4171/AB
vom 11.12.2019 zu 4192/J (XXVI. GP)

Bundesministerium
Inneres

bmi.gv.at

Dr. Wolfgang Peschorn
Bundesminister

Herrn
Präsidenten des Nationalrates
Mag. Wolfgang Sobotka
Parlament
1017 Wien

Geschäftszahl: BMI-LR2220/0661-II/2019

Wien, am 11. Dezember 2019

Sehr geehrter Herr Präsident!

Der Abgeordnete zum Nationalrat Jenewein hat mit Unterstützung weiterer Abgeordneter am 25. September 2019 unter der Nr. **4192/J** an mich eine schriftliche parlamentarische Anfrage betreffend „Datenleck Rubicon" gerichtet, die ich nach den mir vorliegenden Informationen wie folgt beantworte:

Zur Frage 1:

- *Was wird mit dem Programm EDIS im BVT bearbeitet/verarbeitet/gespeichert?*

EDIS („Elektronisches Dokumenteninformationssystem") dient der formalen Behandlung von zu besorgenden Geschäftsfällen des Bundesamtes für Verfassungsschutz und Terrorismusbekämpfung einschließlich der Aufbewahrung der bei dieser Tätigkeit anfallenden Dokumente.

Zu den Fragen 2 bis 6:

- *Welche Informationen werden nach dem InfoSiG-Informationssicherheitsgesetz klassifiziert?*
- *Gilt dieses Gesetz auch für die LVTs-Landesämter für Verfassungsschutz und Terrorismusbekämpfung und andere nachgeordnete Sicherheitsbehörden?*
  a. Wenn nein, warum nicht?
- *Welche Informationen werden nach der GehSO-Geheimschutzordnung klassifiziert?*
- *Wie werden Informationen im BVT klassifiziert?*
- *Nach welchen gesetzlichen Bestimmungen werden diese Informationen im BVT klassifiziert?*

Das Bundesgesetz über die Umsetzung völkerrechtlicher Verpflichtungen zur sicheren Verwendung von Informationen (Informationssicherheitsgesetz, InfoSiG), BGBl I Nr. 23/2002 wurde zur Gewährleistung einheitlicher Informationssicherheitsstandards bei der Zusammenarbeit im Rahmen der Europäischen Union sowie im internationalen Bereich erlassen.

Klassifizierte Informationen, die Österreich im Einklang mit völkerrechtlichen Regelungen erhält, sind in dem von den übermittelnden ausländischen Stellen vorgesehenen Maß und für die von dieser vorgesehenen Dauer zu beschränken. Dies geschieht, indem derartige Informationen einer der in § 2 Abs. 2 Z 1 bis 4 InfoSiG normierten Klassifizierungsstufen („STRENG GEHEIM", „GEHEIM", „VERTRAULICH" oder „EINGESCHRÄNKT") zugeordnet werden.

Gemäß § 1 Abs. 1 InfoSiG gilt das Informationssicherheitsgesetz auch für die nachgeordneten Landespolizeidirektionen und die ihnen unterstehenden Landesämter für Verfassungsschutz und Terrorismusbekämpfung (LVT).

Informationen, die nicht dem Anwendungsbereich des Informationssicherheitsgesetzes unterliegen, aber auf Grund ihres Inhalts einer besonderen Geheimhaltung bedürfen, werden nach den Bestimmungen der Geheimschutzordnung des Bundes (GehSO) klassifiziert. Inhaltlich folgt die GehSO weitgehend der Systematik des InfoSiG, sodass die Systeme für national und international klassifizierte Informationen im Wesentlichen identisch sind; dies jedoch mit der Maßgabe, dass im nationalen Bereich ergänzend die Klassifizierung „VERSCHLUSS" weiterhin zur Verfügung steht.

Informationen werden im Bundesamt für Verfassungsschutz und Terrorismusbekämpfung – gemäß ihrem Ursprung – entweder nach den Bestimmungen des Informationssicherheitsgesetzes oder der Geheimschutzordnung des Bundes klassifiziert.

