Wichtige Sicherheitshinweise für Betroffene im Umgang mit der Veröffentlichung von sensiblen personenbezogenen Daten

Berlin, 02.11.2026

Sehr geehrte Betroffene, sehr geehrte Damen und Herren,

wir bedauern außerordentlich, dass es zu der Veröffentlichung von personenbezogenen Daten gekommen ist. Uns ist bewusst, dass ein solcher Vorfall für die Betroffenen mit erheblicher Verunsicherung und Sorgen verbunden sein kann. Insbesondere die Möglichkeit, dass veröffentlichte Informationen für Betrugsversuche, Identitätsmissbrauch oder unerwünschte Kontaktaufnahmen missbraucht werden könnten, kann das Gefühl der persönlichen Sicherheit beeinträchtigen.

Die von diesem Vorfall betroffenen personenbezogenen Daten wurden im Zusammenhang mit schwerwiegenden rechtswidrigen Angriffen auf die Internetseiten unserer Partei sowie auf Systeme von uns beauftragter Dienstleister erlangt und anschließend unter anderem auf der Internetseite „hexane.cc“ veröffentlicht. Uns ist bewusst, dass die hieraus entstehenden Risiken und Unannehmlichkeiten für die Betroffenen eine zusätzliche Belastung darstellen können.

Um Sie bei der Einschätzung möglicher Risiken zu unterstützen und Ihnen Hilfestellungen für den Umgang mit möglichen Folgeerscheinungen des Vorfalls zu geben, stellen wir Ihnen nachfolgend Sicherheitshinweise und Handlungsempfehlungen zur Verfügung. Diese orientieren sich unter anderem an Veröffentlichungen und Empfehlungen zuständiger Behörden und Fachstellen, insbesondere des Bundesamts für Sicherheit in der Informationstechnik (BSI), der Polizei sowie weiterer Einrichtungen der Cybercrime-Prävention.

Die nachfolgenden Hinweise sollen Ihnen dabei helfen, mögliche Betrugsversuche frühzeitig zu erkennen, Ihre persönlichen Daten bestmöglich zu schützen und angemessen auf verdächtige Kontaktaufnahmen oder Auffälligkeiten zu reagieren.

Für die mit diesem Vorfall verbundenen Unannehmlichkeiten und Belastungen sprechen wir Ihnen unser ausdrückliches Bedauern aus.

Ihr Bundesverband der Partei Alternative für Deutschland

Warnhinweise

Aufgrund der veröffentlichten personenbezogenen Daten ist mit vermehrten Betrugsversuchen per Telefon, SMS, Messenger und E-Mail zu rechnen. Geben Sie keine Passwörter, TANs, Sicherheitscodes oder Ausweisdaten weiter.

Prüfen Sie jede Kontaktaufnahme kritisch. Ändern Sie wichtige Passwörter, aktivieren Sie die Zwei-Faktor-Authentifizierung und dokumentieren Sie verdächtige Vorfälle. Bei Identitätsmissbrauch oder Betrugsversuchen sollte unverzüglich Anzeige erstattet werden. Die Empfehlungen entsprechen den Handlungshinweisen des BSI und der polizeilichen Cybercrime-Prävention.

➔ „Identitätsdiebstahl: Checkliste des BSI für den Ernstfall“

Empfehlung für Betroffene nach unbefugter Veröffentlichung personenbezogener Daten

1. **Keine Anrufe, Nachrichten oder E-Mails ungeprüft beantworten**
   - Betrüger nutzen veröffentlichte Daten häufig für gezielte Betrugsversuche (Social Engineering).
   - Niemals Passwörter, Einmalcodes (TANs), Sicherheits-PINs oder Ausweisdaten per Telefon, Messenger oder E-Mail weitergeben. Das BSI warnt ausdrücklich vor solchen Phishing-Methoden. → [bsi.bund.de] + [bsi.bund.de]
2. **Passwörter sofort ändern**
   - Besonders bei E-Mail-Konten, sozialen Netzwerken, Cloud-Diensten und Online-Shops.
   - Wenn dasselbe Passwort mehrfach verwendet wurde, müssen alle betroffenen Konten geändert werden. → [bsi.bund.de] + [bsi.bund.de]
3. **Zwei-Faktor-Authentifizierung (2FA) aktivieren**
   - Für E-Mail, Messenger, soziale Netzwerke und Finanzdienste die „2FA" verwenden.
   - Das BSI empfiehlt dies ausdrücklich als Schutz vor Kontoübernahmen. → [bsi.bund.de] + [bsi.bund.de]
4. **Konten auf fremde Zugriffe prüfen**
   - Hinterlegte Telefonnummern, E-Mail-Adressen, verbundene Geräte und aktive Sitzungen kontrollieren.
   - Unbekannte Zugriffe entfernen und alle Sitzungen abmelden. → [bsi.bund.de]
5. **Finanzkonten überwachen**
   - Kontoauszüge, Kreditkartenabrechnungen und Online-Banking regelmäßig prüfen.
   - Unbekannte Buchungen sofort der Bank melden.
6. **Beweise sichern**
   - Screenshots von Veröffentlichungen, Betrugsnachrichten, Anrufen, E-Mails und Social-Media-Profilen anfertigen.
   - URLs, Zeitpunkte und Benutzernamen dokumentieren.
   - Diese Informationen können für Strafanzeigen und Datenschutzverfahren wichtig sein.
7. **Anzeige erstatten**
   - Bei Identitätsmissbrauch, Betrug, Erpressung, Doxing oder Kontoübernahmen sollte Strafanzeige bei der Polizei bzw. der Onlinewache gestellt werden. Das BSI verweist Betroffene ausdrücklich auf die Onlinewachen der Polizei. → [bsi.bund.de] + [bsi.bund.de]
8. **Prüfen, welche Daten veröffentlicht worden sind**

   Der Bundesverband der Partei Alternative für Deutschland hat eine Auswertung der veröffentlichten Daten vorgenommen und bereits eine erhebliche Anzahl identifizierte Betroffene benachrichtigt, weitere Analysen erfolgen. Anfragen können Sie stellen an dsgvo-auskunft@afd.de
   - Je nach Art der Daten können zusätzliche Maßnahmen nötig sein:
     - Ausweisdaten: Behörden informieren.
     - Bankdaten: Bank kontaktieren.
     - Zugangsdaten: Konten absichern.
9. **Kontakte warnen**
   - Falls E-Mail-, Messenger- oder Social-Media-Konten betroffen sind, sollten Freunde, Familie und Geschäftspartner informiert werden.
   - Täter nutzen oft kompromittierte Konten oder veröffentlichte Daten, um weitere Personen zu täuschen. → [bsi.bund.de] + [bsi.bund.de]