17711/AB
vom 04.06.2024 zu 18295/J (XXVII. GP)

Bundeskanzleramt

bundeskanzleramt.gv.at

Karl Nehammer
Bundeskanzler

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: 2024-0.263.266

Wien, am 4. Juni 2024

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Dr. Krisper, Kolleginnen und Kollegen haben am 4. April 2024 unter der Nr. **18295/J** eine schriftliche parlamentarische Anfrage betreffend „Folgeanfrage: Warum befinden sich ‚Staatsgeheimnisse' in den Emails des BKA?" an mich gerichtet.

Diese Anfrage beantworte ich nach den mir vorliegenden Informationen wie folgt:

Zu den Fragen 1, 3 bis 5, 7, 19, 20 und 23:

1. *Wurden die Inhalte mit klassifizierten Informationen, die den Vermerk "Eingeschränkt" erhalten haben, im Sinne der Geheimschutzordnung des Bundes ordnungsgemäß verschlüsselt und sind somit ohne Schlüssel nicht einsehbar?*
   a. *Wenn ja, warum wehrt sich dann das BKA gegen die Auswertung der Mails, wenn klassifizierte Informationen ohne Schlüssel nicht gelesen werden können?*
   b. *Wenn ja, wie viele Mails wurden in diesem Sinn verschlüsselt?*
   c. *Wenn nein, warum nicht?*
3. *Wann und wie haben sie erfahren, dass sich klassifizierte Informationen im Sinne der Geheimschutzordnung oder InfoSiG oder Staatsgeheimnisse in den sichergestellten Daten befinden würden?*

4. *Von wem haben sie erfahren, dass sich klassifizierte Informationen im Sinne der Geheimschutzordnung oder InfoSiG oder Staatsgeheimnisse in den sichergestellten Daten befinden würden?*
5. *Haben sie überhaupt konkrete Erkenntnisse, dass sich klassifizierte Informationen im Sinne der Geheimschutzordnung oder InfoSiG oder Staatsgeheimnisse in den sichergestellten Daten befinden würden, oder ist das eine reine "Vorsichtsmaßnahme"?*
7. *Haben sie konkrete Informationen, wonach sich klassifizierte Informationen im Sinne der Geheimschutzordnung oder InfoSiG oder Staatsgeheimnisse in den sichergestellten E-Mails befinden?*
19. *In Ihrem ZIB 2-Interview am 28.02.2024 gaben Sie, Herr Bundeskanzler an, zur Causa mit der WKStA an, dass sie "in Abstimmung mit der Finanzprokuratur vorgehen". Auf die Frage, wie ein Staatsgeheimnis in ein E-Mail kommen könnte, antworteten Sie, dass eine genaue Prüfung geboten sei und es sich um eine Empfehlung der Finanzprokuratur handele "so vorzugehen, auch im Sinne der Mitarbeiterinnen und Mitarbeiter."*
    a. *Wie viele Gespräche mit der Finanzprokuratur fanden seit August 2022 (Anordnung der Sicherstellung durch die WKStA) statt?*
        i. *Wer nahm wann daran Teil und was war der jeweilige Gesprächsinhalt?*
    b. *Wurde das vorgebrachte rechtliche Argument, dass sich möglicherweise "Staatsgeheimnisse" in den Mails befinden, von der Finanzprokuratur vorgeschlagen?*
        i. *Wenn ja, aus welchen Gründen?*
        ii. *Wenn nein, wer hat sonst das Argument vorgebracht?*
    c. *Wurde das vorgebrachte rechtliche Argument der "privaten Daten" von der Finanzprokuratur vorgeschlagen?*
        i. *Wenn ja, aus welchen Gründen?*
        ii. *Wenn nein, wer hat sonst das Argument vorgebracht?*
20. *Welcher Auftrag mit welchem Inhalt wurde von Seiten des BKA sowie der Republik der Finanzprokuratur erteilt?*
    a. *Wurde von Seiten der Finanzprokuratur Bedenken bzgl. eines Widerspruchs mitgeteilt?*
        i. *Wenn ja, welche(r) mit welchem Inhalt?*
23. *Wo jeweils wurden die Mails mit den klassifizierten Informationen abgespeichert?*
    a. *Wurden die Mails mit den klassifizierten Informationen jeweils separat abgespeichert?*
        i. *Wurde diese schon zu Beginn separat abgespeichert?*
    b. *Wurden die Mails mit den klassifizierten Informationen jeweils als solche ausgewiesen?*

i. Wurden diese schon zu Beginn als solche ausgewiesen?

