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

Version: 1. Juli 2021

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 Bearbeitung von Personendaten anwendbar. Die Datenschutzerklärung steht zudem im Einklang mit dem Epidemiengesetz vom 28. September 2012 (EpG; SR 818.101), der Verordnung vom 24. Juni 2020 über das Proximity-Tracing-System für das Coronavirus SARS-CoV-2 (VPTS; SR 818.101.25), dem Bundesgesetz über die gesetzlichen Grundlagen für Verordnungen des Bundesrates zur Bewältigung der Covid-19-Epidemie vom 25. September 2020 (Covid-19-Gesetz; SR 818.102) sowie der Verordnung vom 30. Juni 2021 über ein System zur Benachrichtigung über eine mögliche Ansteckung mit dem Coronavirus Sars-CoV-2 an Veranstaltungen (VBV; SR 818.102.4).

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 werden, 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 bei den Begegnungen via Proximity-Tracing keine erfasst, sondern lediglich verschlüsselte Daten betreffend die Kontakt-Ereignisse. Beim Warnsystem werden nur verschlüsselte Daten über Veranstaltungen und über Ansteckungsgefahren an diesen Veranstaltungen erfasst. Diese Daten werden technisch vor Missbrauch geschützt. Das BAG kann keine Rückschlüsse auf die Benutzerinnen und Benutzer der App ziehen und die Daten nicht entschlüsseln. 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 insb. beim Proximity-Tracing-System 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. Durch die Benutzung der App können somit potenziell auch Personen identifiziert werden. Die Benachrichtigung aufgrund eines engen Kontaktes mit einer positiv getesteten Nutzerin / einem positiv getesteten Nutzer umfasst weiter Verhaltensempfehlungen des BAG, die Information, dass die Benutzerin oder der Benutzer potenziell dem Coronavirus ausgesetzt war, die Angabe, an welchen Tagen dies der Fall war sowie den Hinweis, dass das BAG einen Leitfaden (Web-Formular) und eine Infoline zur kostenlosen Beratung betreibt. Verlässt die Benutzerin oder der Benutzer die App, um den Leitfaden auszufüllen, werden die in der App genannten Tage, an welchen die Möglichkeit einer Ansteckung bestand, automatisch an den Leitfaden übermittelt. Die Benachrichtigung aufgrund der Check-in Funktion umfasst die obengenannten Punkte, jedoch wird hier kein Leitfaden oder eine Infoline angeboten; der primäre Inhalt der Benachrichtigung ist es, sich testen zu lassen.

Das App-System gliedert sich in drei 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.
- ein System zur Verwaltung der Veranstaltungen, bestehend aus einer Software, die von den Benutzerinnen und Benutzern auf ihren Mobiltelefonen installiert wird, und einem Backend (Veranstaltungs-Backend).

Die drei 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 Identifizierungscodes (sog «random ID») der anderen Mobiltelefone mit aktiver App;
- die Signalstärke;
- das Datum und die geschätzte Dauer der Annäherung;
- die Veranstaltungs-Identifizierungscodes mit dem jeweiligen Datum, Dauer des Aufenthaltes und Bezeichnung der Veranstaltung.

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.

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

- die Veranstaltungs-Identifizierungscodes der infizierten Teilnehmenden, die in dem Zeitraum aktuell waren, in dem eine Ansteckung von anderen Personen an einer Veranstaltung möglich war;
- dem Datum jedes Veranstaltungs-Identifizierungscodes;
- dem verschlüsselten relevanten Zeitraum des infizierten Teilnehmenden pro Veranstaltungs-Identifizierungscode.

Darüber hinaus kann das Proximity-Tracing-System mit entsprechenden ausländischen Systemen verbunden werden, wenn im betreffenden Staat ein angemessener Schutz der Persönlichkeit gewährleistet wird (durch die Gesetzgebung oder hinreichende Garantien, insbesondere durch Vertrag). Ausländische Systeme gelten dann als «entsprechend», wenn sie nach den folgenden Grundsätzen des App-Systems ausgestaltet sind:

