



Datenschutzerklärung des Bundesamtes für Gesundheit BAG im Zusammenhang mit der Nutzung der «SwissCovid-App»

Version: 24. Juni 2020

In dieser Datenschutzerklärung erläutert das Bundesamt für Gesundheit (BAG), inwieweit es hinsichtlich der Nutzung der Applikation «SwissCovid-App» (nachfolgend App) in der Schweiz Personendaten bearbeitet. Das ist keine abschliessende Beschreibung; allenfalls regeln andere Datenschutzerklärungen, ähnliche Dokumente, Nutzungsbedingungen oder Anwendungsprogramme spezifische Sachverhalte.

Das Datenschutzrecht regelt die Bearbeitung von Personendaten. Die Bundesgesetzgebung über den Datenschutz ist auf die Datenbearbeitung anwendbar. Die Datenschutzerklärung steht zudem im Einklang mit dem Epidemiegesezt vom 28. September 2012 (EpG; SR 818.101) und der Verordnung vom 24. Juni 2020 über das Proximity-Tracing-System für das Coronavirus SARS-CoV-2 (VPTS; SR 818.101.25).

Unter Personendaten werden alle Angaben verstanden, die sich auf eine bestimmte oder bestimmbare Person beziehen. Bearbeiten meint jeden Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten der Daten.

1 Verantwortlicher

Verantwortlich für die Datenbearbeitungen, die hier beschrieben wird, ist das

Bundesamt für Gesundheit BAG
3003 Bern
Schweiz
Tel. +41 58 462 69 98
recht(at)bag.admin.ch

2 Erhebung und Bearbeitung von Personendaten

Das gesamte App-System ist darauf ausgerichtet, dass der Benutzer und die Benutzerin der App nicht bestimmbar sind. Die Bearbeitung von Personendaten wird minimiert. So sind keinerlei technische Rückschlüsse auf Personen, Standorte oder Geräte möglich. Ortsangaben werden keine erfasst, sondern lediglich verschlüsselte Daten betreffend die Kontakt-Ereignisse. Diese werden technisch vor Missbrauch geschützt. Das BAG kann keine Rückschlüsse auf die Benutzerinnen und Benutzer der App ziehen. Die App schützt die Daten der Benutzerinnen und Benutzer so, dass über weite Strecken kein Personenbezug hergestellt werden kann. Dennoch ist ein Personenbezug nicht absolut auszuschliessen. So besteht eine gewisse Wahrscheinlichkeit, dass bei der Benachrichtigung einer möglicherweise gefährdeten Person, diese aufgrund ihrer Erinnerung an ihre Sozialkontakte der letzten Tage allenfalls Rückschlüsse auf die Identität der infizierten Person ziehen kann. Diese Benachrichtigung umfasst die Information, dass die Benutzerin oder der Benutzer potenziell dem Coronavirus ausgesetzt war, die Angabe, an welchem Tag dies zum letzten Mal der Fall war, den

Hinweis, dass das BAG eine Infoline zur kostenlosen Beratung betreibt und die Verhaltensempfehlungen des BAG. Durch die Benutzung der App können somit potenziell auch Personen identifiziert werden.

Das App-System gliedert sich in zwei Komponenten:

- ein System zur Verwaltung der Annäherungsdaten, bestehend aus einer Software, die von den Benutzerinnen und Benutzern auf ihren Mobiltelefonen installiert wird, und einem Backend (VA-Backend);
- ein System zur Verwaltung von Codes zur Freischaltung der Benachrichtigungen (Codeverwaltungssystem), bestehend aus einem webbasierten Frontend und einem Backend.

Die beiden Backends unterstehen als zentrale Server direkt der Kontrolle des BAG und werden technisch vom Bundesamt für Informatik und Kommunikation (BIT) betrieben. Die Codeverwaltungs-Frontends laufen auf Geräten der für die Generierung des Freischaltcodes («Covidcodes») berechtigten Fachpersonen.

