



Parlamentarischer Vorstoss

Antwort des Regierungsrates

Vorstoss-Nr.: 093-2021
Vorstossart: Interpellation
Richtlinienmotion: ☐
Geschäftsnummer: 2021.RRGR.162

Eingereicht am: 05.06.2021

Fraktionsvorstoss: Nein
Kommissionsvorstoss: Nein
Eingereicht von: Fuhrer-Wyss (Burgistein, SP) (Sprecher/in)
Binggeli (Biel/Bienne, SP)

Weitere Unterschriften: 0

Dringlichkeit verlangt: Ja
Dringlichkeit gewährt: Ja 10.06.2021

RRB-Nr.: 912/2021 vom 18. August 2021
Direktion: Gesundheits-, Sozial- und Integrationsdirektion
Klassifizierung: Nicht klassifiziert

Datenschutz bei der Datenspeicherung der Gastro-Besuchenden garantieren

Die Corona-Pandemie hat uns mit vielen neuen Herausforderungen konfrontiert. Viele Massnahmen, die wir uns vor mehreren Monaten noch nicht vorstellen konnten, waren nötig und zielführend. Bei den nun schon lange ersehnten Öffnungsschritten sind weitere Massnahmen ergriffen worden. Eines ist klar, in der Corona-Pandemie ist die klare Nachverfolgung von Kontakten aus gesundheitlichen Gründen wichtig und richtig. Was der Kanton Bern bei der Öffnung der Gastrobetriebe mit der zentralen Datenspeicherung plant, ist aus Datenschutzgründen jedoch höchst fragwürdig. Gemäss öffentlich verfügbaren Informationen wäre die Datenbank «Swiss Contact Tracing Database», die im Moment bei vielen Restaurationsbetrieben im Einsatz ist, ein veritabler Datenschutzalbtraum: Besuchsdaten aus den führenden Schweizer Check-in-Apps flössen darin zusammen und liessen sich verschiedentlich analysieren: Eine Check-in-Historie der Besuchenden wäre möglich. Der Datenschutz muss gewährleistet sein.

Der Regierungsrat wird um Beantwortung folgender Fragen gebeten:

1. Wie wird der Datenschutz gewährleistet?
2. Warum existiert keine technische Sicherheitshürde für personenbezogene Abfragen?
3. Wie sind die technischen Hürden zur Anonymisierung der Daten?
4. Der Branchenverband Gastro Suisse führt 16 verschiedene Apps auf seiner Website auf. Sie wurden allesamt weder öffentlichen Sicherheitstests unterzogen noch unabhängig auf Datenschutzrisiken überprüft, geschweige denn wurde der Quellcode publiziert. Warum macht der Kanton Bern hier keine Vorgaben?
5. Wie wird sichergestellt, dass die Daten sowohl auf der zentralen Datenbank als auch bei den Gastrobetrieben vernichtet werden?

6. Wie wird sichergestellt, dass keine anderen Direktionen und Behörden die Contact-Tracing-Daten für andere Zwecke nutzen?
7. Wie wird die Sicherheit der zentralen Datenbank gewährleistet? Was für Audits werden durchgeführt?
8. Was für Alternativen zur zentralisierten Sammlung aller Kontaktdaten wurden in Erwägung gezogen?

Begründung der Dringlichkeit: Die Erfassung der Daten in den Gastrobetrieben ist bereits Realität.

Antwort des Regierungsrates

Frage 1

Bei der Implementierung der zentralen Datenbank für die Kontaktdatenerfassung wurden die Vorgaben des Kantons Bern zur Informationssicherheit und zum Datenschutz (ISDS) berücksichtigt. Die entsprechende Datenbank wurde unter engem Einbezug der Datenschutzaufsichtsstelle (DSA) erstellt, dieser zur Vorabkontrolle unterbreitet und es wurden externe Sicherheitstests durchgeführt.

Frage 2

Eine personenbezogene Abfrage ist weder technisch noch organisatorisch möglich (vgl. Antwort zu Frage 3).

