Schlussbericht

vom 16.03.2023

mit Ergänzungen vom 28.04.2023

des

Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten
(EDÖB)

im Verfahren gemäss
Artikel 29 des Bundesgesetzes vom 19. Juni 1992
über den Datenschutz (DSG; SR 235.1)

betreffend die vom
Einzelunternehmen [redacted]
geführten Covid-Testzentren [redacted]

Inhalt

1. Einführung

1.1. Grundlagen und Umfang der Sachverhaltsabklärung

1 Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) beaufsichtigt gestützt auf das Bundesgesetz vom 19. Juni 1992 über den Datenschutz (DSG; SR 235.1) die Datenbearbeitungen von Bundesorganen und privaten Personen. Er klärt von sich aus oder auf Meldung Dritter hin einen Sachverhalt näher ab, wenn Bearbeitungsmethoden geeignet sind, die Persönlichkeit einer grösseren Anzahl von Personen zu verletzen (sog. Systemfehler; Art. 29 DSG). Gemäss Art. 29 Abs. 2 DSG kann er dabei Akten herausverlangen, Auskünfte einholen und sich Datenbearbeitungen vorführen lassen.

2 Zwischen Dezember 2020 und Februar 2022 konnten sich Privatpersonen in den privaten Covid Testzentren [redacted] an acht verschiedenen Standorten in der Schweiz (sowie an einem Standort im Fürstentum Liechtenstein) für einen Covid-19-PCR-Test anmelden und testen lassen. Die PCR-Tests wurden anschliessend in einem Laboratorium in Österreich ausgewertet und in einer Datenbank in Österreich gespeichert.

3 Die vorliegende Sachverhaltsabklärung bezieht sich auf die im Zusammenhang mit einer Meldung einer Privatperson bekannt gewordenen Mängel bei der Datenbearbeitung durch die vom Einzelunternehmen [redacted] in der Schweiz betriebenen Covid-Testzentren.

4 Die Abklärung der datenschutzrechtlichen Aspekte, insbesondere der Datensicherheit, durch den EDÖB stützte sich insbesondere auf die schriftlichen Eingaben des Verantwortlichen, auf einen telefonischen Austausch mit dem Betreiber der Datenbank, auf schriftliche und telefonische Ausführungen der meldenden Person, auf schriftlichen und telefonischen Austausch mit Behörden und auf öffentlich zugängliche Informationen.

1.2. Partei und Beteiligte

5 Partei im vorliegenden Verfahren ist [redacted], verantwortlicher Arzt der Covid-Testzentren und Inhaber des Einzelunternehmens [redacted], welcher die Covid-Testzentren und die Webseite [redacted] zur Durchführung von COVID-19 PCR-Tests betrieben hat. Bei dem Einzelunternehmen mit Sitz in [redacted] handelt es sich um ein Einzelunternehmen im Sinne von Art. 945 OR mit dem im Handelsregister eingetragenen Zweck «COVID-19 Tests».

6 Eine weitere beteiligte Person ist [redacted], der Entwickler und Betreiber der Covid-Test-Datenbank in Österreich, in welcher die Personendaten der Testresultate gespeichert wurden.

7 Das Verfahren wird von folgenden Mitarbeitenden des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB) instruiert:

- Nathalie Weber, Leiterin Team 1 Datenschutz
- Joël Schwizgebel, Jurist Team 1 Datenschutz
- Philippe Schwab Molnar, Informations- und Sicherheitsspezialist, Kompetenzzentrum IT und digitale Gesellschaft

1.3. Chronologie

8 Am **9. November 2022** erhielt der EDÖB Hinweise einer Privatperson, wonach die Datenbank, in welcher die Testresultate von Covid-Testzentren gespeichert worden waren, unzureichend gegen unbefugte Zugriffe gesichert und rund eine Million Datensätze frei zugänglich gewesen seien. Die Person meldete den Vorfall ebenfalls dem Nationalen Zentrum für Cybersicherheit (NCSC) sowie dem Bundesamt für Gesundheit (BAG). Es folgte ein Austausch des EDÖB mit dem NCSC und dem BAG.

9 Der NCSC informierte am **9. November 2022** den zuständigen Betreiber der in Österreich angelegten Datenbank, [redacted], telefonisch über den Vorfall, worauf dieser die Datenbank gemäss seinen Angaben gleichentags vom Server nahm und auf einen verschlüsselten physischen Datenträger verschob.