Einleitend wird festgehalten, dass zum in der Anfrage verwendeten Begriff der „Staatsgeheimnisse“ folgendes klarzustellen ist: Der Begriff „Staatsgeheimnisse“ stammt aus dem Strafrecht (insbesondere § 255 StGB). Diese Definition ist nicht ident mit jener der klassifizierten Informationen. Es kann jedoch zu Überschneidungen zwischen Staatsgeheimissen und klassifizierten Informationen kommen.

Bei den von der WKStA sichergestellten Daten sind ausschließlich Informationen der Klassifizierungsstufe EINGESCHRÄNKT gemäß InfoSiG oder GehSO betroffen. Aufgrund der durchgeführten Sichtung wurde festgestellt, dass keine Staatsgeheimnisse betroffen waren.

Da Staatsgeheimisse geschützt werden, um die „Gefahr eines schweren Nachteils für die Landesverteidigung der Republik Österreich oder für die Beziehungen der Republik Österreich zu einer fremden Macht oder einer über- oder zwischenstaatlichen Einrichtung hintanzuhalten“, wäre im Falle einer Klassifizierung von einer höheren Klassifizierungsstufe als EINGESCHRÄNKT auszugehen.

Dies vorausgeschickt darf zum besseren Verständnis und zur Einordung der Vorgänge der Rahmen und der Ablauf des Vollzuges der Sicherstellung und die sich daran anknüpfenden Schritte skizziert werden, wobei der gesamte Prozess mit Blick auf die besondere Sensibilität mit den einschreitenden Stellen abgestimmt bzw. von der Finanzprokuratur begleitet wurde und ich im Rahmen der üblichen Verwaltungstätigkeit informiert wurde:

Die WKStA hat die Sicherstellung von E-Mail-Postfächern, eOffice-Dokumenten (oder sonstige Co-Working-Spaces), persönlich zugeordneten Laufwerken (und diesbezügliche Backups und Sicherungskopien) von sämtlichen Mitarbeiterinnen und Mitarbeitern des Bundeskanzleramtes, die im Zeitraum von 19. Dezember 2017 bis 6. Oktober 2021

- im Bereich der Öffentlichkeitsarbeit und/oder in der Stabstelle für strategische Kommunikation (insbesondere Pressearbeit, Journalistenbetreuung, Digitale Kommunikation, Informationsdienst),
- im Bereich der Informationstätigkeit der Bundesregierung (insbesondere Informationsinitiativen, Medienplanung – und Budget),
- im Kabinett für die beiden genannten Bereiche, samt jeweils allfällig zugeordneter Teamassistentinnen und -assistenten und Büromitarbeiterinnen und -mitarbeitern

tätig waren, angeordnet.

Die Anordnung zur Sicherstellung wurde von der WKStA und dem Bundesamt zur Korruptionsprävention und Korruptionsbekämpfung (BAK) in Anwesenheit eines Richters des Landesgerichts für Strafsachen Wien durch Übernahme einer Festplatte mit den vom Bundeskanzleramt bereitgestellten Daten vollzogen. Dieser Datenträger wurde versiegelt und beim Landesgericht für Strafsachen Wien hinterlegt.