Zu den Fragen 7 bis 17, 28 bis 32, 34 bis 45, 49 sowie 51 und 52:

- *Wo werden die klassifizierten Dokumente im BVT aufbewahrt?*
- *Warum werden die gesetzlichen Bestimmungen zur Klassifizierung nicht eingehalten?*
- *Wie erfolgt die Bearbeitung der klassifizierten Dokumente?*
  a. *Vor der "BVT-Razzia" am 28.02.2018?*
  b. *Nach der "BVT-Razzia" am 28.02.2018?*
- *Werden diese klassifizierten Dokumente auch elektronisch bearbeitet/verarbeitet?*
- *Ist das EDIS System im BVT dafür zertifiziert?*
  a. *Wenn ja, seit wann?*
  b. *Wenn ja, von wem erfolgte die Zertifizierung?*
  c. *Wenn nein, warum nicht?*
- *lst das E-Mail System im BVT dafür zertifiziert?*

a. *Wenn ja, seit wann?*
b. *Wenn ja, von wem erfolgte die Zertifizierung?*
c. *Wenn nein, warum nicht?*

- *Warum werden die klassifizierten Dokumente im EDIS gespeichert, bearbeitet und verarbeitet?*
- *Warum werden die klassifizierten Dokumente im E-Mail System gespeichert, verschickt, bearbeitet und verarbeitet?*
- *Wurde die ISK-Informationssicherheitskommission davon wie vorgesehen informiert?*
  a. *Wenn nein warum nicht?*
- *lm EDIS-Handbuch befindet sich eine Dienstanweisung des BVT-Direktors, wonach Partnerdienst-Infos im EDIS zu speichern sind?*
- *Wie viele Informationen von Partnerdiensten finden sich nach wie vor im EDIS?*
- *War das Programm EDIS bevor Herbert KICKL Innenminister wurde, zertifiziert?*
  a. *Wenn nein, warum nicht?*
- *Ist das E-Mail System von der ISK-Informationssicherheitskommission im Bundeskanzleramt zertifiziert?*
  a. *Wenn ja, seit wann?*
  b. *Wenn nein, warum nicht?*
- *Wurde der Umstand, dass das Programm und die gesamte EDV-Ausstattung (PC, Laptop, Server, E-Mail Server, Mobiltelefone, Smartphones) des BVT von der ISK-Informationssicherheitskommission im Bundeskanzleramt nicht zertifiziert ist, den Partnerdiensten verschwiegen?*
- *Ist es gesetzlich verboten, klassifizierte Informationen ab der Stufe Vertraulich im EDIS zu speichern?*
- *Ist dieser Umstand, dass klassifizierte Informationen im EDIS gespeichert werden, obwohl das System nicht dafür zertifiziert ist, dem jeweiligen Informationssicherheitsbeauftragten bekannt gewesen?*
  a. *Welche Maßnahmen hat der Informationssicherheitsbeauftragte unternommen, um diesen Missstand abzustellen?*
  b. *Wurde die ISK über diesen Missstand vom Informationssicherheitsbeauftragten informiert?*
- *Wie viele klassifizierte Schriftstücke, aufgeschlüsselt nach Eingangsstücken und Akten gesamt (InfoSiG, GehSO, PolKG) sind dort gespeichert?*
  a. *Wie viele sind eingeschränkt?*
  b. *Wie viele sind vertraulich?*
  c. *Wie viele sind geheim?*
  d. *Wie viele sind Streng geheim?*
- *Wie viele klassifizierte Schriftstücke aufgeschlüsselt nach Eingangsstücken und Akten nach dem InfoSiG sind dort gespeichert?*
  a. *Wie viele sind eingeschränkt?*
  b. *Wie viele sind vertraulich?*