Auf dem Mobiltelefon werden folgende Daten gespeichert:

- die empfangenen Identifizierungscores («zufällige ID resp. Zufalls-ID») der anderen Mobiltelefone mit aktiver App
- die Signalstärke
- das Datum und die geschätzte Dauer der Annäherung

Im Falle einer nachgewiesenen Infektion eines Benutzers oder einer Benutzerin werden im Codeverwaltungssystem folgende Daten erfasst:

- der Freischaltcode («Covidcode»)
- das Datum, an dem die ersten Symptome aufgetreten sind, oder, falls die infizierte Benutzerin oder der infizierte Benutzer keine Symptome zeigt, das Testdatum
- der Zeitpunkt der Vernichtung dieser Daten

Das VA-Backend besteht aus einer Liste mit folgenden Daten:

- die privaten Schlüssel der infizierten Benutzerinnen und Benutzer, die in dem Zeitraum aktuell waren, in dem andere Benutzerinnen und Benutzer potenziell dem Coronavirus ausgesetzt waren
- das Datum jedes Schlüssels

3 Zwecke und Rechtsgrundlagen

Das vom BAG betriebene App-System stützt sich auf das EpG und die VPTS. Die App und die mit ihr einhergehenden Datenbearbeitungen bezwecken ausschliesslich die Benutzerinnen und Benutzer, die potenziell dem Coronavirus ausgesetzt waren, unter Wahrung des Datenschutzes zu benachrichtigen sowie Statistiken aus Daten der beiden Backends im Zusammenhang mit dem Coronavirus zu erstellen.

4 Datenweitergabe

Die Liste mit den Daten des VA-Backends wird der App (bzw. Frontend) im Abrufverfahren zur Verfügung gestellt. Soweit das BAG für diesen Service Dritte im In- oder Ausland beauftragt, verpflichten sich diese vertraglich, die Vorgaben nach Artikel 60a EpG und der VPTS einzuhalten. Davon ausgenommen ist die Regelung betreffend den Quellcode nach Artikel 60a Absatz 5 Buchstabe e EpG. Das BAG kontrolliert die Einhaltung der Vorgaben. Bei der Ausführung des Auftrags anfallende Randdaten dürfen die beauftragten Dritten nicht für eigene Zwecke nutzen. Diese Daten werden nur vom BAG bzw. vom BIT ausgewertet (vgl. Ziffer 8).

Das BAG stellt dem Bundesamt für Statistik (BFS) periodisch den aktuellen Bestand der in beiden Backends vorhandenen Daten in anonymisierter Form für statistische Auswertungen zur Verfügung. Das BIT führt im Auftrag des BAG den Betrieb der gesamten Software durch und stellt den notwendigen technischen Support-Service bereit. Das BIT hat lediglich Zugriff auf Daten, soweit dies für die beschriebenen Zwecke und die Tätigkeit der betreffenden Mitarbeiter erforderlich ist. Diese sind im Umgang mit den Daten zu Vertraulichkeit verpflichtet.

Die App verwendet eine Schnittstelle zum Betriebssystem des Mobiltelefons der Benutzerin oder des Benutzers, welche die Bearbeitung von Daten durch Apple oder Google bedingt. Die über die Schnittstelle genutzten Funktionen der Betriebssysteme müssen die Vorgaben von Artikel 60a EpG und der VPTS erfüllen. Davon ausgenommen ist die Regelung betreffend den Quellcode nach Artikel 60a Absatz 5 Buchstabe e EpG. Das BAG vergewissert sich, dass diese Vorgabe eingehalten werden, insbesondere indem es entsprechende Zusicherungen einholt.

