JuF KK
Jugend- und Freizeiteinrichtungen
Eigenbetrieb des Landkreises Kassel

Jugend- und Freizeiteinrichtungen - Eigenbetrieb des Landkreises Kassel
Parkstraße 12 · 34117 Kassel

Vorname Name
Straße
PLZ Ort

Parkstraße 12
34117 Kassel

Standort
Verwaltung Kassel

Telefon: 0561 / 99 79 79 – 90
(Buchungsstelle)
Fax: 0561 / 99 79 79 – 95
E-Mail: info@jufkk.de

Datum
06.05.2026

Informationsschreiben

Sehr geehrte(r) Frau/Herr NAME,

wir informieren Sie hiermit über einen Vorfall, bei dem es zu einer Verletzung des Schutzes Ihrer personenbezogenen Daten kam. Wir bedauern diesen Vorfall sehr und möchten Ihnen im Folgenden verständlich erläutern, welche Risiken bestehen und wie Sie sich bestmöglich schützen können.

1. **Was ist passiert?**

Wie bereits öffentlich bekannt gegeben, wurde unser IT-System im Februar 2026 Ziel eines Cyberangriffs. Dabei verschafften sich externe Angreifer unbefugten Zugriff auf unseren Verwaltungsserver. Ein Datenabfluss konnte zu diesem Zeitpunkt noch nicht nachgewiesen werden.

Am 19.04.2026 haben die Angreifer einen Teil dieser Daten im sogenannten Darknet (nicht öffentlich zugängliche Bereiche des Internets) veröffentlicht. Das bedeutet: Die Daten können potenziell von Dritten eingesehen, gespeichert und weiterverbreitet werden.

Mithilfe von externen Spezialisten war eine Analyse der veröffentlichten Daten möglich. Hieraus ergab sich, dass Ihre personenbezogenen Daten betroffen sind.

2. **Welche Daten sind betroffen?**

Nach aktuellem Stand **können** insbesondere folgende Arten von Daten zu Ihrer Person betroffen sein:

- Personenstammdaten: Name, Anschrift, Geburtsdatum
- Kontaktdaten: E-Mail-Adresse, Telefonnummer
- Finanzdaten: Bankverbindung/IBAN
- Daten aus der Personalverwaltung: Vertragsinhalte, Arbeitszeugnisse, Qualifikationen, Bewerbungsunterlagen, Schulungszertifikate, Dienstpläne, Abrechnungen Gehalt und Fahrtkosten, Krankmeldungen
- Sozialdaten: Förderpläne/Maßnahmenpläne
- Identifikationsdaten: Ausweiskopien

3. **Welche Risiken bestehen für Sie?**

Durch die Veröffentlichung dieser Daten besteht ein erhöhtes Risiko, dass Dritte die Informationen missbräuchlich verwenden. Die Veröffentlichung erfolgte im sogenannten Darknet. Dabei handelt es sich um einen nicht öffentlich zugänglichen Bereich des Internets, der nur über spezielle Zugangswege erreichbar ist. Das bedeutet, dass die Daten nicht ohne Weiteres für jedermann frei im Internet auffindbar sind.

Gleichzeitig ist jedoch davon auszugehen, dass insbesondere kriminelle Akteure gezielt solche Plattformen nutzen, um sich durch Missbrauch der Daten Vorteile zu verschaffen.

Je nachdem, welche Datenarten zu Ihrer Person veröffentlicht wurden, sind unter anderem folgende Szenarien möglich:

- **Unbefugte Kontaktaufnahme und Belästigung:**
  Ihre Kontaktdaten könnten für unerwünschte oder betrügerische Kontaktaufnahmen genutzt werden.
- **Identitätsmissbrauch:**
  Ihre Daten könnten genutzt werden, um sich unter Ihrem Namen auszugeben, z. B. beim Abschluss von Verträgen oder bei Online-Diensten.
- **Gezielte Betrugsversuche (Phishing / Social Engineering):**
  Angreifer könnten Sie gezielt kontaktieren (E-Mail, Telefon, SMS) und dabei bereits bekannte persönliche Informationen verwenden, um Vertrauen zu gewinnen und Sie zur Herausgabe weiterer Daten oder zu Zahlungen zu bewegen.
- **Missbrauch von Ausweisdaten:**
  Sollten Ausweiskopien betroffen sein, besteht ein erhöhtes Risiko für betrügerische Vertragsabschlüsse oder Kontoeröffnungen.
- **Persönliche Nachteile durch sensible Informationen:**
  Informationen zu Gesundheit und Beschäftigungsverhältnissen könnten im Einzelfall zu Diskriminierung, Rufschädigung oder persönlichen Belastungen führen.

