungsausweise (z.B. Masterdiplom) sein.

In einem ersten Schritt dieses offenen Innovationsprozesses testet das Dekanat der Wirtschaftswissenschaftlichen Fakultät (WWF) die «UZH Student ID» in der «UZH Wallet Pilot» App. Es handelt sich um einen Pilotversuch, bei dem Erkenntnisse aus dem UZH Blockchain Center, praktische Lösungen der Projektpartnerin Procivis sowie Anforderungen aus Sicht Management und Nutzenden zusammengeführt werden.

1.1.2 Partner und Technologie

Die WWF arbeitet in dem Projekt zusammen mit Procivis, einem Schweizer Technologieunternehmen der Orell Füssli zur Digitalisierung von Dienstleistungen im öffentlichen Sektor. Diese wird für gewisse Dienstleistungen durch die Swisscom unterstützt.

Die «UZH Wallet Pilot» App basiert auf den Kernprinzipien der Blockchain-Technologie: dezentrale Datenspeicherung, Selbstkontrolle über persönliche Daten und die Anwendung höchstmöglicher Sicherheitsstandards. Die Blockchain ermöglicht es Dritten (z.B. Mensa, Bibliothek), ihnen vorgelegte VC zu verifizieren, ohne auf die Infrastruktur eines zentralen Anbieters (sog. Identity Provider) oder eines Ausstellers von VC angewiesen zu sein. Die Blockchain wird auch zur Aufzeichnung von Berechtigungsschemata, Widerrufsinformationen, öffentlichen Schlüsseln von vertrauenswürdigen Parteien und öffentlichen dezentralen Identifikatoren verwendet. Die «UZH Wallet Pilot» App wird Schemata und sog. «Decentralized Identifiers» (DID) erstellen, die auf der Hyperledger Indy Blockchain (vorzugsweise eine IDunion Test Net-Infrastruktur) basieren, die von Swisscom bereitgestellt wird.

Die «UZH Wallet Pilot» App wird von der bestehenden White-Label-Lösung «SSI+Wallet» von Procivis abgeleitet. Die «UZH Wallet Pilot» App verwendet als Blockchain-Infrastruktur offene Hyperledger Aries-Protokolle, und ist eine React Native-Mobilanwendung, die auf iOS und Android genutzt werden kann. Als Ableger von Hyperledger Indy bietet Aries die stärksten





Datenschutzgarantien, Interoperabilität und Ausgereiftheit. Im Projekt wird mit «Anoncreds» als bevorzugtem VC-Typ gearbeitet, da es sich dabei um einen nicht korrelierenden Berechtigungsnachweis handelt, was bedeutet, dass Nutzende nicht über verschiedene Dienste hinweg getrackt werden können.

1.1.3 VC 1: «UZH Student ID»

Um die «UZH Student ID» in der «UZH Wallet Pilot» App zu erhalten, laden die Studierenden zunächst die «UZH Wallet Pilot» App aus dem «Testflight»-Stores von Apple bzw. dem entsprechenden Test Store von Google herunter. Danach legen die Studierenden einen Sicherheits-PIN-Code fest. Der Code wird auf dem Smartphone gespeichert und wird mit Löschen der Wallet bzw. der App entfernt. Für den Schutz und die Sicherheit der Login-Angaben gilt das Reglement über den Einsatz von Informatikmitteln (REIM).

Die WWF als Ausstellerin der VC stellt eine neue «UZH Student ID» in der «UZH Desk» Web Applikation aus, indem sie folgende Daten des/der Studierenden einträgt:

- Name und Vorname
- Geburtsdatum
- Matrikelnummer
- Studienprogramm
- Fakultät
- Sonderrabatt
- Gültigkeit
- Portraitfoto

Die Daten werden auf UZH-eigenen Servern gespeichert.

Die Studierenden öffnen anschliessend ihre «UZH Wallet Pilot» App und scannen den QR-Code, der nach Abschliessen des Eintrags in der «UZH Desk» App erscheint. Die Studierenden erhalten in der «UZH Wallet Pilot» App eine Ausgabeaufforderung, um den Empfang der «UZH Student ID» zu genehmigen. Nach der Genehmigung wird die «UZH Student ID» als VC in der «UZH Wallet Pilot» App gespeichert. Die Daten sind auf dem Smartphone gespeichert und werden mit Löschen der Wallet bzw. der App entfernt.

Die Studierenden haben so die Möglichkeit, sich beispielsweise in Mensen, Bibliotheken oder für eine Veranstaltung mittels Strichcode auszuweisen, ohne die Daten an diese Anbieter weiterzugeben. Das Ausweisen bei Dritten mittels «UZH Student ID» wird weder systemtechnisch erfasst noch gespeichert.