5 Dauer der Aufbewahrung

Die Daten werden vernichtet, sobald sie für die Benachrichtigung der Benutzerinnen und Benutzer nicht mehr erforderlich sind. Namentlich werden sie wie folgt vernichtet:

- die Daten des Systems zur Verwaltung der Annäherungsdaten (sowohl auf den Mobiltelefonen als auch im VA-Backend): 14 Tage nach ihrer Erfassung
- die Daten des Codeverwaltungssystems: 24 Stunden nach ihrer Erfassung

6 Datensicherheit

In enger Zusammenarbeit mit seinen internen und externen Hosting-Providern und anderen IT-Dienstleistern trifft das BAG zum Schutz der Daten vor unberechtigtem Zugriff, Verlust und Missbrauch angemessene Sicherheitsvorkehrungen technischer Natur (z.B. Verschlüsselungen, Pseudonymisierung, Protokollierung, Zugangskontrollen und -beschränkungen, Datensicherung, IT- und Netzwerksicherheitslösungen etc.) sowie organisatorischer Natur (z.B. Weisungen an die Mitarbeiter, Vertraulichkeitsvereinbarungen, Überprüfungen etc.) gemäss den Vorgaben der Bundesverwaltung und der schweizerischen Datenschutzgesetzgebung.

7 Rechte der betroffenen Person

Sie haben das Recht auf Auskunft, Berichtigung, Löschung, oder Herausgabe Ihrer Daten. Weiter steht Ihnen das Recht auf Einschränkung der Datenbearbeitung und das Recht auf Widerspruch gegen die Datenbearbeitung zu. Sie haben zudem das Recht, Einwilligungen zu widerrufen, ohne dass dadurch die Rechtmässigkeit der bis zum Widerruf erfolgten Datenbearbeitung berührt ist. Diese Rechte greifen, soweit Personendaten vorhanden sind. Das dem App-System zugrundeliegende «privacy by design», welches mit innovativen kryptografischen Methoden und einer dezentralisierten Datenbearbeitung darauf ausgerichtet ist, dass möglichst keine Angaben zu bestimmten oder bestimmbar Personen (Personendaten) vorhanden sind, verhindert dies jedoch weitestmöglich. Aus diesem Grund ist es dem BAG beispielsweise nicht möglich, Auskunft über die zu einer bestimmten Person erfassten Annäherungsereignisse zu erteilen oder diese Daten zu korrigieren. Das BAG kann diese Daten nicht einsehen, da sie lediglich auf den Mobiltelefonen gespeichert werden.

Die Ausübung der Rechte setzt voraus, dass Sie Ihre Identität eindeutig nachweisen (z.B. durch eine Ausweiskopie). Zur Geltendmachung Ihrer Rechte können Sie das BAG unter der in Ziffer 1 angegebenen Adresse kontaktieren.

Im Falle datenschutzrechtlicher Verstösse können Sie sich an die zuständige

Datenschutzaufsichtsbehörde wenden oder die Rechtswege nach Datenschutzgesetzgebung beschreiten.

8 Weiteres

Es werden Protokolle über Zugriffe auf das VA-Backend und das Codeverwaltungssystem zu den in den Artikeln 57i–57o des Regierungs- und Verwaltungsorganisationsgesetzes vom 21. März 1997 (RVOG; SR 172.010) aufgeführten Zwecken gespeichert. Die Zugriffe können statistisch ausgewertet werden. Es sind die Artikel 57i–57q RVOG und die Verordnung vom 22. Februar 2012 über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen (SR 172.010.442), anwendbar.

Die Protokolldaten werden folgendermassen vernichtet:

- Protokolldaten von den vom BAG beauftragten Dritten: 7 Tage nach ihrer Erfassung.
- Im Übrigen richtet sich die Vernichtung der Protokolldaten nach Artikel 4 Absatz 1 Buchstabe b der Verordnung vom 22. Februar 2012 über die Bearbeitung von Personendaten, die bei der Nutzung der elektronischen Infrastruktur des Bundes anfallen (SR 172.010.442).

9 Änderungen

Das BAG kann diese Datenschutzerklärung jederzeit ohne Vorankündigung anpassen. Es gilt die jeweils aktuelle publizierte Fassung bzw. die für den jeweiligen Zeitraum gültige Fassung. Diese Datenschutzerklärung wurde in mehreren Sprachen verfasst. Bei Divergenzen ist die deutsche Version massgebend. Im Falle einer Aktualisierung wird der Benutzer oder die Benutzerin der App über die Änderung in geeigneter Weise informiert.

* * * * *