**Ministerium für
Schule und Bildung
des Landes Nordrhein-Westfalen**

Die Ministerin

Ministerium für Schule und Bildung NRW, 40190 Düsseldorf

An den Vorsitzenden des
Ausschusses für Schule und Bildung
des Landtags Nordrhein-Westfalen
Herrn Florian Braun MdL
Platz des Landtags 1
40221 Düsseldorf

LANDTAG
NORDRHEIN-WESTFALEN
18. WAHLPERIODE

VORLAGE
18/1256

A15, A20

15. Mai 2023

Aktenzeichen:
131 – 01.11.01
bei Antwort bitte angeben

Dorothee Feller

Bericht zum Thema „Datenschutzmeldungen zu den IT-Datenlecks im Schulministerium“
Bitte der Fraktion der FDP um einen schriftlichen Bericht für die Sitzung des Ausschusses für Schule und Bildung am 17. Mai 2023

Sehr geehrter Herr Vorsitzender,

beigefügt übersende ich den Bericht zum Thema „Datenschutzmeldungen zu den IT-Datenlecks im Schulministerium“ für die Sitzung des Ausschusses für Schule und Bildung am 17. Mai 2023

Ich wäre Ihnen dankbar, wenn Sie diesen den Mitgliedern des Ausschusses für Schule und Bildung vorab zur Information zuleiten würden.

Mit freundlichen Grüßen

Dorothee Feller

Anschrift:
Völklinger Straße 49
40221 Düsseldorf
Telefon 0211 5867-40
Telefax 0211 5867-3220
poststelle@msb.nrw.de
www.schulministerium.nrw

Postanschrift:
Ministerium für
Schule und Bildung NRW
40190 Düsseldorf

Bericht des Ministeriums für Schule und Bildung des Landes Nordrhein-Westfalen

"Datenschutzmeldungen zu den IT-Datenlecks im Schulministerium"

Bitte der Fraktion der FDP um einen schriftlichen Bericht der Landesregierung zur Sitzung des Ausschusses für Schule und Bildung am 17. Mai 2023

Welche Informationen hat diese Mail genau enthalten? (Bitte Text vorlegen)

Wann sind welche Informationen an die Betroffenen versandt worden?

Der folgende Text ist von der Qualitäts- und UnterstützungsAgentur – Landesinstitut für Schule (QUA-LiS NRW) am 27. April 2023 an alle Nutzer des sog. BSCW-Servers, deren Nutzername und Kontaktdaten von der Offenlegung betroffen waren und bei denen in der Nutzerverwaltung eine E-Mail-Adresse hinterlegt war, per E-Mail verschickt worden:

„Sehr geehrte Damen und Herren,

per E-Mail vom 24.04.2023 wurden Sie gebeten, Ihr Passwort für den Zugang zum BSCW-Server zu ändern. In dieser heutigen E-Mail möchten wir Sie über den Hintergrund dieser Aufforderung informieren.

Am 20.04.23 wurden wir auf eine Fehlkonfiguration unseres BSCW-Servers hingewiesen, durch die für technisch versierte Personen die Möglichkeit bestand, auf Vorname, Nachname, Anschrift, Rufnummer, Mailadresse der Nutzenden zuzugreifen.

Sie erhalten diese E-Mail, da wir aufgrund des oben beschriebenen Vorfalls gemäß Art. 34 der Datenschutzgrundverordnung (DS-GVO) gesetzlich verpflichtet sind, Sie als betroffene Person über die Verletzung des Schutzes Ihrer personenbezogenen [Daten] zu informieren.

Nach jetzigem Stand gehen wir davon aus, dass bis auf einen Einzelfall die Nutzerdaten nicht dazu verwendet wurden, Zugang zum BSCW-System zu erlangen. Um unserer Informationspflicht nach Art. 34 Abs. 2 i.V.m. Art. 33 Abs. 3 lit. c nachzukommen, weise ich darauf hin, dass unter diesen Umständen nicht vollständig ausgeschlossen werden kann, dass Ihre hinterlegten Daten zum Beispiel zu Phishingzwecken oder für Werbezwecke verwendet werden.

