Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB

Direktionsbereich Kompetenzzentren
Fachbereich Digitale Gesellschaft

CH-3003 Bern, EDÖB, EDÖB-A-E73B3401/2

Per E-Mail an:

[redacted]

Ergänzung des EDÖB vom 07. Mai 2020:
Die vorliegende Einschätzung berücksichtigt die Informationen aus den Unterlagen zum Projekts PTAPP bis am 23. April 2020. Nach diesem Zeitpunkt sind vom Projekt eine epidemiologische Anpassung (Verlängerung der Aufzeichnungsdauer von 14 auf 21 Tage) und eine konzeptionelle Änderung im Schlüsselmanagement (täglich wird der private Schlüssel SK_t neu generiert und kann nicht mehr vom vorhergehenden abgeleitet werden) erfolgt. Diese beiden Anpassungen haben keine Auswirkungen auf das Resultat dieser datenschutzrechtlichen Einschätzung.

Ihr Zeichen:
Unser Zeichen: EDÖB-A-E73B3401/2
Sachbearbeiter/in: Sidler Andreas
Bern, 23.04.2020

Einschätzung Backend PTAPP

Sehr geehrte Damen und Herren

Bezugnehmend auf die Anfrage des BIT zur Einschätzung der technischen Umsetzung des Backend der Proximity Tracing Applikation können wir Ihnen folgendes mitteilen:

Der EDÖB hat die vorliegende Einschätzung basierend auf die ihm zur Verfügung gestellten Konzepte für das Backend[1] und die Besprechungen vorgenommen. Sie erfolgt losgelöst von der vom Beauftragten geforderten generellen rechtlichen Grundlage für den Betrieb der Proximity Tracing Applikation, aus der die Zwecke und Verantwortlichkeiten bürgerverständlich hervorzugehen haben.

Datenschutzrechtliche Einschätzung

Zur datenschutzrechtlichen Einschätzung wurde das Backend in drei funktionale Systemteile unterteilt:

Black 1	System für die Medizinalpersonen zur Auslösung der Autorisierungscodes für den Upload des anonymen Schlüssels der App der infizierten Nutzer (SK_t[2] und onset date[3]).
Red 1	System zur Aufbereitung der Liste mit den Seed SK_t und onset date.
Red 2	Content Delivery Network (CDN) für die Verbreitung der aktuellen Liste mit den SK_t und den onset date.

[1] Projektdokumentationen 002 000 Data management - legal perspective (vom 17.04.2020), 004 002 Network View - Access to Federal Network (vom 21.04.2020).
https://github.com/DP-3T/documents und dort insbesondere https://github.com/DP-3T/documents/blob/master/DP3T%20White%20Paper.pdf und https://github.com/DP-3T/documents/blob/master/DP3T%20-%20Data%20Protection%20and%20Security.pdf:
https://github.com/SecureTagForApproachRecognition/star-sdk-documentation/;
https://confluence.bit.admin.ch/display/PTAPP/Proximity+Tracing+App+Startseite, Zugriff 17.04.2020.
[2] Privater kryptografischer Schlüssel zum Zeitpunkt t.
[3] Startpunkt des Ansteckungszeitraums.

Gemäss den Konzepten zu DP-3T wird bei der Installation der Applikation auf dem Mobiltelefon ein zufälliger SK_l[4] generiert. Ab diesem Zeitpunkt wird täglich mittels Hashfunktion aus dem vorhergehenden SK_{t-1}[5] ein neuer SK_t[6] berechnet. Diese SK erlauben keine Rückschlüsse auf das Telefon, die Applikation oder den Benutzer. Somit handelt es sich beim SK_t um eine anonymen ID (Schlüssel), welcher kein Personendatum gemäss Art. 3 lit. a des Bundesgesetzes über den Datenschutz (DSG; SR 235.1) darstellt. Diese SK_t sind wichtig in Bezug auf die Generierung der $EphID_t$[7], welche zwischen den Mobiletelefonen für das Proximity Tracing ausgetauscht werden. Bei diesen EphID handelt es sich ebenfalls um anonyme IDs und nicht um ein Personendatum gemäss Art. 3 lit. a DSG. Ohne die Kenntnis von SK_t und onset date, können sie weder berechnet noch einem Telefon oder einer Applikation zugewiesen werden. Die letzten 14 der täglich geänderten SK_t bleiben auf dem Telefon bis zum Zeitpunkt des autorisierten Uploads durch den Nutzer. Nach einem Upload des SK_t und onset date im Falle einer festgestellten Infizierung wird auf dem Mobiltelefon wieder ein neuer zufälliger SK_l generiert.