c. *Wie viele sind geheim?*
d. *Wie viele sind Streng geheim?*

- *Wie viele klassifizierte Schriftstücke aufgeschlüsselt nach Eingangsstücken und Akten nach der GehSO sind dort gespeichert?*
  a. *Wie viele sind eingeschränkt?*
  b. *Wie viele sind vertraulich?*
  c. *Wie viele sind geheim?*
  d. *Wie viele sind Streng geheim?*
- *Wie viele klassifizierte Schriftstücke aufgeschlüsselt nach Eingangsstücken und Akten nach dem PolKG sind dort gespeichert?*
  a. *Wie viele sind eingeschränkt?*
  b. *Wie viele sind vertraulich?*
  c. *Wie viele sind geheim?*
  d. *Wie viele sind Streng geheim?*
- *Exemplarisch: Sind Informationen der CIA, des MI6, des MOSSAD, des BND, des HNaA, etc., die mit CONFIDENTIAL/VERTRAULlCH, gekennzeichnet sind im EDIS gespeichert?*
  a. *Wenn ja, entspricht das dem InfoSiG?*
  b. *Wenn ja, entspricht dies der GehSO?*
  c. *Wenn ja, entspricht dies dem PoIKG?*
- *Exemplarisch: Sind Informationen der CIA, des MI6, des MOSSAD, des BND, des HNaA, etc., die mit SECRET/GEHEIM, gekennzeichnet sind im EDIS gespeichert?*
  a. *Wenn ja, entspricht das dem InfoSiG?*
  b. *Wenn ja, entspricht dies der GehSO?*
  c. *Wenn ja, entspricht dies dem PoIKG?*
- *Exemplarisch: Sind Informationen der CIA, des MI6, des MOSSAD, des BND, des HNaA, etc., die mit TOP-SECRET/STRENG GEHEIM, gekennzeichnet sind im EDIS gespeichert?*
  a. *Wenn ja, entspricht das dem InfoSiG?*
  b. *Wenn ja, entspricht dies der GehSO?*
  c. *Wenn ja, entspricht dies dem PoIKG?*
- *Gibt es spezielle Aufbewahrungsvorschriften entsprechend des InfoSiG und werden/wurden diese durchgehend eingehalten?*
- *Warum sind überhaupt so viele klassifizierte Informationen im EDIS gespeichert?*
- *Wer ordnete diese Speicherungen an?*
- *Seit wann erfolgten diese Speicherungen?*
- *Wenn nein, warum müssen dann klassifizierte Dokumente über EDIS versendet werden oder wurden über EDIS versendet?*
- *lst es möglich, Informationen von Partnerdiensten durch Zusammenfassungen oder Umschreiben zu deklassifizieren?*
- *Entspricht es der Wahrheit, dass es BVT Mitarbeitern mit Laptops möglich ist, via Fernzugriff ("Tunnellösung") von überall aus der Welt auf das interne BVT-System und damit auch auf die im EDIS gespeicherten Partnerdienstinformationen ohne Einschränkung zuzugreifen?*

   a. *Wenn ja, entspricht dies den gesetzlichen Vorgaben des InfoSiG?*
   b. *Wenn ja, entspricht dies den gesetzlichen Vorgaben der GehSO?*
   c. *Wenn ja, entspricht dies den gesetzlichen Vorgaben der PolKG?*
   d. *Wenn ja, ist diese Praxis den Partnerdiensten bekannt?*
   e. *Wenn ja, seit wann ist dies möglich?*
   f. *Wenn ja, wer hat dies angeordnet?*
- *Entspricht es der Wahrheit, dass es BVT Mitarbeitern mit Laptops möglich ist, via Fernzugriff ("Tunnellösung") von jeder Polizeiinspektion/von jedem Polizeicomputer in Österreich auf das interne BVT-System und damit auch auf die im EDIS gespeicherten Partnerdienstinformationen ohne Einschränkung zuzugreifen?*
   a. *Wenn ja, entspricht dies den gesetzlichen Vorgaben des InfoSiG?*
   b. *Wenn ja, entspricht dies den gesetzlichen Vorgaben der GehSO?*
   c. *Wenn ja, entspricht dies den gesetzlichen Vorgaben der PolKG?*
   d. *Wenn ja, ist diese Praxis den Partnerdiensten bekannt?*
   e. *Wenn ja, seit wann ist dies möglich?*
   f. *Wenn ja, wer hat dies angeordnet?*