10 Der EDÖB hatte am **10. November 2022** telefonischen Kontakt mit der meldenden Person. Anlässlich des Austauschs teilte die Person dem EDÖB mit, dass sie sich über die auf der Webseite frei einsehbaren Informationen Zugang zur Datenbank verschafft und eine Kopie der Datenbank heruntergeladen habe.

11 Zwischen dem **10. und 11. November 2022** informierte der EDÖB amtshilfeweise die Datenschutzaufsichtsbehörden der Kantone St. Gallen, Zürich und Glarus sowie die Datenschutzstelle des Fürstentums Liechtenstein und die Österreichische Datenschutzbehörde über den Vorfall.

12 Mit Schreiben vom **11. November 2022** richtete sich der EDÖB an den verantwortlichen Arzt und Betreiber der Covid-Testzentren («Verantwortlicher»), [redacted], und ersuchte ihn, zum gemeldeten Datenleck bis zum 25. November 2022 schriftlich Stellung zu nehmen. Der Verantwortliche wurde insbesondere dazu aufgefordert, darüber Auskunft zu geben, ob er das gemeldete Datenleck bestätigen und mithilfe von Protokollierungen oder Logs feststellen kann, ob es zu einem Datenabfluss gekommen ist, ob und welche Sofortmassnahmen inzwischen ergriffen worden sind und ob und in welcher Form die Betroffenen über informiert worden sind. Weiter informierte der

EDÖB den Verantwortlichen, dass die Österreichische Datenschutzbehörde ebenfalls über den Vorfall informiert wurde, da gemäss den dem EDÖB vorliegenden Angaben die in den Testzentren durchgeführten PCR-Tests in Österreich ausgewertet wurden, und die Datenbank, in welcher die entsprechenden Personendaten gespeichert wurde, ebenfalls in Österreich gehostet und betrieben wurde.

13 Nach einem E-Mail-Austausch und vereinbartem Termin übergab die meldende Person dem EDÖB am **24. November 2022** den betroffenen Datensatz, damit der EDÖB diesen im Rahmen des aufsichtsrechtlichen Verfahrens zu Beweiszwecken sicher verwahrt. Die meldende Person hat dem EDÖB schriftlich bestätigt, den Datensatz bei ihr nach der Übergabe unwiderruflich und vollständig gelöscht zu haben.

14 Am **25. November 2022** kontaktierte der EDÖB den Verantwortlichen per E-Mail und forderte ihn dazu auf, ihm die aktuelle Postadresse anzugeben, da das an die im Handelsregister eingetragene Postanschrift adressierte Schreiben vom 11. November 2022 innerhalb der 7-tägigen Abholfrist nicht zugestellt werden konnte. Gleichzeitig sendete er dem Verantwortlichen eine Kopie des Schreibens vom 11. November 2022. Der Verantwortliche gab dem EDÖB gleichentags seine neue Zustelladresse bekannt. Daraufhin sendete der EDÖB dem Verantwortlichen sein Schreiben vom 25. November 2022 vorab per E-Mail, mit welchem er den Verantwortlichen informierte, dass er ein formelles Verfahren im Sinne von Art. 29 Abs. 1 lit. a DSG eröffnet hat, da von der als mangelhaft angezeigten Bearbeitung gesundheitsbezogener und damit besonders schützenswerter Personendaten i.S.v. Art. 3 Bst. c. Ziff. 2 DSG eine grosse Anzahl von Personen betroffen ist.

15 Am **30. November 2022** richtete sich der EDÖB erneut an den Verantwortlichen, und unterbreitete ihm in Ergänzung seiner vorangehenden Schreiben eine ergänzende Zusammenfassung des dem EDÖB zu diesem Zeitpunkt bekannten Sachverhalts, mit der Bitte um Bestätigung, Ergänzung oder Korrektur, sowie einige zusätzliche Fragen. Weiter teilte der EDÖB dem Verantwortlichen mit, dass sich die meldende Person Zugang zur Datenbank verschafft und eine Kopie der Datenbank oder eines Teils davon heruntergeladen hatte, und er verlängerte die Frist für die Einreichung einer Stellungnahme bis zum 7. Dezember 2022.