A. Systemteil Black 1 – System für die Medizinfachpersonen zur Auslösung der Autorisierungscodes

A1. Sachverhalt Informationen im Systemteil

Die Medizinalpersonen werden über vertrauenswürdige medizinische Systeme, wie beispielsweise das HIN Netzwerk (Health Info Net AG), identifiziert/autorisiert und können einen Autorisierungscode für den Upload des SK_t erstellen lassen. Dazu werden der Authentisierungscode, der Ablaufzeitpunkt (24h nach der Generierung) und ein onset date (vom Arzt errechneter Startzeitpunkt (Datum) des Ansteckungszeitraums) im Systemteil Black 1 erfasst.

Die erfassten Informationen (Autorisierungscode, onset date und Ablaufzeitpunkt) werden im Systemteil Black 1 nach dem Erreichen des Ablaufzeitpunkts gelöscht. Hat der infizierte Nutzer den Autorisierungscode auf seinem Mobiltelefon eingegeben, wird der SK_t des Infektionszeitpunktes (<= 14 Tage) an den Systemteil Red 1 übertragen und - zusammen mit dem onset date - dort abgespeichert. Eine Speicherung des Autorisierungscodes erfolgt nicht.

A1. Einschätzung

Der Autorisierungscode ist für die beteiligten Medizinalpersonen zusammen mit dem onset date ein Personendatum nach Art. 3 lit a DSG. Nach der Löschung von Autorisierungscode, onset date und Ablaufzeitpunkt sind keine Daten mehr im System Black 1 vorhanden, welche eine Identifizierung eines infizierten Nutzers ermöglichen würden. Diese Datenbearbeitung zum Betrieb des Gesamtsystems für das Proximity Tracing ist geeignet, notwendig und daher sachlich verhältnismässig. Die nicht mehr benötigten Daten werden zum frühestmöglichen Zeitpunkt gelöscht, daher ist die Datenbearbeitung auch in zeitlicher Hinsicht verhältnismässig. *Da jedoch eine Personendatenbearbeitung durch ein Bundesorgan erfolgen soll, ist diese auf der richtigen Normstufe entsprechend zu regeln.*

[4] Initialer privater Schlüssel (Secret Key).
[5] Privater Schlüssel zum Zeitpunkt t minus ein Tag.
[6] Errechneter privater Schlüssel nach der Zeitdauer t.
[7] Es werden 1440 EphID pro Tag auf der Basis vom SK_t generiert und zufällig für die Übertragung ausgewählt.

A2. Sachverhalt Logdaten
Die Zugriffe der Medizinalpersonen über vertrauenswürdige medizinische Systeme, wie das HIN Netzwerk, werden zum Zweck der Datensicherheit geloggt.

A2. Einschätzung
Die Logfiles enthalten Personendaten gemäss Art. 3 lit. a DSG. Diese Datenbearbeitung ist für die Sicherheit des Gesamtsystems geeignet, notwendig und damit verhältnismässig. Es bedarf aber auch hier einer klaren Regelung über den Zweck, die Zugriffsberechtigten und die Aufbewahrungsdauer/Löschung dieser Logdaten auf der richtigen Normstufe.

B. Systemteil Red 1 – System zur Aufbereitung der Liste mit den SK_t und onset date

B1. Sachverhalt Informationen im Systemteil
Wird der Autorisierungscode durch den infizierten Nutzer in der Applikation auf dem Mobiltelefon eingegeben, sendet dieses - End-to-End verschlüsselt - der SK_t, das onset date sowie ein Sicherheitstoken an den Systemteil Red 1. Das Sicherheitstoken wird einzig zur Autorisierung der Übermittlung der Daten verwendet und nicht gespeichert. In der Datenbank des Systemteil Red 1 werden lediglich der SK_t sowie das onset date abgelegt. Diese Datenbankeinträge werden nach Ablauf der für das Virus spezifischen Ansteckungsdauer (zurzeit 14 Tage) aus der Datenbank endgültig gelöscht.

B1. Einschätzung
Die übertragenen und gespeicherten SK_t und das onset date der infizierten Nutzer können weder alleine noch zusammen einer Person, einer App oder einem Telefon zugeordnet werden. Sie sind daher im Systemteil Red 1 nicht als Personendaten zu qualifizieren.

B2. Sachverhalt Logdaten
Zur Verhinderung einer personenbezogenen Auswertung bei der Datenübermittlung via IP Adresse des Mobiltelefons eines infizierten Nutzers (z.B. durch das Filtern der Datenübermittlungen an die Bundesinfrastruktur Ziel IP) wird zusätzlicher Datenverkehr, welcher betreffend Struktur, Inhalt und Grösse einer realen Übertragung entspricht (sogenannter Noise), generiert.