Der unberechtigte Zugang wurde nach Bekanntwerden unverzüglich gesperrt.

Im Übrigen wird der Vorfall von uns auch in anonymer Form – also ohne Nennung Ihres Namens oder sonstiger personenbezogener Daten – gemäß Art. 33 DS-GVO der zuständigen Landesbeauftragten für Datenschutz und Informationsfreiheit (LDI NRW) als Datenschutzvorfall ordnungsgemäß gemeldet.

Derzeit führt nun eine externe IT-Sicherheitsfirma eine Prüfung durch und arbeitet mit uns die Gesamtereignisse auf. Wir bedauern den Vorfall sehr und entschuldigen uns dafür.

Wenn Sie zu dem oben beschriebenen Vorfall und den Ihnen insoweit zustehenden Datenschutzrechten Fragen haben, können Sie sich hierzu gerne auch an die Datenschutzbeauftragte unseres Hauses wenden, die Sie wie folgt erreichen:

gez. Datenschutzbeauftragte der QUA-LiS"

Wie viel Zeit ist zwischen der Entdeckung des Datenlecks und der Informationen nach Art. 33 und 34 DSGVO vergangen?

Wurden die gesetzlichen Vorgaben der unverzüglichen Information nach Art. 34 DSGVO bzw. die 72-Stunden-Frist in Art. 33 DSGVO eingehalten?

Gemäß Artikel 33 der DS-GVO muss bei Verletzungen des Schutzes von personenbezogenen Daten, die voraussichtlich mit einem Risiko für

die persönlichen Rechte und Freiheiten von natürlichen Personen einhergehen, der zuständigen Aufsichtsbehörde der Sachverhalt unverzüglich und möglichst binnen 72 Stunden, nachdem dem Verantwortlichen die Verletzung bekannt wurde, angezeigt werden. Bei einem hohen Risiko sind zudem gemäß Art. 34 DS-GVO die Betroffenen unverzüglich über diesen Sachverhalt zu informieren.

Die Risikobewertung ist dabei individuell durch den Verantwortlichen für die Datenverarbeitung durchzuführen und bemisst sich an der Schwere und der Eintrittswahrscheinlichkeit eines möglichen Schades. Wesentliche Faktoren, die ein höheres Risiko auslösen, sind insbesondere

- Daten die in Artikel 9 DS-GVO benannt werden (Daten aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person),
- Daten die in Artikel 10 DS-GVO benannt werden (Daten über strafrechtliche Verurteilungen und Straftaten),
- oder Daten, die einen qualitativ oder quantitativ hohen Datensatz umfassen, die eine Rückidentifizierung nicht nur von einzelnen, sondern größeren Personengruppen ermöglichen.

Am 20. April 2023 erfolgte nach einer Übermittlung einer Sicherheitsmeldung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) bzw. des Computer Emergency Response Team (CERT NRW) an die QUA-LiS, durch das Ministerium für Schule und Bildung die erstmalige Feststellung, dass Daten der QUA-LiS bis zu diesem Zeitpunkt auf dem BSCW-Server öffentlich einsehbar gewesen waren.

Das BSI kam zu der Bewertung, dass es sich bei der vorliegenden Meldung *„... um ein Moving target Rate, welches nur für eine begrenzte*

Zeit ausnutzbar war" handelte (vgl. auch Mündliche Anfrage des Abgeordneten Sebastian Watermeier – Drucksache 18/4216).

Die QUA-LiS ging zu diesem Zeitpunkt von einer möglichen Offenlegung von nur 500 Datensätzen aus. Dabei enthielten diese Datensätze bei der Registrierung zum einen verpflichtende Angaben zum Vor- und Nachnamen sowie eine (dienstliche oder private) E-Mail-Adresse.

Auf freiwilliger Basis war es möglich, weitere Angaben einzutragen:

- organisatorische Rolle im Schulsystem (z.B. „stellvertretende Leitung")
- Institutionszugehörigkeit (z.B. Name der Schule)
- Postalische Adresse
- dienstliche oder private Festnetz- oder Mobilfunknummer

Die Nutzerverwaltung wurde von der QUA-LiS für eine gemeinsame Arbeitsplattform (BSCW-Server) für den Austausch von und die gemeinsame Arbeit an Dokumenten genutzt, die einen nur geringen Schutzbedarf aufweisen. Das betrifft zum Beispiel die Arbeit an Lehrplänen oder den Bereich der Fortbildung.