Diese Fragen betreffen wesentliche Kernbereiche der hochsensiblen Tätigkeit und Aufgabenerfüllung des Verfassungsschutzes. Ihre Geheimhaltung ist zentrale Voraussetzung für die gesetzmäßige Aufgabenerfüllung der Verfassungsschutzbehörden und ist für die Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit unerlässlich. Die öffentliche Beantwortung von Fragen zur elektronischen Kommunikation mit Partnerdiensten, zu Akteninhalten, ihrer Klassifizierung, zu ihrem Speicherort oder zum Umgang mit ihnen, zu technischem und organisatorischem Aufbau der elektronischen Aktenverwaltung und Kommunikation des Verfassungsschutzes, zu Details darüber, in welchen Systemen welche Daten verarbeitet werden oder zur grundsätzlichen Ausgestaltung der Systemarchitektur oder einzelner Programme, würde einen idealen Anknüpfungspunkt für Angriffe durch fremde Geheim- und Nachrichtendienste darstellen, die derartige Informationen für ihre Interessenverfolgung missbrauchen könnten.

Im Hinblick auf die Schlussfolgerungen des parlamentarischen Untersuchungsausschusses, der Defizite bei der Geheimhaltung vertraulicher Informationen des Bundesamtes für Verfassungsschutz und Terrorismusbekämpfung in der Vergangenheit festgestellt hat und aufgrund der Verpflichtung zur Wahrung der Amtsverschwiegenheit, insbesondere im Interesse der Aufrechterhaltung der öffentlichen Ruhe, Ordnung und Sicherheit sowie der auswärtigen Beziehungen, muss von einer inhaltlichen Beantwortung dieser Fragen Abstand genommen werden.

Zur Frage 18:

- *Mit welchen Ländern gilt das InfoSiG, wenn Informationen gekennzeichnet sind*
  a. *Sind Informationen von diesen Ländern, die gekennzeichnet sind, im EDIS gespeichert?*
  b. *Werden oder wurden Informationen von diesen Ländern, die entsprechend gekennzeichnet sind, per Dienstanweisung intern via E-Mail versendet?*

Das InfoSiG zählt keine Staaten oder Internationalen Organisationen auf, für deren Informationen es Gültigkeit hat, sondern stellt generell auf die in der internationalen Zusammenarbeit üblichen Klassifizierungsstufen und auf damit korrespondierende völkerrechtlichen Regelungen ab. Im Übrigen darf auf die obigen Ausführungen verwiesen werden.

Zu den Fragen 19 bis 21:

- *Liegt mit der Fa RUBICON ein entsprechender Vertrag und Vertragsabschluss vor?*
  a. *Wenn ja, wo befindet sich der Vertrag nun?*
  b. *Wenn nein, warum ist der Vertrag nicht vorhanden?*
  c. *Wenn nein, warum erfolgen trotz Fehlen des Vertrages weiterhin die Zahlungen an die Firma RUBICON?*
  d. *Entspricht es der Wahrheit, das für das Servicepaket der Firma RUBICON eine Jahrespauschale von 1 Million Euro zu bezahlen ist?*
  e. *Entspricht es der Wahrheit, dass für eine Rufbereitschaft der Firma RUBICON monatlich der Betrag von € 10.000 Euro zu bezahlen ist?*
- *Wurde das Programm EDIS entsprechend den vertraglichen Vereinbarungen umgesetzt?*
  a. *Wenn nein, warum nicht?*
- *Wurde die volle vereinbarte Summe für das Programm EDIS bezahlt?*
  a. *Wenn ja, wann und in welcher Höhe?*

Über die Erstellung von EDIS durch die Firma RUBICON wurde im Jahr 2007 ein Vertrag geschlossen. Die Vertragsdokumente wurden mit Ausnahme des Angebots im Elektronischen Akt (ELAK) dokumentiert. Das vorausgegangene Angebot wurde im Jahr 2006 aufgrund seines Umfangs nicht elektronisch erfasst. Das Original liegt in der Sektion III des Bundesministeriums für Inneres auf.