Gegen die Sicherstellung wurde in weiterer Folge Widerspruch gemäß §§ 112 und 112a analog StPO erhoben, da:

- die Anordnung der Sicherstellung aufgrund ihrer Unbestimmtheit für einen Vollzug zur Durchbrechung des Amtsgeheimnisses nicht geeignet war, und
- die Möglichkeit bestand, dass klassifizierte Informationen enthalten waren. Gemäß § 11 Abs. 5 GehSO ist für die Übermittlung von klassifizierten Informationen der Stufe EINGESCHRÄNKT „je nach Gegebenheit sowohl eine Sicherung des Übertragungsweges mit kryptographischen Maßnahmen als auch eine Ende-zu-Ende-Verschlüsselung zulässig“. Darauf aufbauend wurde durch die Informationssicherheitskommission (ISK) ein Beschluss gefasst, der für den Bund ein standardisiertes, technisches Übertragungsprotokoll (Sicherheitsprotokoll) für die Übermittlung von E-Mails festgelegt. Aufgrund dieses Beschlusses der ISK erfolgt bei der Übertragung von E-Mails die Verschlüsselung bereits systemseitig. Die Übertragung von Informationen der Klassifizierungsstufe EINGESCHRÄNKT, in den von Ihrer Anfrage umfassten E-Mails, war daher möglich und zulässig. Eine zusätzliche Verschlüsselung von klassifizierten E-Mails und darin enthaltenen Dokumenten der Klassifizierungsstufe EINGESCHRÄNKT selbst ist nicht erforderlich.

Das Landesgericht für Strafsachen Wien hat daraufhin das Bundeskanzleramt aufgefordert, jene elektronischen Dokumente zu bezeichnen, die klassifizierte Informationen enthalten und deren Offenlegung eine Durchbrechung der Verschwiegenheitspflicht bedeuten würde. Seitens des Bundeskanzleramts wurde in Folge die Zulässigkeit und Methodik der Sichtung mit dem Landesgericht für Strafsachen Wien wie folgt abgestimmt:

- Aufgrund datenschutzrechtlicher Bestimmungen konnte das Bundeskanzleramt organisationsseitig keine Sichtung der Dokumente durchführen.
- Daher wurde der von der Sichterstellung betroffene Personenkreis aufgefordert, die Unterlagen und Postfächer (inkl. Sicherungskopien und Backups) zu sichten und all jene Unterlagen bzw. E-Mails zu bezeichnen, welche klassifizierte Informationen enthalten. Selbstverständlich stand das Bundeskanzleramt den betroffenen Personen organisatorisch, technisch und auch rechtlich unterstützend zur Seite.

Im Rahmen der Sichtung wurden klassifizierte Informationen der Stufe EINGESCHRÄNKT identifiziert, wobei aus Sicht des Bundeskanzleramts bei einzelnen Dokumenten das staatliche Geheimhaltungsinteresse gegenüber dem Interesse an der Strafverfolgung überwog. Das Bundeskanzleramt übermittelte dem Landesgericht für Strafsachen Wien in weiterer Folge das Sichtungsergebnis samt Dokumentation des durchgeführten Vorgangs. Bzgl. dieser Dokumente wurde vom zuständigen Richter die Zurückhaltung gemäß § 112a StPO für gerechtfertigt erachtet und somit die Ansicht des Bundeskanzleramtes bestätigt.

Zu Frage 2:

2. *Wurden alle Mitarbeiter des BKA über den Umgang mit klassifizierten Informationen im Sinne der Geheimschutzordnung bzw. des InfoSiG geschult?*
   a. *Wenn ja, wurden diese Schulungen nachweislich erfasst?*
   b. *Wenn ja, was ist Inhalt dieser Schulung?*
   c. *Wenn ja, wie oft wird diese Schulung wiederholt?*
   d. *Wenn nein, warum nicht?*
   e. *Wenn nein, welche Stelle wäre für die Durchführung dieser Schulung verantwortlich laut jeweiliger Geschäftseinteilung für die Jahre 2017 bis 2024?*
   f. *Ist eine solche Schulung in Form einer Online-Schulung verfügbar?*

Der sichere Umgang mit Daten ist im Bundeskanzleramt von grundlegender Bedeutung. Daher sind alle Mitarbeiterinnen und Mitarbeiter des Bundeskanzleramts verpflichtet, Online-Trainings zur Informationssicherheit sowie zur Datenschutzgrundverordnung zu absolvieren. Ein weiteres Online-Training betrifft das Thema „Umgang mit klassifizierten Informationen“ und erfüllt das Erfordernis einer Schulung bzw. Unterweisung, das sowohl gemäß Informationssicherheitsgesetz als auch gemäß Geheimschutzordnung eine der rechtlichen Voraussetzungen für den Zugang zu klassifizierten Informationen darstellt. Eine verpflichtende Absolvierung dieses Trainings ist für alle Mitarbeiterinnen und Mitarbeiter vorgesehen, die im Zuge ihrer dienstlichen Aufgaben mit EINGESCHRÄNKTEN oder höher klassifizierten Informationen arbeiten. Die Erfassung der absolvierten Trainings erfolgt nachweislich im Elektronischen Bildungsmanagement (E-BM).