16 Am **1. Dezember 2022** übermittelte der Verantwortliche seine Stellungnahme bezüglich der vom EDÖB mit den Schreiben vom 11., 25. und 30. November 2022 gestellten Fragen. Der Verantwortliche nahm insbesondere Stellung zur Rollenverteilung und Funktionsweise der Covid-Testzentren. Weiter führte er aus, dass der Datenbank-Betreiber die Datenbank als Sofortmassnahme die Datenbank vom Server genommen habe und gemäss Art. 33 DSGVO eine Stellungnahme an die Datenschutzbehörde in Österreich abgegeben wurde, welche nach einer Prüfung mitgeteilt habe, dass keine weiteren Schritte zu erfolgen haben und das Verfahren eingestellt wurde. Schliesslich führte der Verantwortliche in Bezug auf die Information an Betroffene aus, diese seien nicht zu informieren,

da nur jene Person auf die Datenbank zugegriffen habe, welche die Daten an den EDÖB weitergegeben hatte, und da aufgrund der ergriffenen Sofortmassnahmen die Gefahr für die betroffenen Personen ausgeschlossen sei.

17 Mit Schreiben vom **20. Dezember 2022** stellte der EDÖB dem Verantwortlichen Ergänzungsfragen zu seinen in der Stellungnahme vom 1. Dezember 2022 enthaltenen Ausführungen.

18 Am **22. Dezember 2022** erfolgten Berichterstattungen über den Vorfall der Covid-Testzentren in den Online-Medien Watson (watson.ch) und IT-Inside (it-inside.ch).

19 Am **6. Januar 2023** beantwortete der Verantwortliche die Ergänzungsfragen des EDÖB.

2. Sachverhaltsfeststellung

2.1. Betrieb und Organisation der Testzentren

20 Zwischen Dezember 2020 und dem 17. Februar 2022 konnten sich Privatpersonen in den von [redacted] als verantwortlichen Arzt betriebenen, privaten Covid-Testzentren ([redacted]) an acht verschiedenen Standorten in der Schweiz (je zwei Standorten in Zürich und St. Gallen, sowie einem Standort in Egg bei Zürich, Diepoldsau, Glarus und Frauenfeld) für einen Covid-19 PCR-Test anmelden und testen lassen. Der Inhaber des Einzelunternehmens [redacted] wurde im Impressum der archivierten Webseite [redacted] als verantwortlicher Arzt und Verantwortlicher für Datenschutz aufgeführt.

21 Die in den Testzentren durchgeführten PCR-Tests wurden nach der Entnahme in einem von der [redacted] mit Sitz in Österreich oder von der [redacted] mit Sitz in Österreich [redacted] geführten Laboratorium ausgewertet. Gestützt darauf wurden Covid-Zertifikate durch die mit der Auswertung befassten Gesellschaft ausgestellt.

22 Die Testresultate wurden anschliessend in einer in Österreich gehosteten und betriebenen Datenbank gespeichert. Der Vorfall des gemeldeten Datenlecks, bei der sich die meldende Person über die im frei zugänglichen Verzeichnis einsehbaren Informationen Zugang verschaffen konnte, ereignete sich in dieser Datenbank. Auf die Aspekte der Datensicherheit wird im folgenden Kapitel näher eingegangen.

2.2. Datensicherheit

23 Der Umfang der Analyse beschränkt sich auf die Datensicherheitsaspekte der Datenbank, in welcher die Testresultate gespeichert wurden.

24 In der in Österreich gehosteten und betriebenen Datenbank wurden die Testresultate gespeichert, wobei es sich um Namen und Vornamen der Personen, die sich in den Testzentren testen liessen, sowie deren Telefonnummern, E-Mail-Adressen, Geburtsdaten, PLZ, Angaben zu Datum und Ergebnis des Covid-Tests (einschliesslich CT-Wert) handelte. Für den Betrieb der Datenbank wurde das Datenbankmanagementsystem «MongoDB» verwendet.

25 Bei der entdeckten Sicherheitslücke des Webservers für den Zugriff auf die Datenbank handelte es sich um eine sogenannte «.env»-Schwachstelle, bei der sich die meldende Person über die in der frei zugänglichen «.env»-Datei einsehbaren Informationen Zugang zur Datenbank verschafft und eine Kopie der Datenbank heruntergeladen hat, wobei es sich um Daten von rund 873'000 Tests aus Österreich, 133'000 Tests aus der Schweiz und 19'000 Tests aus dem Fürstentum Lichtenstein handelte.

26 Die Zahl der 133'000 Tests aus der Schweiz konnten mithilfe der Angaben aus dem Covid-Zertifikate-System des BAG plausibiliert werden.

