Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB

Der Beauftragte

CH-3003 Bern, EDÖB, EDÖB-A-3F3C3401/1

An das Bundesamt für Gesundheit

[redacted]

Ihr Zeichen:
Unser Zeichen: EDÖB-A-3F3C3401/1
Sachbearbeiter/in: [redacted]
Bern, 11. Mai 2020

Stellungnahme nach Art. 17a DSG zum Pilotversuch mit dem Swiss Proximity-Tracing-System (SPTS)

Sehr geehrte Damen und Herren

Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte hat die ihm vom BAG in rubrizierter Angelegenheit eingereichten Unterlagen geprüft und nimmt dazu gestützt auf Art. 17a DSG wie folgt Stellung:

Der Beauftragte erachtet den bevorstehenden Versuchsbetrieb des SPTS als datenschutzrechtlich zulässig. Aufsichtsrechtliche Massnahmen und Empfehlungen während des Versuchsbetriebs und nach dem Übergang zum vorgesehenen Vollbetrieb bleiben vorbehalten. Im Einzelnen hat er folgende Bemerkungen:

I. Swiss Proximity-Tracing-System (SPTS)

Unter der Bezeichnung „Decentralized Privacy-Preserving Proximity Tracing" (DP-3T) entwickelte eine internationale Gruppe von Forschern aus verschiedenen Ländern unter massgeblicher Beteiligung der EPF in Lausanne sowie der ETH Zürich ein System, das die Eidgenossenschaft der Schweizer Bevölkerung im Rahmen ihrer Strategie zur Bekämpfung des SARS-CoV-2 Virus als technisches Hilfsmittel zur Verfügung stellen will. Wird die entsprechende Mobile App auf dem eigenen Smartphone eingesetzt, zeichnet sie Annäherungen zu anderen Smartphones mit der Mobile App unter Verwendung von Bluetooth dezentral und anonym auf, wenn sie in einem Abstand von unter zwei Metern stattgefunden haben. Die Mobile App sucht in den auf dem Smartphone gespeicherten Annäherungen nach Kontakten zu bestätigten Infizierten und warnt den Nutzer, falls eine genügend lange Zeitdauer der Exposition gegeben ist.

Feldeggweg 1, 3003 Bern
Tel. 058 463 74 84, Fax 058 465 99 96
www.edoeb.admin.ch

In Zusammenarbeit mit der EPFL und ETHZ soll das Bundesamt für Gesundheit (BAG) im Rahmen des Swiss Proximity-Tracing-Systems (SPTS) eine Mobile App zur Verfügung stellen und das Backend mit Server in die vom Bundesamt für Informatik und Telekommunikation (BIT) betriebene Infrastruktur integrieren. Als für den Betrieb verantwortliches Bundesorgan wird das BAG als Inhaber einer Datensammlung nach Art. 3 Bst. i des Bundesgesetzes über den Datenschutz (DSG, SR 235.1) die entsprechenden Verantwortlichkeiten zu tragen haben.

Der Bundesrat beabsichtigt, die Mobile SPTS-App ab dem 13. Mai 2020 auf der Grundlage einer befristeten Verordnung (nachfolgend SPTS-Verordnung), die Gegenstand dieser Stellungnahme ist, einzuführen und bis zum 30. Juni 2020 zu testen. In der Sommersession im Juni 2020 soll das Parlament die vom Bundesrat in Aussicht gestellte Botschaft zu einer dringlichen Änderung des Epidemiengesetzes (EpG, SR 818.101) beraten können.

II. Projekt und Rolle des Beauftragten

Beim Projekt SPTS handelt es sich um eine komplexe, automatisierte Bearbeitung grosser Mengen von Daten aus Mobiltelefonen und anderen Smart-Device Quellen der Bevölkerung, die mit Meldungen und Code-Generierungen durch schweigepflichtige Medizinalpersonen ergänzt werden. Aufgrund des Bezugs dieser Datenquellen auf Personen und deren Gesundheit werden auch der Personenbezug und die datenschutzrechtliche Sensibilität des Vorhabens als Ganzes offensichtlich. Obgleich die Teilnehmer nicht identifiziert werden dürfen, bleibt das SPTS namentlich mit Re-Identifikationsrisiken verbunden, denen mit technischen Vorkehren zum Schutz der Privatsphäre und informationellen Selbstbestimmung der Betroffenen entgegengetreten werden muss.