1.1.4 VC 2: Leistungsausweise

Die WWF als Ausstellerin der VC stellt im Rahmen des Pilotprojekts Beispiele von Leistungsausweisen in der «UZH Desk» Web Application aus. Für die «UZH Wallet Pilot» App können folgende VC mit den entsprechenden Daten (Attributen) ausgestellt werden:

Masterdiplom:

- Name
- Vorname
- Geburtsdatum
- Ausstellungsdatum
- Art des Studiengangs



- Fakultät
- Major Studienprogramm
- Major-Note
- Minor Studienprogramm
- Minor Note
- Prädikat
- Gesamtnote

Leistungsausweis (Transcript of Records):

- Nachname
- Vorname(n)
- Geburtsdatum
- Matrikelnummer
- Studiengang
- Major
- Minor
- Beispiel absolvierte Leistung(en)
- Modulbezeichnung
- Titel des Moduls
- Status
- ECTS Credits
- Note
- Leistungsausweis Nr.
- Fakultät

Die Studierenden öffnen anschliessend ihre «UZH Wallet Pilot» App und scannen den QR-Code, der nach Abschliessen des Eintrags in der «UZH Desk» App erscheint. Die Studierenden erhalten in der «UZH Wallet Pilot» App eine Ausgabeaufforderung, um den Empfang der des Leistungsausweises zu genehmigen. Nach der Genehmigung wird der Leistungsausweis als VC in der «UZH Wallet Pilot» App gespeichert. Die Daten sind auf dem Smartphone gespeichert und werden mit Löschen der Wallet bzw. der App entfernt. Die Leistungsausweise werden im Rahmen des Pilotprojekts als Beispiel verwendet und sind nur für die befristete Verwendung im Rahmen des Pilotprojekts verfügbar. Die Studierenden haben im Rahmen des Pilotversuchs die Möglichkeit, den Leistungsausweis z.B. im Rahmen eines fingierten Bewerbungsprozesses weiterzusenden. Dabei werden nur die von der jeweiligen Person freigegebenen Daten des Diploms oder des Leistungsausweises übermittelt. Das Ausweisen bei Dritten mittels «UZH Student ID» wird weder systemtechnisch erfasst noch gespeichert. Im Übrigen gelten die gültigen Regelungen der Vertraulichkeit sowie Datenschutzrichtlinien von Bewerbungen.

1.2 Datenschutz

1.2.1 Gegenstand des Datenschutzes

Datenschutz dient dem Schutz der Persönlichkeitsrechte. Er verpflichtet die Datenbearbeitenden zu rechtmässigem Handeln und verleiht den betroffenen Personen durchsetzbare Rechte im Hinblick auf die Bearbeitung ihrer Personendaten. Personendaten sind nach § 3 [Gesetz über die Information und den Datenschutz des Kantons Zürich \(IDG ZH\)](#) alle Informationen, die sich auf eine bestimmte



oder bestimmbare Person beziehen. Hierunter fallen z.B. Angaben wie Name, Anschrift, Telefonnummer, E-Mail- oder IP-Adresse.

1.2.2 Datenerhebung, -bearbeitung, -speicherung

Personendaten fallen nur bei der Benutzung der «UZH Wallet Pilot» App im Zusammenhang mit der Kommunikation mit den Webservern der UZH an. Es werden folgende Zugriffsdaten erhoben und in einer Webserver-Logdatei auf Servern der UZH gespeichert:

- die IP-Adresse des anfordernden Rechners (z.B. 123.456.97.36)
- die Adresse (URL), die von der «UZH Wallet Pilot» App angefordert wurde
- der Pfad und der Name des angeforderten Dienstes der «UZH Wallet Pilot» App
- das Datum und die Uhrzeit der Anforderung
- die übertragene Datenmenge
- der Zugriffsstatus
- die Zugriffsart
- die Beschreibung des verwendeten Betriebssystems
- die Session-ID
- Seriennummer des anfordernden Rechners

Die Bearbeitung dieser Daten erfolgt zu folgenden Zwecken:

- Sicherstellung der Netzinfrastruktur und der technischen Administration
- Optimierung der Nutzung des Angebotes
- Identifikation und Nachverfolgung unzulässiger Zugriffsversuche

Die Webserver-Logdateien werden ab Beendigung des Zugriffs für einen Zeitraum von 6 Monaten gespeichert. Danach werden die Webserver-Logdateien automatisch gelöscht, soweit nicht ein erkannter Angriff auf unsere Netzinfrastruktur zu einer zivil- oder strafrechtlichen Verfolgung des/der Angreifenden führt und damit eine weitere Speicherung erforderlich macht. Auf dem mobilen Gerät selbst werden keine Personendaten gespeichert.

1.2.3 Bekanntgabe von Personendaten

Personendaten werden ausschliesslich dann an Dritte (z.B. an andere Behörden) bekannt gegeben, soweit dies im Rahmen zwingender Rechtsvorschriften (z.B. behördlichen Aufforderungen, Gerichtsbeschlüssen) oder zum Zweck der Rechts- oder Strafverfolgung (z.B. im Fall von Angriffen auf die UZH-Netzinfrastruktur) erforderlich ist. Eine Bekanntgabe an Dritte zu anderen Zwecken findet nicht statt.