Frage 3

Eine Anonymisierung der Daten ist nicht vorgesehen und würde den Anforderungen des Contact Tracings zuwiderlaufen. Die Personendaten sind hingegen durch die implementierte Verschlüsselung pseudonymisiert, d. h. ohne direkten Personenbezug in der Datenbank gespeichert.

Der Abruf der verschlüsselten Daten erfolgt erst in einem durch einen ärztlichen Mitarbeiter bzw. eine ärztliche Mitarbeiterin im Vieraugenprinzip bewilligten Vorgang bei einem epidemiologisch relevanten Ereignis. Die hierzu berechtigten wenigen Mitarbeitenden des Contact Tracings starten mit den Parametern «betroffener Betrieb» und «Zeitfenster» einen Suchlauf und exportieren die verschlüsselten Kontaktdaten in die Contact-Tracing-Applikation TRACY. Erst während des Exportvorgangs werden die Kontaktdaten entschlüsselt. Sie sind erst in TRACY im Klartext (d.h. entschlüsselt) verfügbar.

Frage 4

Dem Kanton Bern unterliegt einzig die Gewährleistung der Datenschutzsicherheit der eigenen Datenbanken. Die sog. Registrierungsapps werden von Privaten angeboten und sind in der Regel in der ganzen Schweiz verfügbar. Alle Kommunikationsbeziehungen von, zu und in der zentralen Datenbank sind ausnahmslos verschlüsselt.

Frage 5

Mittels Löschprozessen werden auf der kantonalen zentralen Datenbank die Daten gemäss Methode der DIN 66398 automatisch nach 14 Tagen gelöscht.

Frage 6

Das Bundesgesetz über den Datenschutz (DSG) verbietet das Zusammenführen von Informationen aus zweckgebundenen Datenbanken ohne Einwilligung der betroffenen Personen. Auf kantonaler Stufe ist Art. 3b Abs. 1 und 2 der kantonalen Covid-19 Verordnung massgebend. Andere Direktionen und Behörden haben keine Zugriffsberechtigung auf die Datenbank.

Frage 7

Die Datenbank wurde unter engem Einbezug mit der Datenschutzaufsichtsstelle des Kantons Bern (DSA) konzipiert und eingeführt. Zur Gewährleistung einer maximalen Datensicherheit wurden marktübliche Penetrationstests durchgeführt. Die nach Art. 17a KDSG notwendigen ISDS-Dokumente wurden erarbeitet

und der Datenschutzaufsichtsstelle zur Vorabkontrolle eingereicht. Zudem plant die Datenschutzaufsichtsstelle in den nächsten Wochen eine eigene Informationssicherheitsprüfung (Audit) durchzuführen, zu welcher die Vorbesprechung bereits erfolgt ist.

Frage 8

Bis im Mai 2021 wurden die Kontaktdaten dezentral und ohne genaue Vorgaben bezüglich Format gespeichert. Dies hatte zur Folge, dass das Contact Tracing bei Ereignissen, in deren Zusammenhang Kontaktdaten eingefordert werden mussten, Daten von sehr unterschiedlicher Qualität erhielt. Die eingereichten Kontaktangaben waren oft sehr lückenhaft und vom Format her nicht einheitlich, was für das Contact Tracing viel Aufbereitungsarbeit gefordert hat. Auch enthielten sie teilweise falsche oder absurde Namen (Hitler, Donald Duck...) oder falsche Daten, was ein Hinweis dafür war, dass die Daten in keiner Weise validiert wurden. Die Daten mussten im Einzelfall vom Contact Tracing eingefordert werden. Teilweise war es sehr schwierig, die zuständigen Personen eines Gastrobetriebs zu erreichen. Die dadurch verursachten zeitlichen Verzögerungen laufen den Anstrengungen eines effizienten Contact Tracings entgegen. Wollte man nicht vollständig auf das Contact Tracing mittels Kontaktdatenerhebung verzichten, musste daher eine zentrale Lösung implementiert werden. Hierbei wurde auch die Lösung eines privaten Anbieters geprüft, aus Datenschutzgründen dann aber zugunsten der jetzigen Lösung verworfen.

Verteiler

– Grosser Rat