In der Sondersession von Anfang Mai 2020 haben National- und Ständerat mit komfortablen Mehrheiten beschlossen, dass die SPTS-Verordnung des Bundesrates in der Juni-Session 2020 durch ein Bundesgesetz abzulösen sei. Aus den Beratungen der Staatspolitischen Kommissionen beider Räte und der Kommission für soziale Sicherheit und Gesundheit des Ständerats, zu denen der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) beigezogen worden ist, ging hervor, dass die vor Erlass des geplanten Bundesgesetzes geplante Einführung des SPTS vom Bundesrat nicht auf notrechtliche oder bestehende Kompetenzen des EpG, sondern auf das DSG zu stützen sei. Mit Durchführung eines Pilotversuchs nach Art. 17a dieses Gesetzes sollen die konzeptuellen und technischen Vorarbeiten für eine kurze Zeit ausgetestet werden in der Erwartung, dass das SPTS per Ende Juni als grundrechts- und praxisverträgliche Applikation in Betrieb genommen werden und bei der entsprechend vorinformierten Bevölkerung auf breite Akzeptanz stossen kann.

Angesichts dieser klaren politischen Vorgaben gilt es für den Beauftragten, den gesetzlichen Vorgaben von Art. 17a DSG i.V.m. Art. 27 DSGV in einer Weise Rechnung zu tragen, die den besonderen zeitlichen Verhältnissen der Pandemiebekämpfung gerecht wird.

Nachdem der EDÖB als unabhängige Aufsichtsbehörde für Datenschutz frühzeitig in das Projekt DP-3T einbezogen wurde und die Öffentlichkeit auf seiner Webseite in mehreren Zwischenberichten über seine Arbeit informiert hatte, gibt er zum Pilotversuch mit dem SPTS in Anwendung von Art. 17a Abs. 1 DSG die vorliegende Stellungnahme zuhanden des Bundesrates ab. Letztere wird als Bestandteil des Bundesratsentscheides zur SPTS-Verordnung zu publizieren und demzufolge auch auf der Webseite des Beauftragten zu veröffentlichen sein.

In Anwendung des datenschutzrechtlichen Grundsatzes von «privacy by design» hat die EPFL den EDÖB am 21. März 2020 kontaktiert, sodass seine «Task Force Corona» das Projekt DP-3T ab dem folgenden Tag gemäss den Art. 27-29 und 31 DSG in allen wesentlichen Phasen aufsichtsrechtlich

und beratend begleiten und durch entsprechende Stellungnahmen zur Datenschutzkonformität beitragen konnte. Diese basierten auf der Dokumentation auf Github[1] sowie den mündlichen Kontakten mit den am Projekt beteiligten Personen der EPFL und der Bundesverwaltung. Am 2. April 2020 äusserten wir uns in einer ersten schriftlichen Grobbeurteilung zu zentralen Anliegen des Datenschutzes wie namentlich der Anonymisierung der personenbezogenen Daten sowie der freiwilligen Verwendung. Mit Schreiben vom 23. April 2020 folgte eine datenschutzrechtliche Einschätzung der technischen Ausgestaltung des Backends, und am 1., 4. und 8. Mai 2020 äusserten wir uns im Rahmen von Ämterkonsultationen zu den rechtlichen Grundlagen des SPTS.

Die Staatspolitischen Kommissionen beider Räte und die Kommission für soziale Sicherheit und Gesundheit des Ständerats haben den Beauftragten am 22. und 30. April sowie 5. und 7. Mai 2020 zum SPTS und weiteren Applikationen zur Pandemiebekämpfung, die seine Task Force Corona aufsichtsrechtlich begleitet, angehört.

III. Beurteilung der Applikation

1. Kriterien

Wie der EDÖB bereits in seiner Mitteilung vom 17.März 2020 festgehalten hat, haben Bundesorgane, die systematisch aus einer grossen Anzahl von personenbezogenen Quellen wie Smartphones Daten beschaffen und automatisiert bearbeiten, die Grundsätze nach Art. 4 des DSG zu beachten.

Von besonderer Bedeutung sind im aktuellen Kontext der Pandemiebekämpfung die Prinzipien der Verhältnismässigkeit und der Zweckbindung, die verlangen, dass die Datenbearbeitung im Rahmen des SPTS zeitlich und umfangmässig auf jenes Mass zu beschränken ist, das für die Leistung eines signifikanten Beitrages zur Bewältigung der aktuellen Krise nötig ist.