Es trifft nicht zu, dass eine Jahrespauschale von 1 Million Euro und ein monatlicher Betrag von 10.000 Euro für eine Rufbereitschaft zu bezahlen sind.

EDIS wurde auf Grundlage einer vertraglichen Vereinbarung umgesetzt und gemäß der folgenden Aufstellung in den Jahren 2007 bis 2010 bezahlt:

Jahr	Kosten in EURO (inklusive Steuern)
2007	429.600,00
2008	760.127,00
2009	1.319.699,20
2010	814.014,00

Zur Frage 22:

- *Entspricht es der Wahrheit, dass der ehemalige Kabinettschef Michael KLOIBMÜLLER oder eine andere derzeit unbekannte Person die Weisung erteilt hat, das Programm EDIS, obwohl es noch nicht fertig ist, abzunehmen und in den Echtbetrieb überzugehen?*
  a. *Wenn ja, wer hat diese Weisung erteilt?*
  b. *Wenn ja, wann ist diese Weisung ergangen?*
  c. *Wenn nein, ist das EDIS gemäß den für den Vertragsabschluss vereinbarten Parameter im Pflichtenheft fertiggestellt?*
  d. *Wenn nein, warum nicht?*

Eine derartige Weisung ist nicht bekannt und EDIS wurde gemäß den vertraglichen Vereinbarungen umgesetzt.

Zu den Fragen 23 bis 27:

- *Berührt das nunmehr medial bekannte Daten-Leak auch das BVT?*
- *Hatte die Fa RUBICON einen Fernzugriff auf das EDIS Programm im BVT?*
- *Ist es Mitarbeitern der Fa RUBICON theoretisch möglich gewesen, innerhalb des BVT auf Echtdaten im EDIS zuzugreifen?*
  a. *Wenn ja, ist dies den Partnerdiensten bekannt?*
  b. *Wenn nein, kann dies zu 100% ausgeschlossen werden?*
- *Ist es Mitarbeitern der Fa RUBICON theoretisch möglich gewesen, von außerhalb des BVT auf Echtdaten im EDIS zuzugreifen?*
  a. *Wenn ja, ist dies den Partnerdiensten bekannt?*
  b. *Wenn nein, kann dies zu 100% ausgeschlossen werden?*
- *Entspricht es der Wahrheit, das Mitarbeiter der Fa RUBICON für das BVT Datenlöschungen im EDIS durchgeführt haben?*

Am 19. September 2019 wurde in diversen (Online-)Medien über ein angebliches „Datenleck" im Zusammenhang mit Wartungsarbeiten für diverse Applikationen durch Mitarbeiter der RUBICON IT GmbH berichtet. Ich habe daraufhin eine Untersuchung angeordnet. Nach den mir derzeit vorliegenden Informationen wurden dabei weder personsbezogene Daten missbräuchlich verarbeitet noch kam es zu Datenabflüssen oder sonstigen Datensicherheitsverletzungen (Databreach) im Sinne der DSGVO.

Zutreffend ist, dass am 1. März 2019 für Wartungszwecke bestehende Remotezugänge für Mitarbeiter des Auftragsverarbeiters gesperrt wurden und diese nunmehr vor Ort und im Beisein eines BMI-Technikers allenfalls notwendige Arbeiten ausführen müssen. Diese organisatorischen und technischen Maßnahmen erfolgten zur weiteren Optimierung der Datensicherheit.

