Nr. 143-BEA der Beilagen zum stenographischen Protokoll des Salzburger Landtages
(4. Session der 16. Gesetzgebungsperiode)

Beantwortung der dringlichen Anfrage

der Abg. Klubobfrau Svazek BA und Dr. Schöppl an Landeshauptmann-Stellvertreter Dr. Stöckl (Nr. 143-ANF der Beilagen) betreffend Datenleck auf der COVID-Anmeldeplattform zum kostenlosen Antigen-Schnelltest

Hohes Haus!

Zur Beantwortung der dringlichen Anfrage der Abg. Klubobfrau Svazek BA und Dr. Schöppl betreffend Datenleck auf der COVID-Anmeldeplattform zum kostenlosen Antigen-Schnelltest vom 3. Februar 2021 erlaube ich mir, Folgendes zu berichten:

Zu Frage 1: Welches Unternehmen ist für die Erstellung, Wartung und Sicherheit der Online-Plattform www.salzburg-testet.at verantwortlich?

Zu Frage 2: Wann haben Sie das erste Mal vom Datenleck und der infolge dessen Absaugung von 2.401 sensiblen Daten von Salzburgerinnen und Salzburgern erfahren?

Zu Frage 3: Wie gestaltete sich in weiterer Folge die Informationskette und wann wurden betroffene Salzburgerinnen und Salzburger vom Datenleck informiert?

Zu Frage 4: Welche Maßnahmen werden getroffen, um derartige Angriffe und Datenlecks in Zukunft zu verhindern?

Zu Frage 5: Bei wem sehen Sie die Verantwortung für den entstandenen Schaden, bei Ihnen als Auftragsgeber, beim Roten Kreuz oder beim beauftragten Unternehmen zur Erstellung, Wartung und Sicherheit der Online-Plattform?

In Beantwortung dieser dringlichen Anfrage darf ich auf die Stellungnahme des Roten Kreuzes und zusätzlich auch darauf verweisen, dass das Verfahren seitens der Datenschutzbehörde am 2. Februar 2021 eingestellt wurde (siehe Beilage).

Ich ersuche das Hohe Haus um Kenntnisnahme dieser Anfragebeantwortung.

Salzburg, am 5. Februar 2021

Dr. Stöckl eh.

STELLUNGNAHME
DRINGLICHE ANFRAGE SALZBURGER LANDTAG
der Abg. Klubobfrau Svazek BA und Dr. Schöppl

1. *Welches Unternehmen ist für die Erstellung, Wartung und Sicherheit der Online-Plattform www.salzburg-testet.at verantwortlich?*

   Insgesamt trägt das Land Salzburg als Auftraggeber sowie das Österreichische Rote Kreuz, Landesverband Salzburg, als Auftragsnehmer die Projektverantwortung für das Angebot freiwilliger SARS-CoV-2 Antigen Schnelltests und damit für dessen Erstellung, Wartung und Sicherheit.

   In einem gemeinsamen Projektausschuss, der aus den beiden angeführten Parteien besteht, wurden die Anforderungen für die Erstellung des „Front-Ends", nämlich der Website „salzburg-testet.at", sowie der angekoppelten Partnerplattform als „Back-End" definiert. Mit diesen vereinbarten Kriterien wurde ein spezialisiertes Softwareunternehmen mit der Erstellung durch das Österreichische Rote Kreuz, Landesverband Salzburg, beauftragt.

2. *Wann haben Sie das erste Mal vom Datenleck und der infolge dessen Absaugung von 2.401 sensiblen Daten von Salzburgerinnen und Salzburgern erfahren?*

   Vorerst ist festzuhalten, dass der in der Frage benutzte Wortlaut „sensiblen Daten" terminologisch irreführend ist.
   Ausschließlich die Sozialversicherungsnummer der von der Verletzung der Vertraulichkeit betroffenen personenbezogenen Daten stellt **ein personenbezogenes Datum besonderer Kategorie** iSd Art. 9 Abs. 1 DSGVO dar. (In der historischen Gesetzeslage des DSG-2000 wurde die Terminologie „sensibles Datum" verwendet.) Die restlichen von der Verletzung der Vertraulichkeit betroffenen personenbezogenen Daten stellen reguläre personenbezogene Daten iSd Art 6 DSGVO dar.