Aufgrund der eingangs erwähnten Risiken für die Privatsphäre und informationelle Selbstbestimmung müssten im Rahmen des SPTS zunächst alle automatisierten Bearbeitungen ausgeschlossen werden, deren Funktionsweise ungeeignet ist, die erwartete Minimalwirkung zu erzielen und die sich dadurch als unverhältnismässig erwiesen. Bearbeitungen, die auf überschiessende Zwecke, wie die Verhütung neuer Seuchen abzielen würden, müssten ebenfalls ausscheiden. Für neue Zielsetzungen müssten über das ordentliche Rechtsetzungsverfahren hinreichend bestimmte, sektorenspezifische Rechtsgrundlagen geschaffen werden. Dieser Hinweis auf die Zweckbindung erfolgt nicht zuletzt auch mit Blick darauf, dass im Falle einer erfolgreichen Anwendung des SPTS im Rahmen der aktuellen Pandemiebekämpfung nicht ausgeschlossen werden kann, dass auch Behörden ausserhalb des Gesundheitssektors auf die Idee kommen könnten, «Proximity Tracing» z.B. für sicherheits- oder kriminalpolizeiliche Zwecke einzusetzen.

Die nachfolgende Beurteilung nach Kriterien des DSG erfolgt im Übrigen in Anlehnung an die Richtlinien des Europäischen Datenschutzausschusses[2] und des Europarats[3] zur Pandemiebekämpfung.

2. Transparente und datenschutzfreundliche Ausgestaltung der Applikation

Damit das SPTS für die unmittelbare Bewältigung der aktuellen Krise und schrittweisen Aufhebung der gesundheitspolizeilichen Einschränkungen von Freiheitsrechten einen wirksamen Beitrag leisten

---

[1] https://github.com/DP-3T/documents, zugegriffen am 4. Mai 2020.
[2] https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-042020-use-location-data-and-contact-tracing_de (zugegriffen am 9. Mai 2020).
[3] https://rm.coe.int/covid19-joint-statement-28-april/16809e3fd7 (zugegriffen am 9. Mai 2020).

kann, muss die Mobile App von einem signifikanten Teil der Bevölkerung, die ein mit Bluetooth Technologie ausgerüstetes Smartphone besitzt, installiert und aktiviert werden. Dies setzt voraus, dass der mobilen App eine vertrauenswürdige Datenbearbeitung i.S.v. Art. 4 Abs. 2 DSG zugrunde gelegt wird, indem die Betreiberin die Benutzer umfassend und leicht verständlich über Zweck und Funktionsweise des SPTS informiert und die damit verbundenen Wahlmöglichkeiten benutzerfreundlich ausgestaltet. Weiter wird vorausgesetzt, dass die Betreiberin für jedermann nachvollziehbar aufzeigt, dass das SPTS datenschutzfreundlich ausgestaltet worden ist (privacy by design).

2.1. Funktionsweise

Die Funktionsweise des auf den Grundsätzen des DP-3T beruhenden SPTS lässt sich grob wie folgt beschreiben:

Nutzerinnen und Nutzer (User) laden die Mobile SPTS-App aus dem App Store von Apple oder aus dem Google Play Store und installieren sie auf ihren Smartphones. Bei der Installation wird ein zufälliger initialer privater Schlüssel erzeugt. Weiter werden die Funktionen «Mitteilungen» und «Bluetooth» benötigt, die gegebenfalls eine Bestätigung erfordern.

Die Mobile SPTS-App sendet nun über Bluetooth laufend wechselnde, vom jeweiligen tagesaktuellen privaten Schlüssel abhängige, zufällige Identifikatoren (Ephemeral IDs, EphIDs) und empfängt solche von anderen Mobile SPTS-Apps in unmittelbarer Nähe. Der eigene, täglich wechselnde private Schlüssel, die empfangenen EphIDs sowie Dauer und ungefähre Zeit der Begegnungen werden für 21 Tage auf dem eigenen Gerät gespeichert.

Werden User positiv auf Covid-19 getestet, können sie freiwillig entscheiden, ob sie den von einer Medizinalperson ermittelten Starttag des Ansteckungszeitraums zusammen mit den, ab diesem Zeitpunkt gültigen privaten Schlüssel über eine verschlüsselte Verbindung an den Backend-Server schicken wollen. Dazu benötigen sie den durch eine Medizinalperson mitgeteilten Autorisierungs-Code. Dieser wird vorausgesetzt, damit nur medizinisch bestätigte Infektionsfälle dem SPTS gemeldet werden können. Nach der Meldung an den Backend-Server erzeugt die Mobile App einen neuen initialen privaten Schlüssel. Dieser wird zufällig und tagesaktuell generiert und lässt keine Rückschlüsse auf einen früheren privaten Schlüssel zu.