27 Einige Software-Produkte speichern ihre Konfiguration in sogenannten Umgebungs-Variablen (environment variables oder «.env»-Datei) ab, auf welchen oft Pfade zu bestimmten Programmen oder Daten, wie Zugriffsinformationen, enthalten sind (vgl. Mitteilung des NCSC vom 27.10.2022, abrufbar unter www.ncsc.admin.ch[1]).

28 Auf dem Webserver für die betroffenen Datenbank war diese «.env»-Datei jedoch nicht versteckt abgelegt, sondern frei zugänglich. Gemäss den Angaben des Verantwortlichen lag der Grund der freien Zugänglichkeit der «.env»-Datei darin, dass anlässlich einer im Oktober 2022 durchgeführten Systemwartung ein ExpressJS-Microservice nicht wieder gestartet wurde, was zu einer Exponierung der betroffenen «.env»-Datei während eines Zeitraums von ungefähr 39 Tagen führte.

29 In der exponierten «.env»-Datei waren unter anderem die Zugriffsdaten für die Datenbank enthalten (Benutzername und Passwort). Da keine Zwei-Faktoren-Authentifizierung eingerichtet wurde (mittels einem weiteren Faktor, der sich nicht in der «.env»-Datei befindet) und alle für den Zugriff der

[1] https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2022/git.html (zuletzt besucht am 13.03.2023)

Datenbank benötigten Informationen in der «.env»-Datei enthalten waren, erlaubte dies der meldenden Person, Zugang zu dieser Datenbank und somit auch zu den darin gespeicherten Personendaten zu erhalten. Die meldende Person hat darauf eine Kopie des Datensatzes heruntergeladen und dem EDÖB die Schwachstelle am 9. November 2022 gemeldet.

30 Der verantwortliche Datenbank-Betreiber nahm am Tag der Kenntnisnahme des Datenlecks (9. November 2022) als Sofortmassnahme die Datenbank vom Server und verschob deren Inhalt auf einen verschlüsselten physischen Datenträger.

31 Am 24. November 2022 übergab die meldende Person dem EDÖB eine Kopie des betroffenen Datensatzes. Der EDÖB hat den Datensatz zu Beweissicherungszwecken für die Dauer des aufsichtsrechtlichen Verfahrens gestützt auf Art. 29 DSG angenommen und als provisorische Massnahme sicher verwahrt, zumal zu diesem Zeitpunkt die Möglichkeit der Gewährleistung der Betroffenenrechte sowie die Notwendigkeit einer Sicherung der Beweismittel noch unklar war. Die meldende Person bestätigte dem EDÖB in der Folge, den Datensatz bei ihr nach der Übergabe unwiderruflich und vollständig gelöscht zu haben.

32 Zu den Sicherheitseigenschaften der Datenbank führte der Verantwortlichen aus, es werde mit der Datenbank (MongoDB) eine durch Benutzername und Passwort gesicherte Verbindung aufgebaut, welche aus einem sehr langen Passwort bestehe, um «BruteForce» Angriffe quasi zu verunmöglichen. Weiter sei die Datenbank nicht auf einem Standardport betrieben, um das System gegenüber massenhaften Portscans nicht zu exponieren.

33 Gemäss einer Analyse des NCSC jedoch wurde der Zugriff auf die Datenbank, d.h. die Verbindung vom Internet zur Datenbank, nicht verschlüsselt, und es wurden offene Netzwerk-Ports verwendet.

34 Die Zugriffe auf die «.env»-Datei wurden mittels einer Logdatei «access.log» des Webservers geprüft, welche die Zugriffe auf die Daten für mindestens zwei Monate protokolliert. Gemäss den Angaben des Verantwortlichen erfolgte kein anderer unbefugter Zugriff als derjenige der meldenden Person.

35 Eine Information der Betroffenen über die Exposition ist nicht erfolgt. Der Verantwortliche führte diesbezüglich aus, die Betroffenen seien nicht zu informieren, da nur die meldende Person auf die Datenbank zugegriffen habe und die Gefahr für die betroffenen Personen aufgrund der ergriffenen Sofortmassnahmen ausgeschlossen sei.

36 Der Verantwortliche führte aus, dass er die Daten weiterhin aufbewahre, da er generell von einer Aufbewahrungspflicht von 10 Jahren ausgehe, da es sich bei den Covid-Tests um eine ärztliche Leistung handelt und diese laut FMH mindestens 10 Jahre dokumentiert werden müssten.