Die kolportierten Sachverhalte bezogen sich im Übrigen gar nicht auf EDIS. Mitarbeiter der Firma RUBICON verfügten zu keiner Zeit über einen Fernzugriff auf die Daten im EDIS. Im Bedarfsfall werden notwendige Supporttätigkeiten, worunter auch etwaige Datenlöschungen fallen können, in den Räumlichkeiten des Bundesamtes für Verfassungsschutz und Terrorismusbekämpfung durchgeführt. Dabei wird durch technische und organisatorische Maßnahmen sichergestellt, dass kein unkontrollierter Zugang besteht. Derartige Tätigkeiten werden ausschließlich von Personen durchgeführt, die sich erfolgreich einer entsprechenden Sicherheitsüberprüfung unterzogen haben.

Es darf um Verständnis ersucht werden, dass über genaue Inhalte, die mit ausländischen Sicherheitsbehörden ausgetauscht werden, auf Grundlage einer Abwägung der Interessen Österreichs an einer internationalen Zusammenarbeit mit ausländischen Sicherheitsbehörden und dem parlamentarischen Interpellationsrecht nach Art. 20 Abs. 3 B-VG, keine Auskunft erteilt werden kann.

Zur Frage 33:

- *Wer war der jeweilige Informationssicherheitsbeauftragte seit Inbetriebnahme des EDIS?*

Die Funktion des Informationssicherheitsbeauftragten für den Wirkungsbereich des Bundesministeriums für Inneres nahm seit Inbetriebnahme des EDIS der Direktor des Bundesamtes für Verfassungsschutz und Terrorismusbekämpfung wahr.

Seit Inkrafttreten des Bundesgesetzes über die Organisation, Aufgaben und Befugnisse des polizeilichen Staatsschutzes (PStSG), BGBl. I Nr. 5/2016 am 1. Juli 2016 ist diese Funktion gemäß § 2 Abs. 1 PStSG dem jeweiligen Direktor des Bundesamtes für Verfassungsschutz und Terrorismusbekämpfung ex lege zugewiesen.

Zu den Fragen 46 und 50:

- *Stimmt es, dass andere Partnerdienste bezüglich der Verwendung ihrer Informationen belogen werden oder ihnen nicht die volle Wahrheit gesagt wurde?*
- *Entspricht es der Wahrheit, dass der stellvertretende Direktor des BVT, Mag. Dominik FASCHING auf die Einhaltung der Gesetze betr. der Vertraulichkeit der Partnerdienstinformationen pocht und vom Direktor des BVT, Mag. Peter GRIDLING daran gehindert wird?*

Es sind mir dafür keine Informationen bekannt geworden.

Zu den Fragen 47 und 48:

- *Ist es möglich, Informationen von Partnerdiensten zu deklassifizieren, ohne deren Einverständnis einzuholen?*
- *Wird diese Vorgangsweise im BVT praktiziert?*
  a. *Wenn ja, wer hat dies angeordnet?*
  b. *Seit wann erfolgt diese Vorgangsweise?*

Die Deklassifizierung von klassifizierten Informationen einer ausländischen Sicherheitsbehörde ist ohne deren vorherige Zustimmung nicht zulässig und wird vom Bundesamt für Verfassungsschutz und Terrorismusbekämpfung auch nicht vorgenommen.

Dr. Wolfgang Peschorn

REPUBLIK ÖSTERREICH AMTSSIGNATUR	Datum/Zeit	2019-12-11T10:02:10+01:00
	Aussteller-Zertifikat	a-sign-corporate-light-02
	Serien-Nr.	1624172
Prüfinformation	Informationen zur Prüfung des elektronischen Siegels bzw. der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at Eine Verifizierung des Ausdruckes kann bei der ausstellenden Behörde/Dienststelle erfolgen.	
Hinweis	Dieses Dokument wurde amtssigniert.	

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2019-12-11T13:12:09+01:00
	Prüfinformation	Informationen zur Prüfung des elektronischen Siegels und des Ausdrucks finden Sie unter: https://www.parlament.gv.at/siegel
Hinweis	Dieses Dokument wurde elektronisch besiegelt.	