Dessen ungeachtet, kann die WWF Dienstleistende damit beauftragen, die über die «UZH Wallet Pilot» App erhobenen Daten zu den oben genannten Zwecken weiter zu bearbeiten. Die UZH und die beauftragten Dienstleistenden werden mittels rechtlicher, technischer und organisatorischer Massnahmen dazu verpflichtet, die Einhaltung datenschutzrechtlicher Bestimmungen zu gewährleisten.

1.2.4 Tracking-Einstellungen

Zur Verbesserung der technischen Stabilität der «UZH Wallet Pilot» App durch Überwachung der Systemstabilität und Ermittlung von Codefehlern verwenden wir den Dienst Sentry (Sentry, 1501 Mariposa St #408, San Francisco, CA 94107, USA). Sentry dient alleine diesen Zielen und wertet



keine Daten zu Werbezwecken aus. Die Daten der Nutzenden, wie z.B. Angaben zum Gerät oder Fehlerzeitpunkt, werden anonym erhoben und nicht personenbezogen genutzt sowie anschliessend gelöscht. Weitere Informationen hierzu finden Sie in der Datenschutzerklärung von Sentry: <https://sentry.io/privacy>

1.2.5 Querverweise (Links) zu Webseiten

Die vorliegende Datenschutzerklärung gilt nur für die «UZH Wallet Pilot» App. Für allfällige Webseiten der UZH, die in dieser App verlinkt und in einem Browser aufgerufen werden können, verweisen wir auf die Datenschutzerklärung der UZH-Webseiten. Diese finden Sie unter www.uzh.ch/de/privacy. Für allfällige externe Webseiten möchten wir Sie bitten, die Datenschutzerklärungen und Sicherheitsbestimmungen der anderen App-Anbieter zu beachten. Die UZH ist weder für den Inhalt noch die Datenschutzpraxis dieser Anbieter verantwortlich. Insbesondere kann die UZH nicht gewährleisten, dass die Inhalte anderer Anbieter frei von Malware sind.

1.2.6 Push-Benachrichtigungen

Unser Angebot umfasst sogenannte Push-Benachrichtigungen für die Mitteilung, dass neue VC in der «UZH Wallet Pilot» App bereitstehen. Um Push-Benachrichtigungen erhalten zu können, müssen Sie diese in den Einstellungen Ihres Betriebssystems aktivieren. Sie haben die Möglichkeit, diese Funktion jederzeit zu deaktivieren oder wieder zu aktivieren. Mit Eingabe der Aktivierung erklären Sie sich damit einverstanden, dass wir die von Ihrem Betriebssystem zu diesem Zweck generierte sogenannte Push-Token-ID auf unseren Servern speichern dürfen. Diese ID wird für die Server-Kommunikation mit Ihrem Betriebssystem-Anbieter verwendet. Der Inhalt der Nachricht ist nicht personenbezogen. Wenn Sie die Benachrichtigungsfunktion in den Systemeinstellungen deaktivieren oder die Log-out Funktion verwenden, wird das Token gelöscht.

1.2.7 Sicherheit

Die WWF setzt technische und organisatorische Sicherheitsmassnahmen ein, damit die Daten, die sie im Rahmen der «UZH Wallet Pilot» App erhebt und weiter bearbeitet,

- vertraulich bleiben und vor zufälligen oder unrechtmässigen Zugriffen, Veränderungen oder Offenlegungen sowie vor Verlusten und Zerstörung geschützt werden,
- ein Zugriff auf die Daten ausschliesslich nach dem Grundsatz der Erforderlichkeit («Need-to-Know») denjenigen Personen erteilt wird, die aufgrund ihrer Funktion und Aufgabe auf die Personendaten zugreifen müssen.

Um die ungewollte Einsicht durch Dritte auf temporär geladene Daten (z.B. Prüfungsergebnisse) auf Ihrem mobilen Gerät zu verhindern, empfehlen wir die Einrichtung einer zeitabhängigen Bildschirmsperre in Kombination mit einer PIN oder einem biometrischem Verfahren.

1.3 Gültigkeit

Die WWF behält sich vor, die Datenschutzerklärung jederzeit zu ändern, sollte die Implementierung neuer Technologien oder die Gesetzeslage eine solche Anpassung erforderlich machen. Änderungen gibt Ihnen die UZH in geeigneter Weise bekannt. Wir empfehlen Ihnen darüber hinaus, regelmässig in die Datenschutzerklärung der «UZH Wallet Pilot» App Einsicht zu nehmen.



1.4 Auskunfts- und Widerrufsrecht

Sollten Sie eine Auskunft zu den über Sie erhobenen und weiter bearbeiteten Personendaten oder eine Berichtigung, Vernichtung oder Sperrung dieser Daten wünschen oder weitergehende Fragen zu deren Verwendung haben, wenden Sie sich bitte schriftlich unter Beilage einer Ausweiskopie an die

Wirtschaftswissenschaftliche Fakultät der Universität Zürich
Dekanat
Rämistrasse 71
CH-8006 Zürich

Die Einwilligung zur Verwendung Ihrer Daten können Sie jederzeit widerrufen, indem Sie die «UZH Wallet Pilot» App löschen.