   Die erste Information über eine potentielle Verletzung der Vertraulichkeit personenbezogener Daten ging am Freitag, dem 15.01.2021, um ca. 11:00 beim Österreichischen Roten Kreuz, Landesverband Salzburg, ein.

3. *Wie gestaltete sich in weiterer Folge die Informationskette und wann wurden betroffene Salzburgerinnen und Salzburger vom Datenleck informiert?*

   Nach Eingang der Information am Freitag, dem 15.01.2021, wurde unverzüglich das zuständige Softwareunternehmen mit einer Analyse dieser beauftragt. Nach Festellung des gegebenen Sachverhaltes wurde umgehend eine Behebungsstrategie erarbeitet und in einem Update um 21:00 umgesetzt. Damit wurde die Gefahr der potentiellen Verletzung der Vertraulichkeit personenbezogener Daten gebannt.

Am Samstag, dem 16.01.2021, fand eine Dringlichkeitssitzung des Datenschutzbeauftragten des Verantwortlichen sowie des Auftragsverarbeiters statt, in der der Vorfall einer rechtlichen Prüfung unterzogen wurde. Es wurde umgehend einvernehmlich beschlossen, dass eine Meldung der Verletzung der Sicherheit personenbezogener Daten gem. Art. 33 DSGVO an die Datenschutzbehörde zu ergehen hat.

Diese wurde fristgerecht innerhalb von 72 Stunden am 18.01.2021 um ca. 11:00 durch den Datenschutzbeauftragen des Land Salzburgs übermittelt.

Auch wurde von dem Softwareunternehmen zur unverzüglichen Erhebung und Dokumentation ein Abschlussbericht angefordert, um ein klareres Bild von der Anzahl der betroffenen Personen sowie den erfolgten Downloads zu haben. Dieser Bericht wurde am Abend des Donnerstags, dem 22. Jänner 2021, übermittelt.

Gleichzeitig wurden die Kontaktadressen der betroffenen Personen erhoben. Diese wurden unter Berücksichtigung der Ergebnisse des Abschlussberichts am 28. Jänner 2021 vom Roten Kreuz, Landesverband Salzburg informiert. Ergänzend dazu wurde auch in einer öffentlichen Bekanntmachung über den Vorfall informiert.

4. *Welche Maßnahmen werden getroffen, um derartige Angriffe und Datenlecks in Zukunft zu verhindern?*

In Bezug auf den gegenständlichen Vorfall der Verletzung der Vertraulichkeit personenbezogener Daten wurden im Speziellen für „salzburg-testet.at“ die WEB Server um weiterer Sicherheitsmechanismen ergänzt. So werden unter anderem die Eingaben, die Anmeldungen sowie die Downloads am System durch eine „Zwei-Stufen-Authentifizierung“, wie beispielsweise auch von Banken im Onlinezahlungsverkehr verwendet, abgesichert.
In concreto bedeutet dies, dass bei der Anmeldung ein automatisch generierter TAN vergeben wird, der nur einmalig verwendet werden kann.

Darüber hinaus wurden auch auf organisatorischer Ebene Maßnahmen getroffen.
In technischer Beziehung wurden die Kontrollmechanismen des Softwareunternehmens als auch die der Projektverantwortlichen dementsprechend verschärft. Dies betrifft vor allem vorhergehende Testungen sowie Analysen.

In datenschutzrechtlicher Beziehung sind nun die Datenschutzbeauftragten des Verantwortlichen sowie des Auftragsverarbeiters in einem stark erhöhten Detailgrad in die Planungsphasen eingebunden, um potentielle Risiken schneller aufzeigen und deren Realisierung vorab verhindern zu können.