- Bei der Datenbearbeitung sind alle angemessenen technischen und organisatorischen Massnahmen zu treffen, um zu verhindern, dass die teilnehmenden Personen bestimmbar sind;
- Die Daten werden so weit wie möglich auf dezentralen Komponenten, die von den teilnehmenden Personen auf ihren Mobiltelefonen installiert werden, bearbeitet. Insbesondere dürfen Daten, die auf dem Mobiltelefon einer teilnehmenden Person über andere Personen erfasst werden, ausschliesslich auf diesem Mobiltelefon bearbeitet und gespeichert werden;
- Es werden nur Daten beschafft oder in anderer Art und Weise bearbeitet, die zur Bestimmung der Distanz und der Zeit der Annäherungen und zur Ausgabe der Benachrichtigungen erforderlich sind, nicht aber Standortdaten;
- Die Daten werden vernichtet, sobald sie für die Benachrichtigung nicht mehr erforderlich sind.

Zum gegenwärtigen Zeitpunkt besteht eine Verbindung mit der in Deutschland verwendeten Corona-Warn-App. Bei der Verbindung werden das VA-Backend und das ausländische System an ein Verbindungssystem angeschlossen, das die gegenseitige Übermittlung der privaten Schlüssel von infizierten Benutzerinnen und Benutzern ermöglicht. Das App-System übermittelt sodann die privaten Schlüssel der App an das Verbindungssystem und speichert die privaten Schlüssel der verbundenen ausländischen Apps auf dem VA-Backend ab.

3 Zwecke und Rechtsgrundlagen

Das vom BAG betriebene App-System und das Verbindungssystem stützt sich auf das EpG, die VPTS, das Covid-19-Gesetz sowie die VWV. 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 drei Backends im Zusammenhang mit dem Coronavirus zu erstellen.

Das Verbindungssystem dient dazu, dass eine solche Benachrichtigung auch zwischen verbundenen nationalen Apps möglich ist. Damit können Benutzerinnen und Benutzer der App auch dann benachrichtigt werden, wenn sie eine Annäherung zu infizierten Benutzerinnen und Benutzern einer ausländischen App gehabt haben (z.B. zu Grenzgängern und Touristen im Inland oder Kontakten im Ausland). Umgekehrt können auch Benutzerinnen und Benutzer einer verbundenen ausländischen App benachrichtigt werden bei Annäherungen zu infizierten Benutzerinnen und Benutzern der App.

4 Datenweitergabe

Die Liste mit den Daten des VA-Backends sowie des Veranstaltungs-Backends wird der App 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, der VPTS, Artikel 3 Absatz 7 Buchstabe a Covid-19-Gesetz und der VWV einzuhalten. Davon ausgenommen ist die Regelung be-

treffend den Quellcode nach Artikel 60*a* Absatz 5 Buchstabe e EpG und Artikel 15 VWV. 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).

Die Liste mit den privaten Schlüsseln der infizierten Benutzerinnen und Benutzer des VA-Backends wird zudem regelmässig für eine grenzüberschreitende Benachrichtigung an das Verbindungssystem übermittelt. Sodann laden die verbundenen ausländischen Systeme (zurzeit: die deutsche Corona-Warn-App) diese privaten Schlüssel herunter und stellen sie ihren Apps zum Abruf zur Verfügung (siehe Ziffer 2).

Das BAG stellt dem Bundesamt für Statistik (BFS) periodisch den aktuellen Bestand der in den drei Backends vorhandenen Daten in anonymisierter Form für statistische Auswertungen zur Verfügung. Die Daten des Verbindungssystems können dem BFS und der zuständigen ausländischen Stelle zu Statistikzwecken in vollständig anonymisierter Form bekanntgegeben werden. 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 für das Proximity-Tracing-System 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 60*a* 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 Systems zur Verwaltung der Veranstaltungen (sowohl auf den Mobiltelefonen als auch im Veranstaltungs-Backend): 14 Tage nach ihrer Erfassung;
- die Daten des Codeverwaltungssystems: 24 Stunden nach ihrer Erfassung;
- die Daten des Verbindungssystems: spätestens 14 Tage nach ihrer Übermittlung an das Verbindungssystem.

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 bestimmbaren 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 Annährungsereignisse 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, das Veranstaltungs-Backend und das Codeverwaltungssystem zu den in den Artikeln 57*l*–57*o* 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 57*i*–57*q* 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.

* * * * *