3. Rechtliche Würdigung

3.1. Auftragsdatenbearbeitung mit Auslandbezug

37 Im Rahmen des Betriebs der Covid-Testzentren hat der Verantwortliche als leitender Arzt verschiedene Dritte mit der Datenbearbeitung beauftragt:

- die Auswertung der Covid-Tests wurde durch ein Laboratorium der [redacted] mit Sitz in Österreich oder der [redacted] mit Sitz in Österreich durchgeführt;
- das Ausstellen der Covid-Zertifikate erfolge durch die [redacted] mit Sitz in Österreich oder die [redacted] mit Sitz in Österreich;
- die Speicherung der Testresultate erfolgte schliesslich durch einen Datenbank-Betreiber in einer Datenbank in Österreich.

38 Mit der Durchführung von Covid-19 PCR-Tests durch die erwähnten Testzentren wurden Gesundheitsdaten und somit besonders schützenswerte Personendaten im Sinne des Datenschutzgesetzes im Auftrag eines Arztes bearbeitet. Bei einer Auftragsdatenbearbeitung von Gesundheitsdaten im Ausland sind folgende Voraussetzungen zu erfüllen:

39 Erstens dürfen Personendaten ins Ausland nur bekannt gegeben werden, wenn die Gesetzgebung des Ziellands einen angemessenen Schutz gewährleistet (Art. 6 Abs. 1 DSG) oder alternative Bedingungen eingehalten werden (Art. 6 Abs. 2 DSG).

40 Zweitens müssen die Voraussetzungen von Art. 10a DSG erfüllt sein. Gemäss Art. 10a Abs. 1 DSG kann das Bearbeiten von Personendaten durch Vereinbarung oder Gesetz Dritten übertragen werden, wenn die Daten nur so bearbeitet werden, wie der Auftraggeber selbst es tun dürfte und keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet. Bei dem für Ärztinnen und Ärzte anwendbaren Berufsgeheimnis (Art. 321 Ziff. 1 Abs. 1 StGB) umfasst die Pflicht zur Verschwiegenheit auch Hilfspersonen, die einbezogen werden können, soweit dies für die Erfüllung der übertragenen Aufgabe notwendig ist. Dabei sind auf folgende Punkte achten:

- Der Beizug von Dienstleistern im Ausland für die Bearbeitung von Personendaten (insb. Datenbank- oder Cloud-Anbieter sowie Auswertungen) sollte im medizinischen Kontext vermieden werden, da das ausländische Recht nicht immer einen dem Art. 321 StGB gleichwertigen Schutz aufweist.
- Die Wahrung von Geheimhaltungspflichten ist durch vertragliche Regelungen sicherzustellen, die den Anforderungen aus dem Arztgeheimnis genügen. Alle Personen mit Zugriff auf die Patientendaten müssen der ärztlichen Schweigepflicht unterstehen.

- Der Auftraggeber muss sich ausserdem vergewissern, dass der Dritte die Datensicherheit gewährleistet (Art. 10a Abs. 2 DSG).

41 Drittens sollten die betroffenen Personen gemäss dem Grundsatz von Treu und Glauben (Art. 4 Abs. 2 DSG) und dem Transparenzprinzip (Art. 4 Abs. 4 DSG) vorgängig über die Auslagerung der Datenbearbeitung ins Ausland informiert werden. Ob und in welcher Form diese Information beim Betrieb der Covid-Testzentren erfolgt ist (mündlich, mittels Abgabe von Formularen, etc.), bildete nicht Gegenstand der vorliegenden Untersuchung.

42 Es wird unter Hinweis des Gegenstands der vorliegenden Untersuchung und angesichts der Tatsache, dass der Betrieb der Testzentren inzwischen eingestellt worden ist, ausdrücklich offengelassen, ob die Auslagerung an Dritte in Österreich in der vorliegenden Konstellation die Voraussetzungen erfüllt haben (mit Ausnahme der Aspekte der Datensicherheit der Datenbank, welche im nachfolgenden Kapitel besprochen werden).

3.2. Datensicherheit

43 Gemäss Art. 7 DSG i.V.m. Art. 8 ff. VDSG müssen Personendaten durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden. Wer Daten bearbeitet, hat für die Vertraulichkeit, die Verfügbarkeit und die Integrität der Daten zu sorgen.

44 Im Falle einer Auftragsdatenbearbeitung muss sich der Auftraggeber insbesondere vergewissern, dass der Dritte die Datensicherheit gewährleistet (Art. 10a Abs. 2 DSG). Der Auftraggeber hat die Verpflichtung der sorgfältigen Wahl, Instruktion und Überwachung des Dritten und bleibt letztlich gegenüber den betroffenen Personen verantwortlich für die Einhaltung der datenschutzrechtlichen Vorschriften und haftet bei allfälligen Verletzungen.

