Wichtige Information nach Art. 34 DSGVO auf Grund eines Cyberangriffs

Als Verband medizinischer Fachberufe e.V. möchten wir Sie transparent und umfassend über einen aktuell eingetretenen Vorfall informieren, bei dem personenbezogene Daten durch einen Phishing-Angriff kompromittiert wurden. Unser Anliegen ist es, unseren gesetzlichen Verpflichtungen und unserer Verantwortung gegenüber unseren Verbandsmitgliedern, Beschäftigten und Geschäftspartnern nachzukommen, Sie bei der Sicherung Ihrer Daten zu unterstützen und größtmögliche Transparenz zu gewährleisten.

Beschreibung des Vorfalls

Am 10.07.2025 wurde uns mitgeteilt, dass es zum unbefugten Zugriff auf E-Mail-Konten innerhalb unserer Organisation gekommen ist. Nach derzeitigem Stand verschafften sich Angreifer durch einen Phishing-Angriff Zugang zu mindestens drei E-Mail-Accounts und konnten auf darin enthaltene personenbezogene Daten und E-Mail-Kontakte zugreifen. Einer der kompromittierten Accounts wurde für den Versand weiterer Phishing-Mails verwendet. Nicht auszuschließen ist, dass zudem Inhalte aus dem betroffenen E-Mail-Postfach abgeflossen sind. Da es hierfür erstmals jedoch keine weiterführenden Hinweise gab, dass dies erfolgt ist, wurde das Risiko für die Rechte und Freiheiten der Betroffenen im Rahmen der Risikoanalyse zuerst als moderat eingeschätzt, weshalb wir in erster Linie die unmittelbar von dem Vorfall betroffenen Personen hierüber informiert haben. Ein bekanntgewordener Vorfall (Betrugsversuch unter Verwendung einer Unterschrift der betroffenen Beschäftigten) am 18.07.2025 stellt jedoch nun mehr auch ein Indiz für einen Abfluss von weiteren Daten aus diesen betroffenen E-Mail-Postfächern dar, weshalb im Rahmen der Risikoanalyse nun mehr ein hohes Risiko von uns angenommen wird.

Welche Daten sind betroffen?

Die folgende Übersicht informiert, welche Datenkategorien möglicherweise kompromittiert wurden:

- **E-Mail-Adressen** (Verbandsmitglieder, Beschäftigte, Geschäftspartner)
- **Namen und ggf. Kontaktinformationen** (sofern im E-Mail-Verkehr enthalten)
- **Inhalte der E-Mail-Kommunikation** (z.B. Korrespondenzen, Anhänge)

- **Besondere Kategorien personenbezogener Daten:** Nach aktueller Erkenntnislage sind wahrscheinlich auch Daten zur Gewerkschaftszugehörigkeit sowie möglicherweise politische Meinungen und weitere besonders schützenswerte Informationen gemäß Art. 9 DSGVO betroffen.

Mögliche Risiken für Sie

Wir haben eine Risikoanalyse durchgeführt und bewerten das Risiko, wie bereits vorab dargestellt, als hoch. Betroffene könnten durch die in den E-Mai-Postfächern enthaltenen Daten insbesondere mit folgenden Risiken konfrontiert werden:

- Identitätsdiebstahl und Phishingversuche durch Folgeangriffe
- Betrugs- und Täuschungsversuche, z.B. mit gefälschten E-Mails im Namen des Verbands oder weiterer nahestehender Stellen
- Kontrollverlust über eigene personenbezogene Daten im Internet (z.B. durch Verbreitung im Darknet)
- Im Einzelfall Einblick in besonders schützenswerte Informationen, z.B. Gewerkschaftszugehörigkeit oder politische Einstellungen
- Finanzielle Schäden oder Rufschädigung durch Datenmissbrauch

Welche Maßnahmen wurden von uns bereits getroffen?

