

Sitzung vom 9. November 2022

**1477. Anfrage (Fehlender Datenschutz bei der kantonalen Corona-Datenbank)**

Die Kantonsrätinnen Nicola Yuste, Zürich, Michèle Dünki-Bättig, Glattfelden, und Pia Ackermann, Zürich, haben am 11. Juli 2022 folgende Anfrage eingereicht:

Wie der Tagesanzeiger am 11. Juli berichtete, kam es bei der Corona-Datenbank «Sormas» des Kantons Zürich, die von der Firma JDMT im Auftrag des Kantons geführt wird, zu einem massiven Datenleck, welches erst durch die journalistische Recherche entdeckt wurde. Die kantonale Datenbank enthält rund 950'000 Datensätze mit teils höchst privaten und damit besonders schützenswerten Daten: z. B. Namen, Kontaktdaten, Krankengeschichte oder Ansteckungsdatum sind dort von allen Bewohnerinnen und Bewohnern gespeichert, die einmal positiv getestet oder in Quarantäne geschickt wurden. Die Sicherheitslücke kam wohl dadurch zustande, dass ein Grossteil der Mitarbeitenden Ende März 2022 entlassen wurde, sie aber weiterhin uneingeschränkt Zugang zur Datenbank hatten. Ausserdem blieben nichtpersonalisierte Gruppenzugänge mit weitreichenden Administratorinnenrechten aktiv.

Gesundheitsdaten sind besonders sensitiv und schützenswert. Während der Corona-Pandemie wurden u. a. im Zuge des Contact Tracings unüblich viele dieser besonders schützenswerten Daten gesammelt und gespeichert. Die Bevölkerung musste viel «Vorschuss-Vertrauen» aufbringen. Sicherheitslücken wie diese gefährden das Vertrauen der Bevölkerung in den Staat.

Vor diesem Hintergrund bitten die Antragstellerinnen den Regierungsrat um die Beantwortung der folgenden Fragen:

1. Wie ist der Prozess, um neue Logins im Sormas-System einzurichten? Wer resp. welche Abteilungen ist/sind involviert und wer führt welche Schritte aus?
2. Wie ist der Prozess, um nicht mehr gültige Logins im Sormas-System zu löschen? Wer resp. welche Abteilungen ist/sind involviert und wer führt welche Schritte aus?
3. Welche vertragliche Regelung gab es zwischen dem Amt für Gesundheit und der Firma JDMT im Bezug auf den Datenschutz?
4. Die Verantwortung für das Sormas-System liege gemäss eigenen Aussagen beim Amt für Gesundheit. Wie wurde die Datenschützerin in den Betrieb des Systems einbezogen?

5. Wusste das Amt für Gesundheit, dass die Betreiberin JDMT es versäumt hat, Sicherheitsprüfungen vorzunehmen, bevor die Angestellten Zugang zu den besonders schützenswerten Daten (z. T. mit Administratorinnenrechten) erhielten? Wenn Ja: Was hat das Amt dazu unternommen?
6. Das Sormas-System soll nur noch bis Ende August in Betrieb sein. Was geschieht mit den darin enthaltenen Datensätzen danach und wie wird der Schutz der Daten sichergestellt?
7. In Zukunft möchte das Amt für Gesundheit die Anbieter verpflichten, die Daten des Contact Tracings in einer eigenen Software zu speichern. Eine weitere Software soll künftig als Schnittstelle zwischen Tracing-Firma und Amt für Gesundheit dienen. Wie will die Regierung den Datenschutz sicherstellen, wenn die besonders schützenswerten Personendaten in Zukunft bei Drittanbietern liegen? Ist die Datenschutzzerin in diese Abklärungen involviert?

Auf Antrag der Gesundheitsdirektion

beschliesst der Regierungsrat:

I. Die Anfrage Nicola Yuste, Zürich, Michèle Dünki-Bättig, Glattfelden, und Pia Ackermann, Zürich, wird wie folgt beantwortet:

Zu Fragen 1, 2, 4, 6 und 7:

Sormas ist eine E-Health-Software, die zum Management für Massnahmen zur Epidemienbekämpfung entwickelt worden ist. Der Kanton Zürich hat sich, wie auch elf weitere Kantone, nach der Evaluation der vorhandenen Pandemie-Software-Plattformen für das Contact Tracing für Sormas entschieden. Die Software war von Herbst 2020 bis Ende August 2022 im Einsatz (vgl. RRB Nrn. 841/2020, 351/2021 und 1122/2021). Vor der Implementierung des Systems wurde auch eine umfassende Prüfung hinsichtlich Informationssicherheit und Datenschutz vorgenommen. Die kantonale Datenschutzbeauftragte war in diesen Prozess einbezogen (vgl. Tätigkeitsbericht Datenschutzbeauftragte 2020, S. 25). Betrieben wurde Sormas vom Amt für Gesundheit (AFG). So war das AFG verantwortlich dafür, dass die Mitarbeiterinnen und Mitarbeiter der mit dem Contact Tracing beauftragten JDMT Medical Services AG (JDMT) Zugriff auf diese Datenbank hatten und der Zugriff bei Austritt einer Mitarbeiterin bzw. eines Mitarbeiters wieder gelöscht wurde. Aufgrund eines Fehlers im Prozessmanagement des AFG wurde die Zugriffsberechtigung beim Austritt der Mitarbeiterinnen und Mitarbeitern des Contact Tracings nicht gelöscht. Als diese Sicherheitslücke am 4. Juli 2022 festgestellt worden ist, hat das AFG diesen Fehler umgehend behoben und die veralteten Logins sofort deaktiviert. Bis zum vollständigen Ab-

bau des Systems wurde eine verantwortliche Person im AFG festgelegt, die sämtliche Zugriffsberechtigungen geprüft und gelöscht hat. Auch die kantonale Datenschutzbeauftragte wurde umgehend über den Vorfall informiert. Bis anhin ist kein weiterer unbefugter Zugriff auf die Daten bekannt geworden. Es gibt auch keine Hinweise auf weitere Auswirkungen des Vorfalls.

Der Vertrag des AFG mit dem Anbieter der Software Sormas lief Ende August 2022 aus. Mit der Beendigung der Zusammenarbeit wurden die Datensätze der Sormas-Software per 2. September 2022 unwiderruflich gelöscht.

Die von der kantonalen Datenschutzbeauftragten in ihrer Stellungnahme vom 25. August 2022 vorgeschlagenen technischen und organisatorischen Massnahmen werden umgesetzt, um die Informationssicherheit und den Datenschutz in Zukunft zu verbessern. Auch die Entwicklung der eigenen Software für das Contact Tracing erfolgte unter Einbezug der Datenschutzbeauftragten. So wurde ihr insbesondere das Informationssicherheits- und Datenschutzkonzept zur Prüfung vorgelegt. Künftig soll die Software in das Amt für Informatik migriert werden, sodass die Daten nicht mehr bei einem Drittanbieter, sondern beim Kanton liegen.

Zu Frage 3:

Für die Sicherstellung des kantonalen Contact Tracings in der Coronapandemie wurde am 26. August 2020 eine Leistungsvereinbarung mit JDMT abgeschlossen. Es wurden dabei die im Kanton anwendbaren Vorgaben bezüglich Geheimhaltung und Datenschutz berücksichtigt und insbesondere die vom Regierungsrat festgelegten Allgemeinen datenschutzrechtlichen Geschäftsbedingungen bei der Datenbearbeitung durch Dritte miteingeschlossen. Weitere Anregungen der Datenschutzbeauftragten, welcher der Vertragsentwurf zur Prüfung der datenschutzrechtlichen Vorgaben vorgelegt worden ist, wurden berücksichtigt (vgl. Tätigkeitsbericht Datenschutzbeauftragte 2020, S. 25).

Zu Frage 5:

Zu Beginn der Pandemie stand im Vordergrund, möglichst rasch Mitarbeiterinnen und Mitarbeiter für das Contact Tracing zu rekrutieren und auszubilden (z. B. mussten zu Spitzenzeiten bis zu 8000 Anrufe pro Tag verarbeitet werden). Zürich als bevölkerungsreichster Kanton der Schweiz war beim Aufbau des Contact Tracings deutlich stärker gefordert als kleinere Kantone. JDMT musste teilweise mehrere Dutzend Personen pro Tag einstellen und beschäftigte eine Zeit lang mehr als 800 Mitarbeiterinnen und Mitarbeiter. Bei der Einstellung mussten alle Mitarbeitenden eine Vertraulichkeits- und Geheimhaltungserklärung unterzeichnen, die laut JDMT auch eingehalten worden ist.

II. Mitteilung an die Mitglieder des Kantonsrates und des Regierungsrates sowie an die Gesundheitsdirektion.

Vor dem Regierungsrat

Die Staatsschreiberin:

**Kathrin Arioli**