45 Bei der Bearbeitung von besonders schützenswerten Personendaten sind erhöhte Anforderungen an die Datensicherheit zu stellen. Dabei gilt es bei der Auslagerung der Aufbewahrung solcher Daten durch angemessene technische und organisatorische Massnahmen dafür zu sorgen, dass keine ungerechtfertigte Bearbeitung durch Dritte erfolgt. Alle Verbindungen, insbesondere die Verbindung für den Zugriff auf die Datenbank, müssen verschlüsselt werden und eine Zwei-Faktoren-Authentifizierung sollte die Zugriffe auf die Daten auf die berechtigen Personen beschränken. Diese Massnahmen sind periodisch zu überprüfen.

46 Im Rahmen des Betriebs der Covid-Testzentren hat der Verantwortliche verschiedene Dritte mit der Datenbearbeitung beauftragt, insbesondere den Datenbank-Betreiber für die Speicherung der ausgewerteten Testresultate in einer Datenbank. Dabei musste der Verantwortliche sicherstellen, dass

die Datensicherheit jederzeit gewährleistet ist und der beauftragte Datenbank-Betreiber angemessene technische und organisatorische Massnahmen trifft, um die Datenbank gegen unbefugtes Bearbeiten zu schützen.

47 Somit gilt auch festzustellen, dass die Ausführungen des Verantwortlichen gegenüber den Online-Zeitschriften Watson und IT-Inside im Rahmen der Berichterstattungen vom 22. Dezember 2022, dass er Arzt und kein IT-Dienstleister sei, die Daten von einem externen IT-Unternehmen gesichert würden und die Vorkommnisse deswegen ausserhalb seines Wirkungsbereichs lägen, unzutreffend sind. Als Verantwortlicher und Auftraggeber bleibt er verantwortlich für die Datensicherheit und Datenschutzkonformität der beauftragten Dienstleister.

48 Im Rahmen des Betriebs der in Österreich gehosteten Datenbank sind verschiedene Datensicherheitsmängel festzustellen:

3.2.1. Freie Zugänglichkeit der «.env»-Datei

49 Da «.env»-Konfigurationsdateien sensible Daten wie Zugriffsinformationen enthalten, sollten diese auf einem produktiven System zu keinem Zeitpunkt öffentlich im Internet zugänglich sein. In der Datenbank wurde die «.env»-Konfigurationsdatei infolge einer Systemwartung nicht versteckt abgelegt, sondern war frei im Internet zugänglich. Da auf der «.env»-Datei alle notwendigen Zugangsdaten enthalten waren und dadurch ein Zugriff auf die Datenbank durch unbefugte Personen möglich war, stellte dies eine kritische Schwachstelle dar. Einer solchen Konfigurationsdatei müssen jederzeit die richtigen Attribute gesetzt werden, damit diese zu keinem Zeitpunkt öffentlich im Internet zugänglich ist. Aufgrund der kritischen Informationen, die auf der «.env»-Datei enthalten sind, muss dies regelmässig überprüft werden, insbesondere nach einer erfolgten Systemwartung. Der Datenbank-Betreiber hätte somit nach der im Oktober 2022 erfolgten Systemwartung sicherstellen müssen, dass die «.env»-Datei nicht exponiert wurde.

3.2.2. Unzureichende Authentifizierungsmethode

50 Weiter war die gewählte Authentifizierungsmethode für den Zugriff zur Datenbank und der darin gespeicherten Daten in der vorliegenden Konstellation unzureichend. Die Authentifizierung mittels Benutzername und Passwort – welche beide in der «.env»-Datei enthalten waren – ermöglichte es, durch eine Einsicht in die versehentlich freigestellte «.env»-Datei sowohl den Benutzernamen und als auch Passwort ausfindig zu machen und sich damit den Zugriff auf die Datenbank zu verschaffen. Die vom Verantwortlichen ausgeführte Tatsache, dass es sich um ein sehr langes Passwort handelt, ist in dieser Hinsicht nicht hilfreich, da alle für den Zugriff der Datenbank benötigten Informationen in der «.env»-Datei enthalten waren.

