Liebe Eltern und Erziehungsberechtigte,

hiermit informieren wir Sie gemäß Art.34 Datenschutz-Grundverordnung (DSGVO) über eine Verletzung des Schutzes personenbezogener Daten, bei der nach aktuellem Ermittlungsstand unbefugt Daten kopiert und im Darknet veröffentlicht wurden.

1. **Beschreibung des Vorfalls:**

Am 15.01.2025 verübte die Hackergruppe Lockbit einen Hackerangriff auf die IT-Systeme des IT-Dienstleisters Topackt IT Solutions GmbH, der das Schulnetzwerk „DSNX“ betreibt, das auch von unserer Schule genutzt wird. Wie jetzt bekannt wurde, sind Daten kopiert und im Darknet veröffentlicht worden.

2. **Betroffene Datenkategorien**

Nach aktuellem Kenntnisstand können folgende Daten betroffen sein:

- Namen, Anschriften und Geburtsdaten von Schüler*innen
- Namen und Anschriften von Erziehungsberechtigten
- Kontodaten aus Essensbestellungen
- Unterschriften
- E-Mail-Adressen und Telefonnummern von Schüler*innen und Erziehungsberechtigten
- Zeugnisse
- Dokumentation zu Fehlzeiten und Verspätungen
- Beurteilungen
- Schulinterne Vermerke; Interne aus Schulgremien
- Gesundheitsdaten, darunter auch sonderpädagogische Gutachten, Schwerbehindertenausweise, Ergebnisse schulärztlicher Untersuchungen
- Disziplinarische Maßnahmen
- Fotos und Videos

3. **Mögliche Risiken**

Durch den Vorfall besteht ein erhöhtes Risiko insbesondere für:

- Identitätsmissbrauch
- Phishing- und Betrugsversuche
- Unbefugte Kontaktaufnahme

- Social Engineering (zwischenmenschliche Beeinflussung mit dem Ziel, Personen zu Handlungen zu bewegen, um unberechtigt an Informationen oder in IT-Infrastrukturen zu gelangen. Angreifer nutzen Vertrauen, Hilfsbereitschaft, Angst oder Neugier aus, um Sicherheitsmaßnahmen zu umgehen)
- Erpressungsversuche

Wir weisen ausdrücklich darauf hin, dass ein Missbrauch nicht ausgeschlossen werden kann.

4. Bereits ergriffene Maßnahmen (Art. 33 DSGVO)

Bislang wurden folgende Maßnahmen umgesetzt:

- Isolierung und Sicherung der betroffenen Systeme
- Hinzuziehung externer IT-Forensik- und Sicherheitsexperten
- Meldung an die zuständige Datenschutzaufsichtsbehörde
- Einleitung zusätzlicher technischer und organisatorischer Schutzmaßnahmen
- Prüfung und ggf. Zurücksetzung von Zugangsdaten

5. Empfohlene Schutzmaßnahmen

Wir empfehlen Ihnen dringend:

- Besondere Vorsicht bei unerwarteten Nachrichten (E-Mail, Telefon, Social Media etc.). Prüfen Sie insbesondere E-Mails, bevor Sie darin enthaltene Links anklicken.
- Keine Weitergabe sensibler Daten ohne sichere Verifizierung
- Änderung von Passwörtern
- Erhöhte Aufmerksamkeit bei Konto- und Vertragsaktivitäten

Insgesamt ist höchste Aufmerksamkeit gegenüber ungewöhnlichen Mitteilungen, Phishing-Versuchen und Identitätsmissbrauch geboten. Öffnen Sie keine unbekannten Links oder Anhänge und antworten Sie nicht ungeprüft auf unaufgeforderte Schreiben.

6. Haben Sie Fragen?

Sollten Sie Fragen haben, stehen wir Ihnen selbstverständlich gerne zur Verfügung. Kontaktieren Sie uns gerne per E-Mail: Datenpanne@fmsg-speyer.de

Der Schulträger und unsere vorgesetzte Behörde arbeiten mit Nachdruck daran, die Hintergründe dieses Vorfalls vollständig aufzuklären und ihre Sicherheitsmaßnahmen nachhaltig zu stärken.

Mit besten Grüßen,
Lenelotte Möller