

**Johannes Rauch**  
Bundesminister

Herrn  
Mag. Wolfgang Sobotka  
Präsident des Nationalrates  
Parlament  
1017 Wien

Geschäftszahl: 2022-0.318.344

Wien, 24.6.2022

Sehr geehrter Herr Präsident!

Ich beantworte die an mich gerichtete schriftliche parlamentarische **Anfrage Nr. 10813/J der Abgeordneten Mag. Christian Ragger und weiterer Abgeordneter betreffend Ex-PVA-Manager: Drei Jahre Haft** wie folgt:

Vorauszuschicken ist, dass sich die vorliegende parlamentarische Anfrage auf Angelegenheiten des Vollzugs durch die Sozialversicherungsträger im Rahmen ihrer Selbstverwaltung bezieht. Ungeachtet der Tatsache, dass diese an sich nicht Gegenstand des Interpellationsrechts nach Art. 52 B-VG sind, habe ich hierzu eine koordinierte Stellungnahme des Dachverbandes eingeholt, der dazu die einzelnen Sozialversicherungsträger befragt hat. Diese Stellungnahme habe ich der Beantwortung zu Grunde gelegt.

**Frage 1:**

- *Wurde von der PVA die genaue Schadenssumme ermittelt?*

Ja, die genaue Schadenssumme wurde ermittelt.

**Frage 2:**

- *Wenn ja, wie hoch ist diese?*

Der Gesamtschaden beläuft sich nach Auskunft der PVA auf EUR 1.403.164,91.

**Frage 3:**

- *Wie viel wurde von diesem Betrag bereits zurückgezahlt?*

Bis dato konnte die PVA noch keinen Zahlungseingang verzeichnen.

**Fragen 4 und 22:**

- *Welche Zahlungen sind zur Wiedergutmachung noch zu erwarten?*
- *Wie soll der fehlende Geldbetrag zurückgezahlt werden?*

Im Rahmen des strafrechtlichen Ermittlungsverfahrens wurde nach Auskunft der PVA ein Betrag von EUR 602.427,41 sichergestellt. Infolge der rechtskräftigen Verurteilung und Zuerkennung der gesamten Schadenssumme kann mit der Ausfolgung dieses Betrages gerechnet werden.

Es ist ferner damit zu rechnen, dass der PVA an weiteren Vermögenswerten EUR 186.066,98 zur Schadenswiedergutmachung zukommen. Hinsichtlich des verbleibenden Schadensbetrages verfügt die PVA über einen rechtskräftigen Exekutionstitel.

**Fragen 5 und 14:**

- *Wie konnte dieser Fall jahrelang unentdeckt bleiben?*
- *Wie ist dieser Betrug genau vonstattengegangen?*

Durch Aufwendung erheblicher krimineller Energie wurden das Vier-Augen-Prinzip, technische Kontrollfunktionen sowie systemgenerierte Erhebungsaktionen umgangen.

**Frage 6:**

- *Woher hatte der Mann die im Artikel genannten Log-in-Daten anderer Mitarbeiter?*

Die Erhebungen haben nach Auskunft der PVA ergeben, dass der Verurteilte die Passwörter ausgespäht bzw. erschlichen hat.

**Frage 7:**

- *Besteht in diesem Zusammenhang ein Sicherheitsproblem bei der PVA und / oder anderen Versicherungen?*

Die PVA verweist hier auf ihre Ausführungen zu Frage 5: durch Aufwendung erheblicher krimineller Energie des mittlerweile Verurteilten wurden das Vier-Augen-Prinzip, technische Kontrollfunktionen sowie systemgenerierte Erhebungsaktionen umgangen. Aufgrund des besonders betrügerischen Datenverarbeitungsmissbrauchs besteht aus Sicht der PVA kein Sicherheitsproblem.

Einige der wesentlichsten Kontrollinstrumente der PVA stellen sich wie folgt dar:

- Datenschutzdienstweisung und die Passwortrichtlinie stellen klar, dass Passwörter geheim zu halten sind und Eingaben stets unbeobachtet zu erfolgen haben. Den Bediensteten wurden und werden diese Regelungen und die Verpflichtung zu ihrer Einhaltung und zur regelmäßigen Änderung der Passwörter wiederholt in Erinnerung gerufen. Datenschutz und Datensicherheit sind ein wesentlicher Bestandteil der laufenden Schulungen der Mitarbeiter:innen der PVA.
- In Form von Stichprobenprüfungen wird regelmäßig mit einer entsprechenden Applikation erhoben, ob für die Zugriffe auf Akten ein dienstlicher Zusammenhang besteht. Dabei ist der Grund für die getätigte Datenabfrage vom bzw. von der Mitarbeiter:in anzugeben. Die jeweilige Abteilungsleitung hat das Vorliegen eines dienstlichen Zusammenhangs zu kontrollieren und eine entsprechende Dokumentation vorzunehmen. Ab diesem Jahr fällt das Monitoring dieser Rückmeldungen zusätzlich in den Aufgabenbereich von neu geschaffenen Qualitätssicherungsbeauftragten in den Landesstellen. Seit Jänner 2021 liegen der Datenschutzstichprobenprüfung sämtliche Protokolldatensätze (ITSV- und PVA-Applikationen) zugrunde. Damit sind im Gegensatz zur früheren Stichprobenprüfung nunmehr neben den ITSV-Applikationen auch die PVA-Applikationen von der Prüfung umfasst.
- In bestimmten Sachgebieten (zB Ausgleichszulage, Jahresausgleich, Lohnsteuer) werden automatisiert Datenlisten erzeugt und diese in Folge bearbeitet.

- Die PVA bedient sich seit Jahren eines externen Dienstleisters für den zentralen Druck und die Abfertigung ihrer Schreiben, weshalb eine Versendung von systemgesteuerten Schriftstücken nur mit erheblicher krimineller Energie unterbunden werden kann. Insbesondere würden an fiktive Personen versandte Schriftstücke bei ihrem Rücklangen mit hoher Wahrscheinlichkeit auffallen und weitere Nachforschungen auslösen.

Zur Beantwortung der Frage im Hinblick auf die anderen Sozialversicherungsträger verweise ich auf die Beantwortung der Fragen 26, 27, 28 und 29.

**Fragen 8, 9, 10, 11 und 12:**

- *Inwiefern sind die entsprechenden Kollegen für diesen Missbrauch verantwortlich?*
- *Können Sie ausschließen, dass die entsprechenden Kollegen von den illegalen Machenschaften, die mit ihren Log-in-Daten betrieben wurden, etwas gewusst hätten?*
- *Wenn nein, warum nicht?*
- *Können Sie ausschließen, dass die entsprechenden Kollegen von den illegalen Machenschaften finanziell profitiert haben?*
- *Wenn nein, warum nicht?*

Weder interne Überprüfungen noch Ermittlungen der Staatsanwaltschaft ergaben Hinweise auf eine Mitwirkung von Kolleginnen bzw. Kollegen.

**Frage 13:**

- *Warum ist es so einfach, SV-Nummern und Personen zu erfinden?*

Die Anlage der fiktiven Leistungsbezieher:innen im hier relevanten Fall liegt Jahre zurück. Heute steht die gesamte Architektur zur Anlage von Versicherungsnummern in einem engen Zusammenhang mit dem Dachverband der Sozialversicherungsträger, den angebotenen Versicherungsträgern und der IT-Services der Sozialversicherung GmbH (ITSV GmbH). Seit der Anbindung sämtlicher Systeme der PVA an die Zentrale Partnerverwaltung (ZPV), das Zentrale Personenstandsregister (ZPR) und das Zentrale Melderegister (ZMR) ist die Anlage eines bzw. einer fiktiven Leistungsbezieher:in de facto ausgeschlossen.

**Frage 15:**

- *Welche Sicherheitsvorkehrungen gibt es in diesem Zusammenhang, die etwas dem Entsprechendes zu verhindern?*

Zur Verhinderung von Manipulationen im Leistungswesen der PVA sind zahlreiche Kontrollmechanismen – insbesondere erfolgen Ein- und Freigaben grundsätzlich nach dem Vier-Augen-Prinzip – eingerichtet, welche regelmäßig evaluiert und angepasst werden. Auch das Anlegen von Versicherungsnummern steht heute in einem engen Zusammenhang mit dem Dachverband und den angebotenen Versicherungsträgern, sodass eine wie hier angesprochene Manipulation durch Anlage fiktiver Leistungsbezieher:innen de facto auszuschließen ist.

**Frage 16:**

- *Welche Konsequenzen hat dieser Fall innerhalb der PVA?*

Die Datenschutzdienstweisung und die Passwortrichtlinie stellen klar, dass Passwörter geheim zu halten sind und Eingaben stets unbeobachtet zu erfolgen haben. Den Bediensteten wurden und werden diese Regelungen und die Verpflichtung zu ihrer Einhaltung wiederholt in Erinnerung gerufen.

Unmittelbar nach Bekanntwerden der Malversation wurde erneut darauf hingewiesen, dass der Einstieg mit einer fremden BenutzerID und somit auch die Weitergabe der Kennwörter an andere Personen ausdrücklich untersagt ist, Zugangsdaten nicht notiert werden dürfen und streng geheim gehalten werden müssen.

Zusätzlich ist technisch sichergestellt, dass eine regelmäßige Änderung des Passwortes erfolgen muss; widrigenfalls ist kein Datenzugriff möglich. Weiters wurden die Sicherheitspolicies bezüglich der Korrelation zwischen technischer UserID und zugeordneter/m menschlichen Benutzer:in deutlich verschärft.

Datenschutz und Datensicherheit sind ein wesentlicher Bestandteil der laufenden Schulungen der Mitarbeiter:innen der PVA. In diesem Zusammenhang wurde beschlossen, zur Bewusstseinsbildung aller PVA-Mitarbeiter:innen eLearning-Module zu Informationssicherheitsthemen (Umgang mit Passwörtern, Phishing-eMails, etc.) über eine Learning-Management-Plattform zur Verfügung zu stellen. Diese Inhalte sind für alle

Mitarbeiter:innen als verpflichtende Schulung vorgesehen. Dies kann über die Learning-Management-Plattform automatisiert sichergestellt und dokumentiert werden.

Die Abteilung Interne Revision wurde beauftragt, zwei zusätzliche Prüfungen durchzuführen, in denen auf den angewandten Tatmustern aufbauend bundesweit Fälle ausgewählt wurden, um zu überprüfen, ob ähnlich gelagerte Fälle festgestellt werden konnten. Diese Überprüfungen haben keine ähnlich gelagerten Fälle ergeben.

Ferner wurde die Abteilung Interne Revision beauftragt, regelmäßige Stichprobenprüfungen durchzuführen, bei der Anwesenheitszeiten der Mitarbeiter:innen mit den Eingabezeiten der jeweiligen Usercodes abgeglichen werden.

**Frage 17:**

- *Wird eine weitere Klärung innerhalb der PVA angestrebt, wohin der Fehlbetrag verschwunden ist?*

Die Nachforschungen hinsichtlich des Verbleibs der durch die Straftat lukrierten Vermögenswerte erfolgten im Rahmen des Strafverfahrens durch die dafür zuständigen Strafverfolgungsbehörden.

**Frage 18:**

- *Gibt es hierzu schon neue Erkenntnisse?*

Diese Frage wäre unter Hinweis auf die Beantwortung zu Frage 17 allenfalls durch die Bundesministerin für Justiz zu beantworten.

**Fragen 19 und 20:**

- *Kann die PVA in dem vorliegenden Fall ausschließen, dass es weitere Mitwisser gibt?*
- *Wenn nein, warum nicht?*

Es haben sich keine Anhaltspunkte für eine Mitwissenschaft weiterer Personen ergeben.

**Frage 21:**

- *Haben andere von diesem Betrug profitiert?*

Ja, die Eltern und das Kind des Mannes.

**Frage 23:**

- *Aus welchem parteipolitischen Umfeld kommt der Mann?*

Diese Frage kann nicht beantwortet werden.

**Fragen 24 und 25:**

- *Welche ähnlichen Rechtsfälle gab es bei dieser und anderen Versicherungen in der Vergangenheit?*
- *Welche Strafen hatten hierbei die Verurteilung zur Folge?*

Bei der Pensionsversicherungsanstalt (PVA) gab es während der letzten Jahre einen weiteren Fall, in welchem ein Mitarbeiter wegen betrügerischen Datenverarbeitungsmissbrauchs verurteilt worden ist. Der Täter wurde zu einer Freiheitsstrafe von drei Jahren, davon ein Jahr unbeding, verurteilt.

Bei der Österreichischen Gesundheitskasse (ÖGK) gab es im Bereich Kostenerstattung der Wahlarzthilfe in den letzten Jahren vereinzelt Fälle von Malversationen in der Höhe bis maximal 15.000 Euro. Dabei wurden Kontodaten manipuliert und Gelder rechtswidrig auf die eigene Geldadresse bzw. jene der Angehörigen ausbezahlt. Die Frage hinsichtlich der Strafen kann mangels Erfassung der entsprechenden Daten nicht beantwortet werden.

Bei der Sozialversicherungsanstalt der Selbständigen (SVS) sind im Vorgängerträger Sozialversicherungsanstalt der gewerblichen Wirtschaft (SVA) in den Jahren 2001 und 2011 Fälle von dolosen Handlungen im Bereich Gesundheitsservice vorgekommen. In beiden Fällen gab es gerichtliche Verurteilungen.

Bei der Versicherungsanstalt öffentlich Bediensteter, Eisenbahnen und Bergbau (BVAEB) liegen keine vergleichbaren Fälle vor.

In der Allgemeinen Unfallversicherungsanstalt (AUVA) sind keine derartigen Rechtsfälle (bzw. etwaige daraus resultierenden Strafen und/oder dienst- bzw. arbeitsrechtlichen Konsequenzen) bekannt.

**Fragen 26, 27, 28 und 29:**

- *Wird bei Versicherungen aktuell geprüft, ob es zu ähnlichen Betrugs- und Missbrauchsfällen kommt oder gekommen ist?*
- *Wenn ja, ist dieser Fall für weitere Prüfungen ausschlaggebend gewesen?*
- *Wenn ja, welche Versicherungen werden überprüft?*
- *Wie oft werden in diesem Zusammenhang Versicherungen routinemäßig geprüft?*

Die ÖGK führt dazu aus, dass – neben der Klärung von Anlassfällen – Sachverhalte mit Malversationsverdacht für eine risikoorientierte systemische Prüfung des Prozessablaufs und für die Prüfung der Wirksamkeit des internen Kontrollsystems stets prioritär sind. Derartigen Verdachtsmomenten wird stets nachgegangen und bei Feststellung von Malversationen werden die erforderlichen arbeits- und disziplinarrechtlichen Schritte gesetzt.

Der Jahresprüfplan der Internen Revision (IR) wird risikoorientiert erstellt; die Malversationsgefahr ist für die Auswahl des Prüfthemas ein Kriterium. Im Anlassfall (Dienstpflichtverletzung, Malversationsverdacht) wird die IR einbezogen und gegebenenfalls mit einer Sonderprüfung beauftragt.

Darüber hinaus erfolgt anhand von Stichproben eine laufende Prüfung personenbezogener Zugriffe. Geprüft wird dabei der dienstliche Zusammenhang des Datenzugriffs zur Minimierung des Datenschutzrisikos bzw. der missbräuchlichen Verwendung von Zugriffsberechtigungen (aufdeckende und präventive Wirkung).

In allen Bereichen, wo Geldanweisungen durchgeführt werden, spielt das interne Kontrollsystem eine wichtige Rolle. Durch Risikoanalysen in den Geschäftsprozessen werden Kontrollmaßnahmen festgelegt, die in einer Risiko-Kontroll-Matrix dokumentiert sind. Zudem wird insbesondere bei Zahlungs- oder Anweisungsfreigaben bzw. bei wesentlichen Vorgängen ein 4-Augen-Prinzip angewendet, z.B. gemäß der Dienstanweisung „Mindeststandards Internes Kontrollsystem“, die für alle organisatorischen Bereiche der ÖGK verbindlich ist.

Die SVS führt derzeit interne Prüfungen zu den Themen „Fraud Detection und Protection in der SVS“ und „Zugriffskontrolle“ durch, nicht zuletzt auch auf Grund des Betrugsfalls in der PVA. Diese sollen dazu dienen, bestehende Maßnahmen in diesen Bereichen zu optimieren.

Laufende Kontrollen werden zudem durch die jeweilige Führungskraft und auch die interne Revision geführt.

Seitens der BVAEB ergeht diesbezüglich keine Stellungnahme, da keine vergleichbaren Fälle vorliegen.

In der AUVA erfolgt die Fallbearbeitung nach Arbeitsunfällen und Berufskrankheiten seit Jänner 2010 in dem gemeinsam mit der (nunmehrigen) BVAEB und der (nunmehrigen) SVS entwickelten Standardprodukt EFEU (Elektronische Feststellung und Erledigung in der Unfallversicherung). Eine Anlage von „fiktiven“ Personen ist in EFEU nicht möglich. Die Neuanlage einer Person erfolgt ausschließlich aus der Zentralen Partnerverwaltung des Dachverbandes (Standardprodukt: ZPV) durch Übernahme einer dort bereits vorhandenen Person (mit Sozialversicherungsnummer). Darüber hinaus gibt es je nach Art des Geschäftsfalls ein Vier- bzw. Sechs-Augen-Prinzip der Kontrolle in jedem einzelnen Fall.

**Frage 30:**

- *Welchen Beitrag leistet in diesem Zusammenhang Ihr Ministerium, um weitere Betrugs- und Missbrauchsfälle aufzudecken?*

Die Versicherungsträger unterliegen der Aufsicht des Bundes, die von mir bzw. meinem Ressort auszuüben ist. Diese staatliche Aufsicht greift in das den Selbstverwaltungskörpern verfassungsgesetzlich (Art. 120b Abs. 1 B-VG) gewährleistete Recht ein, ihre Aufgaben eigenverantwortlich zu besorgen, und ist daher nur innerhalb der verfassungsrechtlichen Schranken zulässig.

Vorliegend sind keine Anhaltspunkte bekannt, dass weitere derartige Betrugs- und Missbrauchsfälle bei den Sozialversicherungsträgern vorgefallen sind, weshalb es mir bzw. meinem Ressort auf Grund des verfassungsrechtlich garantierten Rechts auf Selbstverwaltung der Sozialversicherungsträger nicht zukommt, weitergehende Nachforschungen anzustellen.

Mit freundlichen Grüßen

Johannes Rauch