Die Mobile Apps aller User rufen die auf dem Backend-Server gespeicherte Liste der privaten Schlüssel der bestätigten Infektionen ab und verifizieren auf dem jeweiligen Smartphone mit den erhaltenen privaten Schlüsseln, ob bei den aufgezeichneten Begegnungen EphIDs vorhanden sind. Aus den von Infizierten gesendeten Informationen (privater Schlüssel und Startdatum) kann weder auf dem Backend-Server noch auf den Smartphones die Identität der Infizierten festgestellt werden.

Der datenschutzfreundliche Ansatz des SPTS schlägt sich insbesondere in den folgenden Aspekten der Ausgestaltung nieder:

- es wird nur auf die Nähe zwischen den Usern abgestellt, es werden keine Ortungsdaten gesammelt;
- kein Kennungsaustausch mit Smartphones ohne installierte Mobile App;
- basierend auf den wechselnden EphIDs ist ein Tracking von Personen und Geräten nicht möglich;
- solange keine Meldung durch eine verifizierte, infizierte Person erfolgt, werden keine Daten auf den Server hochgeladen;
- nur Kontaktsituationen von zwei Metern oder weniger werden aufgezeichnet und führen bei einer Dauer von insgesamt mindestens 15 Minuten pro Tag zu einer Benachrichtigung;
- die Dauer der Aufbewahrung der Daten ist begrenzt auf ihren Nutzen zur Erkennung von möglichen Infektionen;

- der Einsatz desSystems ist auf die Dauer der Pandemie begrenzt;
- das System basiert auf einem dezentralen Ansatz (s. sogleich).

Ein Proximity Tracing-System benötigt eine Infrastruktur im Hintergrund. Um dabei nur so viel Daten, wie für die Zwecke des Tracing unbedingt nötig sind, zu bearbeiten (Datenminimierung), stehen heute namentlich zwei Ansätze im Vordergrund: Die zentralisierten und die dezentralisierten Modelle. Die Grundsätze des DP-3T sehen ein dezentralisiertes System vor, bei welchem so viele Daten wie möglich auf den Geräten der User verbleiben sollen. Daten über stattgefundene Begegnungen werden zu keiner Zeit auf einem zentralen Server gesammelt. Ein Server existiert nur, um den Usern zu ermöglichen, mit ihren eigenen Geräten festzustellen, ob es zu relevanten Begegnungen kam. Der Server nimmt keine Informationen auf, die Personen zugeordnet werden können, und vergibt keine Identifikatoren. Dadurch kann eine zentrale Profilbildung ausgeschlossen werden. Auch sind beim dezentralen Ansatz die Risiken von Zweckänderungen und Angriffen auf den Server geringer, weshalb er aus Sicht des EDÖB bei einer Gesamtwürdigung dem zentralen Ansatz vorzuziehen ist.

Im Sinne der Transparenz ist das dem SPTS zugrundeliegende DP-3T offen zugänglich (open-source). Die Dokumentation und der Quell-Code sind auf der GitHub-Projektseite[4] abrufbar.

2.2. Exposure notification solution von Apple und Google

Am 10. April 2020 haben Apple und Google eine «exposure notification solution» auf der Basis von Bluetooth auf Smartphones angekündigt, die Bemühungen beim Contact Tracing unterstützen soll. Die zur Verfügung gestellte Schnittstelle (API) soll die Nutzung vom Bluetooth zur ständigen Messung der Nähe zwischen autorisierten Mobile Apps sicherer, präziser und effizienter machen. Die Verwendung des API soll prinzipiell nur auf eine Mobile App pro Land beschränkt werden. Nach eigenen Angaben werden Apple und Google keine identifizierenden Informationen über User, Ortungsdaten oder Informationen über andere Geräte in der Nähe des Users erhalten. Weiter werde das Projekt nicht kommerzialisiert. Die beiden Unternehmen sind bei diesen Aussagen zu behaften. Ein Update des SPTS bzw. der Mobile App zur Einbindung der von Apple und Google bereitgestellten Schnittstellen für die Kommunikation über Bluetooth soll bei deren Verfügbarkeit erfolgen.

2.3. Datenschutzerklärungen und Nutzungsbedingungen

Die dem Beauftragten vorliegenden Datenschutzerklärungen und Nutzungsbedingungen beziehen sich auf den Pilotversuch. Sie haben vorübergehenden Charakter und erweisen sich, abgesehen von noch zu verbessernden untergeordneten Einzelpunkten, in datenschutzrechtlicher Hinsicht als konform. Punktuelle Anpassungen während des Pilots bleiben vorbehalten.