Beim Eintritt des Datenverkehrs in das Bundesnetzwerk werden unter anderem zum Zweck der Sicherung der elektronischen Infrastruktur (vgl. Art. 57l lit. b des Regierungs- und Verwaltungsorganisationsgesetzes (RVOG; SR 172.010)) die Randdaten zu den Kommunikationsvorgängen geloggt.

B2. Einschätzung
Der Noise wird im Systemteil Red 1 herausgefiltert und nur der SK_t und das onset date der infizierten Nutzer werden gespeichert.

Die Logs der Kommunikationsvorgänge auf den Firewalls enthalten, neben den Übermittlungen der SK_t der infizierten Nutzer, auch den gesamten Verkehr des erzeugten Noise. Eine Auswertung dieser Logfiles (z.B. nach IP Adresse und Timestamp) ist einzig zu den, in der RVOG genannten Zwecken, erlaubt. Die Einhaltung der RVOG wird durch die bestehenden technischen- und organisatorischen Massnahmen sichergestellt. Zudem kann eine einfache Identifizierung von Nutzern über die verwendete IP Adresse aus dem Mobilfunknetz oder einem WLAN-Zugang ausgeschlossen werden. Dies, weil hierzu zusätzliche Informationen der Fernmeldedienstanbieter notwendig wären. *Die Datenbearbeitung ist in der RVOG geregelt, jedoch wäre angezeigt, aus Gründen der Transparenz/Vertrauenswürdigkeit der Datenbearbeitung in der auszuarbeitenden Verordnung diesbezüglich auf die RVOG zu verweisen.*

C. Systemteil Red 2 – Content Delivery Network (CDN) für die Verbreitung der aktuellen Liste mit den Seed SK_t und den onset date

C1. Sachverhalt Informationen im Systemteil
Zur Verteilung einer Liste aus den im Systemteil Red 1 verwalteten Datensätzen mit den SK_t und den zugehörigen onset date wird das CDN von Amazon Webservices (AWS) genutzt. Diese Nutzung ist notwendig, da alle aktiven Proximity Tracing Applikationen in einer hohen Frequenz nach Updates dieser Liste nachfragen und so eine riesige Anzahl von Abfragen generieren. Nur ein speziell dafür ausgelegtes Netzwerk kann eine solche Anzahl von Abfragen verarbeiten. Hierzu wird die aktuellste Liste im Cache des CDN gespeichert und verteilt.

C1. Einschätzung
Wie bereits im Text zum Systemteil Red 1 ausgeführt, enthält die im CDN gespeicherte Liste keine Personendaten. *Gemäss dem DSG bedarf es keine Regelung für diese Datenbearbeitung, jedoch wäre es angezeigt, aus Gründen der Transparenz/Vertrauenswürdigkeit die Speicherung dieser anonymen Daten bei einem Drittanbieter in der Verordnung auszuführen.*

C2. Sachverhalt Logdaten
Trotzdem werden auch im CDN (AWS S3) Logs der Zugriffe zum Zweck von geoblocking, code injection check, ddos resistance und throttling erstellt. Diese Logdaten werden in der Region «EU (Frankfurt)» gespeichert. Über den Zugriff auf die Logfiles verfügt das Bundesamt für Informatik. Eine Nutzung dieser Logs von AWS zu eigenen Zwecken ist vertraglich ausgeschlossen. Neben der Wahl der Speicherregion «EU (Frankfurt)» für die Logs, wird im DSGVO konformen Vertrag mit AWS der Gerichtsstand Schweiz und die Rechtswahl Schweiz festgelegt. In der Amazon Cloud gelten zudem die Grundschutzstandards des deutschen Bundesamtes für Sicherheit in der Informationstechnik BSI, sowie der Standards ISO/IEC 27001 und PCI/DSS. Diese Standards enthalten differenzierte Anforderungen an die Aufrechterhaltung der Geschäftstätigkeit respektive der Informationssicherheit während Stör- oder Notfällen und Katastrophen. Die TÜV Trust IT Gruppe überprüft regelmässig deren Einhaltung durch Amazon Web Services (siehe aws.amazon.com/de/compliance).

C2. Einschätzung
Die Datenbearbeitung (Logdaten) im Systemteil Red 2 ist verhältnismässig. *Da die Bearbeitung der Informationen im Log nicht durch die RVOG abgedeckt wird, ist eine spezifische Regelung (Zweck der Datenbearbeitung inkl. Zugriffsberechtigte, Löschfrist vom 7 Tagen) in der auszuarbeitenden Verordnung zur App notwendig.*

Wir hoffen, Ihnen mit dieser Einschätzung zum Backend des Proximity Tracing Applikation gedient zu haben und stehen für Fragen gerne zur Verfügung.

Mit freundlichen Grüssen

Andreas Sidler
Verantwortlicher Fachbereich Digitale Gesellschaft