Ein Zugriff auf die von den Nutzerinnen und Nutzern auf dem BSCW-Server gespeicherten Daten war mittels dieser offengelegten Datensätze in der Nutzerverwaltung grundsätzlich nicht möglich. Passwörter konnten nicht eingesehen werden. Es war jedoch nicht ausgeschlossen, dass in Einzelfällen durch die Übernahme einer verwaisten E-Mail-Domain ein neues Passwort generiert werden könne und mit diesen Daten eine Anmeldung möglich sei.

Das Risiko hinsichtlich einer Verletzung des Schutzes personenbezogener Daten für die Betroffenen wurde daher von der QUA-LiS als gering bewertet und mangels einer gesetzlichen datenschutzrechtlichen Verpflichtung von einer unverzüglichen Meldung an die Betroffenen und die LDI abgesehen, da es sich nicht um besonders geschützte personenbezogene Daten nach DS-GVO und nur um eine geringe Anzahl von Datensätzen handelt.

Am 25. April 2023 wurde in sozialen Medien kommentiert, dass eine deutlich größere Anzahl von Nutzerdaten für Dritte generierbar sei. Parallel ging jetzt auch die QUA-LiS davon aus, dass mehr als 500 Datensätze offengelegt werden konnten. Zu diesem Zeitpunkt ist dann seitens des Ministerium für Schule und Bildung entschieden worden, dass die QUA-LiS die betroffenen Nutzerinnen und Nutzer umfangreich informiert und eine Meldung an die LDI vorbereitet, um ein Höchstmaß an Transparenz und Sicherheit für die Betroffenen zu realisieren.

Am Dienstag, dem 25. April 2023, ist die LDI bereits mündlich vorab über den Sachverhalt informiert worden und ein schriftlicher Bericht der QUA-LiS angekündigt worden. Die Meldung der QUA-LiS erfolgte über das offizielle Online-Formular der LDI am Mittwoch, dem 26. April 2023. Da weiterhin die Bewertung des Risikos als gering angesehen wurde, konnte die Meldung auf dem Online-Weg der LDI nicht abgegeben werden.

Im Nachgang hat das Ministerium für Schule und Bildung dann die Meldung der QUA-LiS am Donnerstag, dem 27. April 2023, an die LDI per E-Mail verschickt und um Beratung hinsichtlich der vorgenommenen Risikobewertung gebeten. Wichtig ist, dass die LDI in diesen Vorgang vollumfänglich eingebunden ist.

Gleichzeitig hat die QUA-LiS auf Aufforderung durch das Ministerium für Schule und Bildung die Betroffenen rein vorsorglich über den aufgetretenen Verstoß informiert, auch wenn dazu gemäß Artikel 34 Abs. 1 DS-GVO mangels Feststellung eines hohen Risikos keine Verpflichtung bestand. Es wurden dabei am 27. April 2023 alle Nutzerinnen und Nutzer angeschrieben, die am 20. April 2023 in der Datenbank hinterlegt waren.

Die Darstellung zeigt, dass die Anforderungen der DS-GVO eingehalten worden sind. Die rechtliche Verpflichtung zur Information der Betroffenen bzw. zur Meldung an die LDI besteht in Abhängigkeit von der Bewertung des Risikograde für die Rechte und Freiheiten der Betroffenen.

Das Ministerium für Schule und Bildung geht zum gegenwärtigen Zeitpunkt weiterhin davon aus, dass die Bewertung mit einem geringen Risiko angemessen ist. Die datenschutzkonforme und transparente Information der Nutzerinnen und Nutzer durch die QUA-LiS am 27. April 2023 ist insofern als überobligatorisch anzusehen.

Eine Beratung seitens der LDI ist vom Ministerium für Schule und Bildung erbeten worden. Eine abschließende Bewertung steht noch aus.