- Umgehende Sperrung und Zurücksetzung der betroffenen Zugänge und Passwörter
- Vollumfängliche Löschung und Neueinrichtung betroffener Accounts
- Direkte Einbindung unserer IT-Sicherheitsdienstleister und Datenschutzbeauftragten
- Durchführung umfassender Sicherheitsaudits und Virenscans (keine fortbestehende Schadsoftware festgestellt)
- Kontrolle weiterer Accounts und Schutzmaßnahmen durch den IT-Dienstleister
- Proaktive Information unmittelbar betroffener Kontaktpersonen

- Laufende Planung und schneller Ausbau technischer Maßnahmen, insbesondere Einführung der Multi-Faktor-Authentifizierung

Was empfehlen wir Ihnen?

Bitte beachten Sie folgende Schutzempfehlungen und Hinweise, um Ihre eigenen Daten und Zugänge zu schützen:

- Seien Sie besonders wachsam gegenüber verdächtigen E-Mails, die Sie zum Anklicken von Links oder zum Öffnen von Anhängen auffordern (Phishing).
- Überwachen Sie ungewöhnliche Aktivitäten in Ihren Konten (z.B. Passwortänderungen, neue Login-Versuche) und dokumentieren Sie solche Ereignisse.
- Ziehen Sie im Zweifel den IT-Support oder externe Experten (z.B. Ihre Bank bei betrugsverdächtigen Aktivitäten) hinzu.
- Im Falle eines finanziellen Schadens empfehlen wir die zeitnahe Anzeige bei den zuständigen Behörden sowie eine Meldung bei Ihrem Geldinstitut

Ihre Rechte

Betroffene Personen haben verschiedene Rechte nach der DSGVO, insbesondere:

- **Auskunftsrecht:** Sie können Auskunft darüber verlangen, ob und welche Ihrer personenbezogenen Daten betroffen sind.
- **Recht auf Berichtigung oder Löschung:** Sie haben das Recht auf Berichtigung unrichtiger oder Löschung unrechtmäßig verarbeiteter Daten, soweit keine gesetzlichen Aufbewahrungspflichten entgegenstehen.
- **Recht auf Einschränkung der Verarbeitung**
- **Recht auf Widerspruch:** Sie können der weiteren Verarbeitung Ihrer Daten begründet widersprechen.

Setzen Sie sich hierzu jederzeit mit uns oder unserem Datenschutzbeauftragten in Verbindung (s.u.).

Kontaktmöglichkeiten und weitere Informationen

Für Rückfragen, Beschwerden oder bei Hinweisen stehen wir Ihnen unter folgenden Kontaktdaten zur Verfügung:

Verband medizinischer Fachberufe e.V.
Ansprechperson: Stephanie Schreiber

(Geschäftsführender Vorstand,1. Vorsitzende)

Gesundheitscampus-Süd 33
44801 Bochum

Tel.: (0234) 777 28-0
Mail: datenschutz@vmf-online.de

Datenschutzbeauftragter: Erik Hallmann, LL.M.

Biehn & Professionals GmbH
Wiesenstraße 32
33397 Rietberg-Mastholte

Tel.: (0294) 97971-0
Mail: datenschutz@biehn-und-professionals.de

Sie können sich auch an die zuständige Aufsichtsbehörde wenden, z.B. die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen.

Wir entschuldigen uns ausdrücklich für die möglichen Unannehmlichkeiten. Die Sicherheit Ihrer Daten hat für uns höchste Priorität. Wir setzen alles daran, derartige Vorfälle künftig zu vermeiden und haben bereits weitergehende technische wie organisatorische Schutzmaßnahmen initiiert.

Sollten sich zukünftig neue Informationen ergeben, die für Sie von Relevanz sind, werden wir dieses Informationsschreiben entsprechend aktualisieren.

Diese Information ist Teil unserer Melde- und Transparenzpflicht gemäß Art. 34 DSGVO und dient Ihrem Schutz.