5. *Bei wem sehen Sie die Verantwortung für den entstandenen Schaden, bei Ihnen als Auftragsgeber, beim Roten Kreuz oder beim beauftragten Unternehmen zur Erstellung, Wartung und Sicherheit der Online-Plattform?*

   Die Skizzierung der Verantwortlichkeit wurde bereits in der 1. Frage abschließend beantwortet.

   Darüber hinaus ist in diesem Zusammenhang die Entscheidung der Datenschutzbehörde im Zuge des Verfahrens bezüglich der Meldung der Verletzung der Sicherheit personenbezogener Daten gem. Art. 33 DSGVO noch ausständig.

Republik Österreich
Datenschutz
behörde

Barichgasse 40-42
A-1030 Wien
Tel.: +43-1-52152 302596

E-Mail: dsb@dsb.gv.at

GZ: D084.2381
2021-0.080.648

Sachbearbeiterin: Mag. Vanessa NEUDECKER

Amt der Salzburger Landesregierung

Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde
(Art. 33 DSGVO, „Data-Breach-Verfahren“)
Sicherheitsverletzungen Art. 33 DSGVO - Amt der Salzburger Landesregierung

per E-Mail buero-lad@salzburg.gv.at

Betreff: Einstellung des Verfahrens

Mit Meldung vom 18. Jänner 2021 sowie der ergänzenden Meldung vom 1. Februar 2021 teilte das Land Salzburg - Amt der Salzburger Landesregierung (Verantwortlicher) mit, dass er die Verletzung des Schutzes personenbezogener Daten melde.

Zusammengefasst sei es am 14. Jänner 2021 (Zeitpunkt der Kenntniserlangung: 15. Jänner 2021) dazu gekommen, dass im Zuge des Anmeldevorgangs auf „salzburg-testet.at“ zu unberechtigten Downloads und damit zu einer Verletzung der Vertraulichkeit von personenbezogenen Daten gekommen sei. Die Behebung der Datenpanne sei am 15. Jänner 2021 erfolgt.

Insgesamt seien 2401 Personen von dem Vorfall betroffen.

Es seien die Daten der Kategorien

- Vor- und Nachname
- Sozialversicherungsnummer
- Geburtsdatum
- Angegebene Telefonnummer/ E-Mail-Adresse

betroffen gewesen.

Der Verantwortliche hat folgende Maßnahmen ergriffen, um die Verletzung zu beheben bzw. mögliche nachteilige Auswirkungen abzumildern:

- Der Download des Probandenlaufzettels auf der Bestätigungsseite wurde auf eine abgesicherte Downloadseite verlinkt. Diese ist mit einer generierten Download-ID (12-stellige alphanummerische ID) abgesichert.
- Darüber hinaus wird nun die Zugehörigkeit des Downloads mit dem Geburtsdatum der Person überprüft.

Der Verantwortliche hat die betroffene/n Person/en gemäß Art. 34 Abs. 1 DSGVO benachrichtigt. Ergänzend dazu wurde auch in einer öffentlichen Bekanntmachung durch das Rote Kreuz, Landesverband Salzburg, über den Vorfall informiert.

Der Verantwortliche hat geeignete Schritte unternommen, um das Risiko zu minimieren und um die nachteiligen Folgen der Sicherheitsverletzung, soweit möglich, zu beseitigen. Weitere Maßnahmen der Datenschutzbehörde iSd. Art 58 Abs. 2 lit. e DSGVO (Anweisung bzgl. Benachrichtigung der betroffenen Personen) bzw. § 22 Abs. 4 DSG (Mandatsbescheid bei Gefahr im Verzug) sind nicht geboten.

Das Verfahren wird daher beendet und dies dem Verantwortlichen abschließend zur Kenntnis gebracht.

Die Datenschutzbehörde behält sich im gegenständlichen Fall vor, zeitnah eine Datenschutzüberprüfung gemäß Art. 58 Abs. 1 lit. b DSGVO durchzuführen.

Unabhängig von der Einstellung des gegenständlichen Verfahrens behält sich die Datenschutzbehörde zudem vor, die Einleitung eines Verwaltungsstrafverfahrens zu prüfen.

2. Februar 2021
Für die Leiterin der Datenschutzbehörde:
NEUDECKER