51 In Anbetracht der Bearbeitung von besonders schützenswerten Personendaten hätte zur Gewährleistung der Datensicherheit z.B. eine Zwei-Faktoren-Authentifizierung eingerichtet werden müssen, mit welcher ein Zugriff nur mithilfe eines weiteren Faktors, der sich nicht in der «.env»-Datei befindet, erlaubt hätte. Damit hätte verhindert werden können, dass ein unbefugter Zugriff auf die Datenbank alleine mithilfe der in der «.env»-Datei enthaltenen Zugangsdaten möglich ist.

3.2.3. Unverschlüsselte Verbindung zur Datenbank

52 Schliesslich erweist sich auch die Verwendung einer unverschlüsselten Verbindung zur Datenbank, offene Netzwerk Ports sowie exponierte Services als unzureichend, um einen angemessenen Schutz der Daten zu gewährleisten.

53 Angesichts der Sensibilität der Daten sowie dem aktuellen Stand der Technik stellt eine solche Konfiguration ein unzureichend geschütztes System dar. Es wurden somit nicht die angemessenen technischen und organisatorischen Massnahmen zur Gewährleistung der Datensicherheit getroffen, was eine Verletzung von Art. 7 DSG darstellt.

3.3. Information an Betroffene bezüglich der Datenschutzverletzung

54 Das geltende Schweizer Datenschutzrecht kennt keine ausdrückliche Pflicht zur Meldung von Datenschutzverletzungen gegenüber den Betroffenen. Nach Auffassung des EDÖB sowie der Lehre kann der Grundsatz der Datenbearbeitung nach Treu und Glauben (Art. 4 Abs. 2 DSG) jedoch eine Meldepflicht gegenüber dem betroffenen Datensubjekt begründen.

55 Sinn und Zweck dieser Informationspflicht ist es insbesondere, weitere Folgeschäden zu vermeiden oder zu reduzieren, indem die Betroffenen entsprechende Massnahmen treffen können. Die Informationspflicht an Betroffene besteht somit insbesondere, wenn Schritte von Betroffenen (oder sogar Dritten) zum Schutz der Daten notwendig sind. Dies entspricht auch der Auslegung des neuen Datenschutz-Gesetzgebung, die am 1. September 2023 in Kraft tritt[2].

56 In der vorliegenden Konstellation kann davon ausgegangen werden, dass aufgrund der ergriffenen Sofortmassnahmen keine Gefahr für die betroffenen Personen mehr besteht und dass diese keine

[2] Gemäss Art. 24 Abs. 4 revDSG informiert der Verantwortliche die betroffene Person, wenn es zu ihrem Schutz erforderlich ist. Gemäss der Botschaft des Bundesrats ist dies «insbesondere der Fall, wenn die betroffene Person entsprechende Vorkehren zu ihrem Schutz treffen muss, zum Beispiel indem sie ihre Zugangsdaten oder Passwörter ändert» (Botschaft, BBl 2017, 7065).

konkreten Massnahmen zum Schutz ihrer Daten ergreifen müssen: Am Tag der Kenntnis des Datenlecks wurde die Datenbank umgehend vom Server genommen und sämtliche Datensätze wurden offline auf einem verschlüsselten Datenträger gespeichert. Es war zudem kein anderer unbefugter Zugriff als derjenige der meldenden Person erfolgt, was die Verantwortlichen dank der Zugriffslogs bestätigen konnten (vgl. Rz 35). Darüber hinaus sind die Covid-Testzentren seit Februar 2022 nicht mehr in Betrieb.

57 Da keine Gefahr für die betroffenen Personen mehr besteht und diese keine weiteren Massnahmen zum Schutz ihrer Daten ergreifen müssen, kann in dieser spezifischen Konstellation von der Information an die Betroffenen abgesehen werden.

3.4. Aufbewahrung der Testresultate

3.4.1. Verantwortlicher

58 Die Daten waren noch vorhanden und werden weiterhin auf einer Datenbank aufbewahrt. Der Verantwortliche macht geltend, dass eine Aufbewahrungspflicht gelte und führte aus, dass er generell von einer Aufbewahrungspflicht von 10 Jahren ausgehe, da es sich bei Covid-Tests um eine ärztliche Leistung handele und diese laut FMH mindestens 10 Jahre dokumentiert werden müssten. Sämtliche Datensätze seien nun offline auf einem verschlüsselten Datenträger gespeichert.