2.4. Ausstehende Testversion der Mobile App

Da zurzeit noch keine lauffähige und prüfbare SPTS-Mobile-App vorliegt, stützt sich die Beurteilung des EDÖB vorläufig auf das datenschutzkonforme DP-3T Konzept. Sobald prüfbare, visualisierte Versionen der Mobile-App vorliegen, wird der Beauftragte auch die Datenschutz- und Nutzungsbedingungen sowie die Benutzerfreundlichkeit der für den unbeschränkten Betrieb vorgesehenen SPTS-Mobile-App beurteilen können und gegebenenfalls entsprechende Anpassungen verlangen.

[4] https://github.com/DP-3T/ (zugegriffen am 9. Mai 2020) sowie https://github.com/admin-ch.

2.5. Zwischenergebnis

Aufgrund des Gesagten kommt der EDÖB zum Schluss, dass das Backend im aktuellen Entwicklungsstand über eine datenschutzfreundliche Architektur verfügt und den Grundsätzen der vertrauenswürdigen und transparenten Datenbearbeitung i.S.v. Art. 4 DSG entspricht.

3. Risiken und Angemessenheit der dagegen getroffenen Massnahmen

Gemäss ständiger Praxis des EDÖB haben Bundesorgane, die systematisch Daten aus personenbezogenen Quellen beschaffen und bearbeiten, die damit einhergehenden Risiken für die Privatsphäre und die dagegen ergriffenen Massnahmen im Rahmen einer Datenschutz-Folgenabschätzung aufzuzeigen. Letztere hat insbesondere auf die mit der Anonymisierung personenbezogener Daten verbundenen Re-Identifikationsgefahren der vorliegenden App zur Pandemiebekämpfung einzugehen.

Im Rahmen des DP-3T-Projekts wurden dem EDÖB Dokumente vorgelegt, die in wesentlichen Bereichen einer Risikofolgeabschätzung entsprechen. Am 1. Mai 2020 wurde dem EDÖB zudem ein förmlicher «Data Protection Impact Assessment Report» vorgelegt, erstellt durch die EPFL und eine externe Beratungsfirma[5]. Dort werden namentlich folgende Risiken benannt und entsprechende Massnahmen aufgezeigt:

- Widerrechtlicher Datenzugriff
- Identifikation von positiv getesteten Kontakten
- Ausbleiben einer Warnung trotz Kontakt zu Infizierten
- Falschmeldungen
- Offenlegung der App-Nutzung und Tracking von Geräten der User
- Beschaffung von Informationen über User aufgrund lokalem Gerätezugriff
- Beschaffung einer signifikanten Anzahl von EphIDs durch Relay Attack
- Datennutzung zu anderen Zwecken / Zweckänderung / Massenüberwachung
- DP-3T-System funktioniert nicht wie erwartet
- Freiheitsbeschränkungen bei Nichtverwendung der User App

Aufgrund des Gesagten kommt der EDÖB zum Schluss, dass die Applikation die für die Privatsphäre der Benutzer der App bestehenden Gefahren hinreichend aufzeigt und diesen mit angemessenen Massnahmen begegnet. So werden beispielsweise die Übertragungen verschlüsselt und Fake-Posts (Noise) generiert, damit Dritte keine Identifizierungen von infizierten Personen vornehmen können. Für Details wird auf die technische Beurteilung vom 23. April 2020 sowie die oben erwähnte Dokumentation verwiesen.

4. Geeignetheit

Das SPTS ist Teil einer Gesamtstrategie des Bundesrats und des BAG zur Überwindung der gegenwärtigen Pandemie-Krise und schrittweisen Aufhebung der gesundheitspolizeilichen Einschränkungen von Freiheitsrechten[6]. Damit der Einsatz des SPTS angesichts der oben dargelegten Risiken für die

---

[5] https://github.com/DP-3T/documents/blob/master/data_protection/DP-3T%20Model%20DPIA.pdf (zugegriffen am 9. Mai 2020)

[6] https://www.bag.admin.ch/dam/bag/de/dokumente/cc/kom/covid-19-faktenblatt-swiss-pt-app.pdf.download.pdf/BAG_Faktenblatt_Coronavirus_Swiss-PT-App.pdf (zugegriffen am 9. Mai 2020).

Privatsphäre in datenschutzrechtlicher Hinsicht als verhältnismässig beurteilt werden kann, muss dieses grundsätzlich geeignet sein, im Rahmen dieser Gesamtstrategie einen wirksamen Beitrag zu leisten resp. eine signifikante Teilwirkung zu erzielen.

In der öffentlichen Diskussion des SPTS wurde dessen Geeignetheit verschiedentlich in Frage gestellt. So wurde bezweifelt, ob es zu einer signifikanten Anzahl von freiwilligen Installationen kommen wird. Oder es wurde befürchtet, dass das Vorhaben an der fehlenden Bereitschaft, über die App eine Ansteckung zu melden, scheitern könnte. Auch wurde kritisiert, dass in Gebäuden viele irrelevante Annäherungen erfasst würden, die Falschalarme generieren, oder dass der Dauerbetrieb von Bluetooth viel Batterie-Strom verbrauche. Weiter wurde bemängelt, dass die älteste Gruppe der Senioren mit der höchsten Verletzlichkeit mehrheitlich kein Smartphone benützt. Schliesslich wurde angesichts der verschiedenen Ansätze, die vom paneuropäischen Konsortium PEPP-PT[7] zurzeit verfolgt werden, und des Austritts der DP-3T Gruppe aus dem Konsortium die internationale Kompatibilität des SPTS nach den Grundsätzen desDP-3T angezweifelt.

Angesichts dieser Kritik kann in der Tat nicht mit Gewissheit vorausgesagt werden, dass das SPTS die erhoffte Wirkung entfalten wird. Hingegen gehen der Bundesrat, das BAG als zuständiges Fachamt sowie die EPFL von einer hinreichenden Wahrscheinlichkeit aus, dass sich SPTS bewähren wird und so zu einer zusätzlichen Reduktion und Nachvollziehbarkeit der lebensbedrohenden Ansteckungen beitragen kann. Zudem scheinen repräsentative Umfragen, wie jene der Zürcher Hochschule für angewandte Wissenschaften[8], darauf hinzudeuten, dass sich eine Mehrheit der Bevölkerung nicht nur zu einer Installation, sondern auch zur Meldung einer Infektion über die App entschliessen würde.

Angesichts der günstigen Prognosen des fachkundigen BAG sowie der umfangreichen Dokumentation der EPFL und wissenschaftlichen Umfragen muss sich der EDÖB als Aufsichtsbehörde für Datenschutz mit Blick auf die Beurteilung der Geeignetheit des SPTS insoweit Zurückhaltung auferlegen, als er sein Ermessen nicht ohne Weiteres über das pflichtgemässe Ermessen des zuständigen Fachamtes stellen darf und keine Hinweise darauf bestehen, dass das BAG nicht pflichtgemäss ausgeübt hätte. Neben der technischen Tauglichkeit des SPTS bildet auch das Benutzerverhalten eine wichtige Komponente der Geeignetheit. Dieses Verhalten lässt sich durch die vom EDÖB noch zu beurteilende Benutzerfreundlichkeit der Mobile-App und die vom BAG in Aussicht gestellte Kampagne zur Einführung der App zwar beeinflussen, aber dennoch nur bedingt voraussagen. Konkrete Erkenntnisse zur Akzeptanz werden sich erstmals durch die Evaluationen des Pilotbetriebs gewinnen lassen.

Aufgrund des Gesagten beurteilt der Beauftragte das SPTS nach dem heutigen Wissensstand als geeignet, einen Teilbeitrag zur Verhinderung lebensbedrohender Ansteckungen zu leisten. Demzufolge erweist es sich als verhältnismässig. Mit Blick auf die erwähnten Zweifel und den Umstand, dass aus Zeitgründen auf einen erläuternden Bericht zur SPTS-Verordnung verzichtet werden musste, erwartet der EDÖB, dass das BAG in der geplanten Botschaft zur Anpassung des Epidemiengesetzes die Geeignetheit begründet und dabei insbesondere auch auf die geäusserte Kritik eingeht. Sollte sich im Rahmen des Pilot- oder Vollbetriebs abzeichnen, dass die Applikation die in sie gesetzten Erwartungen nicht erfüllen kann, behält sich der EDÖB vor, dem BAG zu empfehlen, auf die Aufnahme des Vollbetriebs oder dessen Fortführung zu verzichten.

[7] https://www.pepp-pt.org/ (zugegriffen am 9. Mai 2020).
[8] https://www.zhaw.ch/de/ueber-uns/aktuell/news/detailansicht-news/event-news/viele-schweizer-fuerchten-ueberwachung-durch-contact-tracing-app/, zugegriffen am 04. Mai 2020.

5. Gesetzliche Grundlage

Bundesorgane, die systematisch aus einer grossen Anzahl von personenbezogenen Quellen wie Mobil-Telefonen Daten beschaffen und automatisiert bearbeiten, müssen angesichts der damit verbundenen Risiken für die Privatsphäre und informationelle Selbstbestimmung über eine gesetzliche Grundlage i.S.v. Art. 17 Abs. 1 DSG verfügen. Dieses Erfordernis gilt auch, wenn die Verwendung der Applikation auf Freiwilligkeit beruht.

Die vom Bundesrat zur Einführung des SPTS vorgelegte befristete Verordnung, die Gegenstand dieser Stellungnahme des EDÖB ist, stützt sich im Ingress auf Art. 17a DSG. Sie stellt damit eine hinreichende Gesetzesgrundlage für die Durchführung des Versuchsbetriebs des SPTS dar. In der Sommersession im Juni 2020 soll das Parlament die geplante Botschaft zu einer dringlichen Änderung des Epidemiengesetzes (EpG, SR 818.101) beraten können. In inhaltlicher Hinsicht hat der EDÖB zur SPTS-Verordnung Stellung genommen. Seine Anliegen wurden in der Ämterkonsultation berücksichtigt.

Das BAG verfügt somit für die Dauer des bis am 30. Juni 2020 befristeten Versuchsbetriebs des SPTS über eine genügende gesetzliche Grundlage. Die SPTS-Verordnung und der darauf gestützte Versuchsbetrieb erweisen sich als datenschutzkonform.

6. Zulässigkeit des Versuchsbetriebs SPTS

Im Hinblick auf unsere Stellungnahme gemäss Art. 17a Abs. 1 DSG i.V.m. Art. 27 Abs. 2 VDSG hat das BAG mit E-Mail vom 7. Mai 2020 sowie im Rahmen der Ämterkonsultation zur SPTS-Verordnung folgende Dokumente eingereicht:

A. *Allgemeine Beschreibung des Pilotversuches:* Es finden sich Hinweise auf Ziel, Zweck und Planung im Antrag an den Bundesrat. Diese Ausführungen sind noch an die Projektmanagementmethode Hermes anzupassen.

B. *Bericht, der nachweist, dass die Erfüllung der gesetzlich vorgesehenen Aufgaben die Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen erfordert und dass eine Testphase vor dem Inkrafttreten des Gesetzes im formellen Sinn zwingend erforderlich ist (Art. 17a Abs. 1 Bst. c DSG):* Die im Rahmen der Ämterkonsultation zur SPTS-Verordnung gemachten Erläuterungen äussern sich zur Erforderlichkeit der Datenbearbeitung mittels SPTS und einer Testphase.

C. *Beschreibung der internen Organisation sowie der Datenbearbeitungs- und Kontrollverfahren (Art. 21 VDSG):* Das Bearbeitungsreglement fehlt. Dieses muss spätestens zwei Wochen vor Initialisierung des Vollbetriebs eingereicht werden.

D. *Beschreibung der Sicherheits- und Datenschutzmassnahmen:* Die Risikofolgeabschätzung und weitere Dokumente betreffend das dem SPTS zugrunde Konzept DP-3T liegen dem EDÖB vor. Hingegen hat das BAG dem EDÖB mit E-Mail vom 7. Mai 2020 für das Gesamtsystem erst vier Dokumente zur Risikoanalyse übermittelt[9]. Folgende Informationen / Dokumente fehlen noch und sind nachzureichen:

[9] Security Testplan Proximity Scanning, 14. April 2020, NCSC; Privacy Issue to be discussed v100, CSIRT-BIT/GovCERT-CH; Risikoeinschätzung Proximity Tracing, 30. April 2020, CSIRT-BIT/GovCERT-CH; Checksums providing privacy in case a user mistypes its authentication code, 5. Mai 2020, NCSC.

- Aktueller Stand Risikoeinschätzung NCSC und Umsetzungsmassnahmen
- Finale Fassung der Datenflüsse für Pilot
- Finale Systemdokumentation (inkl. Anbindung externe Systeme) für Pilot
- Schutzbedarfsanalyse (Schuban)
- Nachweis Bewertung Risikoanalyse
- Visualisierung App

E. *Entwurf oder das Konzept einer Verordnung, welche die Einzelheiten der Bearbeitung regelt:* Im Rahmen der Ämterkonsultation vom 8. Mail 2020 wurde der Entwurf für die SPTS-Verordnung inkl. begründetem Antrag an den Bundesrat vorgelegt.