Wichtig: Ein tatsächlicher Missbrauch muss nicht eintreten – das Risiko ist jedoch aufgrund der Veröffentlichung als erhöht einzustufen.

4. **Welche Maßnahmen haben wir ergriffen?**

Nach Bekanntwerden der Veröffentlichung der Daten wurden umgehend Maßnahmen eingeleitet:

- Einrichtung sicherer Analyseumgebungen für die betroffenen Daten
- Auswertung der betroffenen Daten in einem geschützten Bereich von einem begrenzten Personenkreis

Der Personalrat war von Beginn an involviert und stets über den Fortgang der Analyse und den Umgang mit den Daten informiert.

5. **Um mögliche Risiken zu reduzieren, empfehlen wir Ihnen folgende konkrete Maßnahmen:**

- **Besondere Vorsicht bei Kontaktaufnahmen:**
  Seien Sie aufmerksam bei E-Mails, Anrufen oder Nachrichten, in denen auf persönliche Daten Bezug genommen wird oder zur Herausgabe weiterer Informationen aufgefordert wird.
- **Keine Weitergabe sensibler Daten:**
  Geben Sie insbesondere keine Konto- oder Zugangsdaten weiter – auch dann nicht, wenn der Anschein erweckt wird, die Anfrage sei berechtigt.
- **Konten und Unterlagen im Blick behalten:**
  Prüfen Sie regelmäßig Kontoauszüge, Verträge oder andere relevante Unterlagen auf Auffälligkeiten.
- **Ausweisdokumente:**
  Sofern Sie vermuten, dass eine Kopie Ihres Ausweises betroffen ist, kann eine Beratung bei der zuständigen Ausweisbehörde sinnvoll sein. Da es sich um reine Kopien handeln würde, ist die eID-Funktion nicht betroffen: Für die Online-Ausweisfunktion ist die Ausweiskarte und die sechsstellige PIN erforderlich.
- **Bei konkretem Missbrauch handeln:**
  Sollten Sie Anzeichen für einen Identitätsbetrug feststellen (z. B. unbekannte Verträge, ungewöhnliche Abbuchungen), wenden Sie sich bitte umgehend an Ihre Bank und erstatten Sie ggf. Anzeige gegen die Täter (gegen unbekannt). Weiterhin können Sie den Identitätsbetrug bei der SCHUFA melden, mehr dazu finden Sie auf deren Website. Erhalten Sie Schreiben zu angeblichen Verträgen, können Sie umgehend Widerspruch einlegen und wenn vorhanden, die Strafanzeige zum Identitätsbetrug beifügen.

6. **Weitere Informationen und Kontakt**

Sollten Sie über dieses Informationsschreiben hinaus individuelle Anliegen oder konkrete Nachfragen haben, richten Sie bitte Ihre Nachricht an sicherheitsvorfall@kreiskassel.de.

Wünschen Sie ein Gespräch mit der externen Datenschutzbeauftragten, können Sie sich an folgende Stelle wenden:

Kontakt Externe Datenschutzbeauftragte:
Datenschutzberatung Moers GmbH, Anne Borell
E-Mail: kreis-kassel@dsb-moers.de
Telefon: 05671 74925-29

Wir bedauern diesen Vorfall sehr und nehmen den Schutz Ihrer Daten äußerst ernst. Wir arbeiten mit Hochdruck daran, die Wiederholung einer solchen Situation für die Zukunft auszuschließen und weitere Risiken zu minimieren.

mit freundlichen Grüßen

Uwe Pietsch
Betriebsleitung