Zu den Fragen 6 und 8:

6. *Wurden irgendwelche disziplinarrechtlichen Schritte im BKA eingeleitet, die im Zusammenhang mit klassifizierten Informationen im Sinne der Geheimschutzordnung oder InfoSiG oder Staatsgeheimnisse in den sichergestellten Daten in Zusammenhang stehen?*
   a. *Wenn ja, wie viele Suspendierungen sind erfolgt?*

b. Wenn ja, wie viele Mitarbeiter sind betroffen?

8. Besteht die Möglichkeit, dass Mitarbeiter:innen des BKA Informationen, die im Sinne der Geheimschutzordnung bzw. des InfoSiG unter diese Regelungen fallen, einfach ignorieren?

a. Wenn ja, gibt es da häufigere Fälle in bestimmten Abteilungen oder Referaten?

Es gab keine dienst- bzw. disziplinarrechtlichen Verletzungen im Sinne der Fragestellung.

Zu Frage 9:

9. Gemäß der Informationssicherheitsvorschriften iSd InfoSiG und der dazugehörenden Verordnung müssen alle klassifizierten Informationen in einem Register erfasst werden. In diesem Register ist ersichtlich, wer die Informationen an wen weitergegeben hat. Gibt es dieses Register im BKA?

a. Wenn ja, wer führt dieses Register?

b. Wenn ja, gibt es in diesem Register Einträge aus der Zeit der Sicherstellung der E-Mails?

c. Wenn ja, betreffen Einträge in diesem Register von der Sicherstellung betroffene Mitarbeiter?

d. Wenn nein, warum nicht?

e. Wurde der Informationssicherheitsbeauftragte des BKA bereits tätig?

f. Wenn ja, welche Maßnahmen hat er genau getätigt?

g. Wenn nein, warum nicht?

Informationen der Klassifizierungsstufe EINGESCHRÄNKT gemäß InfoSiG oder GehSO unterliegen nicht einer solchen Registrierungspflicht und ausschließlich solche waren von der Sicherstellung betroffen.

Zu Frage 10:

10. Wer ist derzeit der Informationssicherheitsbeauftragte des BKA?

Informationssicherheitsbeauftragter gemäß § 7 InfoSiG im Bundeskanzleramt ist der Abteilungsleiter der Abteilung I/10 (Informationssicherheit).

Zu den Fragen 11 und 12:

11. Welche IKT-Systeme sind von der Informationssicherheitskommission im BKA für die Verarbeitung von klassifizierten Informationen akkreditiert?

12. *Sind IKT-Systeme, die von der Sicherstellung betroffen sind, von der Informationssicherheitskommission im BKA für die Verarbeitung von klassifizierten Informationen akkreditiert?*

Eine Akkreditierung von Informations- und Kommunikationssystemen ist für die Verarbeitung von Informationen der Klassifizierungsstufe EINGESCHRÄNKT nicht vorgesehen. Nach InfoSiV und GehSO bedarf es besonderer Schutzmaßnahmen. Dafür sind die Bundesministerien im eigenen Wirkungsbereich unter Berücksichtigung der Vorgaben der ISK zuständig.

Für die Verarbeitung von Informationen der Klassifizierungsstufe EINGESCHRÄNKT ist insbesondere der ELAK im Bund vorgesehen. Nach Einhaltung vorgegebener Sicherungsprotokolle am Übertragungsweg können solche Informationen auch per E-Mail versandt werden.