F. *Informationen betreffend die Planung der verschiedenen Phasen des Pilotversuches:* Eine Projektmanagement-Planung fehlt. Auf eine solche kann angesichts der Kürze des dringlichen Pilotversuchs verzichtet werden.

Angesichts der Dringlichkeit der Pandemie ist die Unvollständigkeit der dem EDÖB vorgelegten Unterlagen nachvollziehbar. Die Einführung des SPTS als ergänzende Massnahme der Pandemiebekämpfung soll deshalb nicht verzögert werden. Der Beauftragte erwartet jedoch, dass die fehlenden Unterlagen rechtzeitig vor Beginn des Vollbetriebs nachgereicht werden.

Die erste Voraussetzung für einen Pilotversuch nach Art. 17a Abs. 1 Bst. a. DSG ist, dass die Aufgaben, die die automatisierte Bearbeitung erforderlich machen, in einem Gesetz im formellen Sinn geregelt sind. Zutreffend bejaht das Eidg. Departement des Innern (EDI) im Antrag an den Bundesrat zur erwähnten SPTS-Verordnung diese Voraussetzung unter Verweis auf Art. 31 Abs. 2 und Art. 33 EpG, die namentlich vorsehen, dass die zuständigen Bundesbehörden und mithin das BAG die kantonalen Behörden bei der Benachrichtigung von ansteckungsverdächtigen Personen unterstützen.

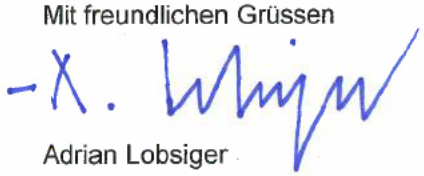
Als zweite Voraussetzung müssen nach Art. 17a Abs. 1 Bst. b. ausreichende Massnahmen zur Verhinderung von Persönlichkeitsverletzungen getroffen werden. Auch wenn der Beauftragte noch nicht sämtliche relevanten Aspekte des SPTS prüfen konnte, namentlich liegt ihm noch keine Testversion der Mobile App inkl. Visualisierungen vor, erachtet er die Umsetzung der SPTS gestützt auf die bisherigen Erkenntnisse und die Umschreibung des geplanten Versuchsbetriebs als ausreichend.

Zu den Voraussetzungen für einen Pilotversuch nach Art. 17a Abs. 1 Bst. c. DSG gehört schliesslich, dass die praktische Umsetzung einer automatisierten Datenbearbeitung eine Testphase vor dem Inkrafttreten des Gesetzes im formellen Sinn zwingend erfordert. Dies kann insbesondere dann der Fall sein, wenn bei erforderlichen technischen Neuerungen sowie organisatorischen oder technischen Massnahmen die Auswirkungen bzw. die Wirksamkeit zunächst evaluiert werden müssen (Art. 17a Abs. 2 Bst. a. und b. DSG). Im Antrag an den Bundesrat zur erwähnten Verordnung bejaht das Eidg. Departement des Innern (EDI) die genannten Voraussetzungen unter Verweis auf neue Lösungsansätze, die vor der definitiven Einführung einen Testbetrieb unabdingbar machen. Angesichts der Risiken und der Komplexität des SPTS teilt der EDÖB diese Auffassung. Wie das EDI indes feststellt, fällt der geplante Pilotversuch kurz aus. Es führt zutreffend aus, dass dennoch wesentliche Erkenntnisse für die definitive Einführung gewonnen werden können. Diese betreffen namentlich den Betrieb inkl. technische Infrastruktur, die Wirksamkeit von technischen Sicherheitsmassnahmen und die Anwendung der Applikation durch Teilnehmende und zugriffsberechtigte Fachpersonen. Zudem entspricht die Durchführung eines kurzen Pilotversuchs nach Art. 17a DSG bis zum Inkrafttreten der beabsichtigten Regelung im EpG dem ausdrücklichen Willen der zuständigen parlamentarischen Kommissionen (vgl. oben Ziff. II.). Die Durchführung eines Pilotversuchs erweist sich somit als zwingend erforderlich.

7. Fazit

Der Beauftragte erachtet den bevorstehenden Versuchsbetrieb des SPTS durch das BAG als datenschutzrechtlich zulässig. Die noch fehlenden Dokumente sind dem EDÖB rechtzeitig vor Einleitung des geplanten Vollbetriebs nachzureichen. Aufsichtsrechtliche Massnahmen und Empfehlungen während des Versuchsbetriebs und nach dem Übergang zum vorgesehenen Vollbetrieb bleiben vorbehalten.

Mit freundlichen Grüssen



Adrian Lobsiger