59 Eine Aufbewahrungspflicht eines leitenden Arztes von Covid-Testzentren könnte sich nach Auffassung des EDÖB aus kantonalen Gesundheitsgesetzen der Kantone, in welchen Testzentren betrieben wurden (Kantone Zürich, St. Gallen, Glarus, Thurgau), ergeben, welche eine zehnjährige Aufbewahrungsfrist vorsehen[3]. Die zehnjährige Frist entspricht ausserdem der steuerrechtlichen Aufbewahrungspflicht (Art. 126 Abs. 3 DBG) sowie der kaufmännischen Buchführungspflicht (Art. 957 ff OR).

60 Eine vertiefte Klärung der gesetzlichen Grundlagen ist nicht Gegenstand der vorliegenden Abklärung, das Bestehen einer mehrjährigen Aufbewahrungspflicht erscheint jedoch plausibel. Es bleibt mithin in der Verantwortung des Verantwortlichen, die Wahrung der Rechte der Betroffenen zu gewährleisten.

[3] Art. 13 Gesundheitsgesetz des Kantons Zürich; Art. 14 und 15 Verordnung über die Ausübung der medizinischen Berufe des Kantons St.Gallen; Art. 32 Gesundheitsgesetz des Kantons Glarus; Art. 20 Gesundheitsgesetz des Kantons Thurgau.

3.4.2. Vernichtung der Daten beim EDÖB

61 Der EDÖB hat den Datensatz als provisorische Massnahme zu Beweissicherungszwecken während der Dauer des aufsichtsrechtlichen Verfahrens (Art. 29 DSG) angenommen und sicher verwahrt.

62 Nach Abschluss des Verfahrens sowie des Sachverhaltsberichts wird der EDÖB den Datensatz unwiderruflich und vollständig vernichten, da keine Notwendigkeit für dessen Aufbewahrung mehr besteht.

3.5. Verzicht auf Erlass von Empfehlungen

63 Der EDÖB verzichtet im vorliegenden Verfahren auf den Erlass einer Empfehlung. Die in der vorliegenden Sachverhaltsabklärung festgestellten Mängel der Datensicherheit erweisen sich als erheblich, jedoch konnten die Risiken durch die ergriffenen Sofortmassnahmen behoben werden.

64 Da keine Gefahr für die betroffenen Personen mehr besteht und diese keine weiteren Massnahmen zum Schutz ihrer Daten ergreifen müssen, kann in dieser spezifischen Konstellation von der Information an die Betroffenen abgesehen werden.

4. Verfahren

4.1. Veröffentlichung des Schlussberichts

65 Der EDÖB kann seinen Schlussbericht gestützt auf Art. 30 Abs. 2 DSG veröffentlichen, wenn ein allgemeines Interesse daran besteht, über seine Feststellungen zu informieren.

66 Vorliegend besteht insbesondere im Hinblick auf eine allfällige Wiederaufnahme der Testzentren ein allgemeines Interesse daran, die Öffentlichkeit über die Feststellungen zu informieren. Der EDÖB beabsichtigt deshalb, den vorliegenden Bericht in angepasster Form, insbesondere ohne namentliche Nennung der beteiligten Personen und Unternehmen auf seiner Website (www.edoeb.admin.ch) zu veröffentlichen.

4.2. Rechtliches Gehör

67 Der EDÖB hat dem Verantwortlichen den vorliegenden Abschlussbericht überdies zur Prüfung der inhaltlichen Richtigkeit vorgelegt und ihn aufgefordert, ihm innerhalb von 30 Tagen nach Erhalt mitzuteilen, ob er eine Stellungnahme abgeben möchte.

68 Die Veröffentlichung des vollständigen Berichts (vgl. oben Ziff. 4.1) steht unter dem Vorbehalt, dass aus Sicht des Verantwortlichen keine vertraulichen Daten offengelegt werden, welche Geschäftsgeheimnisse preisgeben oder die Wettbewerbsfähigkeit beeinflussen könnten. Der Verantwortliche wurde deshalb auch aufgefordert, den Bericht auf solche vertraulichen Inhalte zu prüfen und dem EDÖB innert 30 Tagen schriftlich mitzuteilen, ob er eine teilweise Schwärzung des Berichts vor dessen Publikation als geboten erachtet.

69 Der EDÖB hat gestützt auf die eingegangene Stellungnahme des Verantwortlichen zwei punktuelle inhaltliche Präzisierungen im Abschlussbericht vorgenommen. Im Sinne des Persönlichkeitsschutzes wird der für die Publikation vorgesehene Bericht zudem teilweise geschwärzt.

Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte	Der zuständige Jurist
Adrian Lobsiger	Joël Schwizgebel