Zu den Fragen 13 bis 15:

13. *Haben sie als Minister mit anderen Beschuldigten in gegenständlicher Causa Kontakt gehabt?*
    a. *Wenn ja, mit wem und wann?*
14. *Haben Ihre Mitarbeiter mit anderen Beschuldigten in gegenständlicher Causa Kontakt gehabt?*
    a. *Wenn ja, mit wem und wann?*
15. *Haben sie als Minister in gegenständlicher Causa Kontakt mit ihrem Generalsekretär der ÖVP gehabt?*
    a. *Wenn ja, mit wem und wann und was wurde besprochen?*

Fragen betreffend meine Ministertätigkeit sind kein Gegenstand des aktuellen Vollziehungsbereiches nach dem Bundesministeriengesetz 1986 in der nunmehr geltenden Fassung, BGBl. I Nr. 44/2024.

Zu Frage 16:

16. *Waren alle Empfänger der klassifizierten Informationen (auch CC und BCC) in den E-Mails berechtigt, die Staatsgeheimnisse zu erhalten?*
    a. *Wenn nein, wusste der Informationssicherheitsbeauftragte des Bundeskanzleramtes davon Bescheid?*
        i. *Wenn nein, warum nicht und warum wurde dieser nicht benachrichtigt?*
        ii. *Wenn ja, hat der Informationssicherheitsbeauftragte dies bemängelt?*

iii. Wenn ja, wie hat der Informationssicherheitsbeauftragte jeweils davon Kenntnis erlangt?

b. Wenn nein, welche Maßnahmen wurden dagegen getroffen?

Der von der Sicherstellung betroffene Personenkreis war generell berechtigt, klassifizierte Informationen zu erhalten. Die konkrete inhaltliche Berechtigung richtet sich nach dem Need-To-Know-Prinzip, dessen Festlegung nicht zentral erfolgt, sondern durch die jeweilige Absenderin, den jeweiligen Absender. Die Sichtung der Dokumente wurde ausschließlich von den betroffenen Personen selbst vorgenommen. Bis zum Anfragestichtag sind keine Dienstpflichtverletzungen in diesem Zusammenhang bekannt.

Zu den Fragen 17 und 18:

17. Wie viele der betroffenen E-Mail Konten haben die E-Mails auf Handys empfangen?

18. Gab oder gibt es Bedienstete, die ihre E-Mails samt Staatsgeheimnissen auch auf privaten Handys empfangen haben?

a. Wenn ja, wusste der Informationssicherheitsbeauftragte des Bundeskanzleramtes davon Bescheid?

i. Wenn nein, warum nicht und warum wurde dieser nicht benachrichtigt?

ii. Wenn ja, hat der Informationssicherheitsbeauftragte dies bemängelt?

iii. Wenn ja, wie hat der Informationssicherheitsbeauftragte jeweils davon Kenntnis erlangt?

b. Wenn ja, welche Maßnahmen wurde daraufhin getroffen?

Der betroffene Personenkreis hat keine E-Mails mit Staatsgeheimnissen über dienstlich zur Verfügung gestellte Handys empfangen. Im Bundeskanzleramt sind private Handys von Bediensteten nicht im hauseigenen Netzwerk integriert.

Zu den Fragen 21, 22 und 24:

21. Befinden sich in den Mails klassifizierte Informationen von anderen Staaten, mit denen bilaterale Abkommen über den Austausch und Gleichbehandlung von klassifizierten Informationen abgeschlossen wurden?

a. Wenn ja, welche Pflichten und Anforderungen waren alle einzuhalten?

i. Die logische Netztrennung von Netzwerken?

ii. Die Implementierung von "Data Loss Prevention"?

iii. Die komplette logische Trennung von höher klassifizierten Informationen zu Informationen anderer Klassifizierung?

iv. Andere?

22. *Befinden sich in den Mails klassifizierte Informationen der Stufe "Eingeschränkt" von den USA?*
24. *Wurden klassifizierte Informationen betreffend "SkyShield" im Mailpostfach und/oder auf dem Laptop gespeichert?*
    a. *Wenn ja, sind diese von anderen Staaten übermittelt worden?*
    b. *Wenn ja, sind diese vom BMLV übermittelt worden?*

Aufgrund datenschutzrechtlicher Bestimmungen konnte das Bundeskanzleramt organisationsseitig keine Sichtung der Dokumente durchführen. Die E-Mailpostfächer wurden von den betroffenen Personen selbst gesichtet. Auf Basis dieser Sichtung kann festgehalten werden, dass sich keine klassifizierten Informationen zu den genannten Themen in den E-Mails befanden.

Zu Frage 25:

25. *Befanden sich in der Mailbox und/oder auf dem Laptop von Sebastian Kurz Mails mit klassifizierten Informationen und/oder wurden diese verarbeitet?*
    a. *Wenn ja, inwiefern?*

Die Mailbox von Sebastian Kurz war nicht von der Sicherstellung umfasst.

Zu den Fragen 26 bis 28:

26. *In Ihrer Anfragebeantwortung 16183/AB vom 19.12.2023 (https://www.parlament.gv.at/gegenstand/XXVII/AB/16183) auf unsere parlamentarische Anfrage 16650/J (https://www.parlament.gv.at/gegenstand/XXVII/J/16650), verwiesen Sie bzgl der Frage, welche sichergestellten Unterlagen von welchen (ehemaligen) Mitarbeiter:innen welcher Abteilung, Sektion, oder welcher anderen Organisationseinheit klassifizierte nachrichtendienstliche Informationen oder klassifiziert übermittelte Informationen nach §112a Abs 1 beinhalten, die der Geheimhaltung unterliegen sollen, dass dies eine Sichtung benötigen würde und die Information außerdem unter Amtsverschwiegenheit fallen würde. Welche Gründe der Amtsverschwiegenheit iSd § 20 Abs 3 B-VG wären denn erfüllt?*
27. *In Ihrer Anfragebeantwortung 16183/AB vom 19.12.2023 (https://www.parlament.gv.at/gegenstand/XXVII/AB/16183) auf unsere parlamentarische Anfrage 16650/J (https://www.parlament.gv.at/gegenstand/XXVII/J/16650), verwiesen Sie bzgl der Frage 9, wie oft und wann der Informationssicherheitsbeauftragte auf einen Mangel iSd § 7 Abs 1 InfoSiG hingewiesen hat, auf die Amtsverschwiegenheit? Welche Gründe der Amtsverschwiegenheit iSd § 20 Abs 3 B-VG wären denn erfüllt?*

28. *In Ihrer Anfragebeantwortung 16183/AB vom 19.12.2023 (https://www.parlament.gv.at/gegenstand/XXVII/AB/16183) auf unsere parlamentarische Anfrage 16650/J (https://www.parlament.gv.at/gegenstand/XXVII/J/16650), verwiesen Sie bzgl. der Frage 10, wie oft und wann der Informationssicherheitsbeauftragte Ihnen, Herr Bundeskanzler, oder jemand anderem in Ihrem Ressort Vorschläge zur Verbesserung der Informationssicherheit gem § 7 Abs 4 InfoSiG gemacht hat und ob Sie oder Ihr Ressort dem jedes Mal nachgekommen sind, auf Amtsverschwiegenheit. Welche Gründe der Amtsverschwiegenheit iSd § 20 Abs 3 B-VG wären denn erfüllt?*

Zu der angeführten vorangegangenen parlamentarischen Anfrage vom 19. Oktober 2023 ist festzuhalten, dass eine Veröffentlichung der dort angefragten Informationen mögliche Angriffsvektoren auf das Bundeskanzleramt preisgeben würde, welche die in Art. 20 Abs. 3 B-VG genannten Interessen „Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit“ berühren bzw. diesen zuwiderlaufen würde.

Karl Nehammer

REPUBLIK ÖSTERREICH BUNDESKANZLERAMT AMTSSIGNATUR	Unterzeichner	serialNumber=734173660,CN=Bundeskanzleramt,C=AT
	Datum/Zeit	2024-06-04T18:07:56+02:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at Informationen zur Prüfung des Ausdrucks finden Sie unter: https://www.bundeskanzleramt.gv.at/verifizierung
	Hinweis	Dieses Dokument wurde amtssigniert.

	Unterzeichner	Parlamentsdirektion
	Datum/Zeit-UTC	2024-06-04T18:13:02+02:00
Prüfinformation	Dieses Dokument wurde elektronisch besiegelt. Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel	