3795/AB
vom 26.08.2019 zu 4016/J (XXVI.GP)

Bundeskanzleramt

bundeskanzleramt.gv.at

Dr. Brigitte Bierlein
Bundeskanzlerin

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: BKA-353.110/0082-IIM/2019

Wien, am 26. August 2019

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Dr. Krisper, Kolleginnen und Kollegen haben am 22. Juli 2019 unter der Nr. **4016/J** an mich eine schriftliche parlamentarische Anfrage betreffend „‚Schredder-Gate' im BKA" gerichtet.

Zur Beantwortung der gegenständlichen Fragen darf ich mit von den zuständigen Organisationseinheiten des Bundeskanzleramtes aufbereiteten grundsätzlichen Erläuterungen und erforderlichen Differenzierungen einleiten. Dies scheint einerseits zum besseren Verständnis der Beantwortung der Fragen und andererseits zur Vermeidung von Wiederholungen geboten. Angemerkt werden darf, dass sich die Fragen überwiegend auf Vorgänge vor meiner Amtszeit beziehen.

Zur Funktionsweise und korrekten Handhabung moderner IT-Lösungen und IT-Geräte dürfen einzelne relevante Themenstellungen (v.a. Recht, Technik, Organisation und technischer Fortschritt) interdisziplinär dargestellt werden.

1. Allgemeine technisch-organisatorische Themenstellungen

Ein wesentliches Merkmal zur Kategorisierung von Daten bildet die Form der Datenquelle. So können grundsätzlich unterschieden werden:

- Benutzerverwaltete Daten (z.B. durch Eingabe, Lesen, Speichern/Ablage, Löschen, Drucken)
- Systemverwaltete Daten, ohne Zugriffsmöglichkeiten durch Benutzerinnen und Benutzer

Zum Umgang mit Datenträgern darf bereits an dieser Stelle festgehalten werden: Datenträger wie z.B. Festplatten (PCs, Laptops, Server, Multifunktionsgeräte) oder USB-Sticks werden nach den mir vorliegenden Informationen seit Frühjahr 2015 grundsätzlich einer Vernichtung im Wege des Bundeskanzleramtes, Zentrales Ausweichsystem des Bundes (ZAS) zugeführt. Damit soll die Möglichkeit des Abflusses von Daten über den Weg gebrauchter Datenträger aus dem Bundeskanzleramt ausgeschlossen werden. Defekte Festplatten aus PCs oder Laptops, die nicht mehr im geordneten Weg unlesbar gemacht werden können, werden ebenfalls einbehalten und einer Verschredderung zugeführt.

1.1. Benutzerverwaltete Daten

Bei benutzerverwalteten Daten wird danach unterschieden, ob es sich einerseits um Daten in Aktensystemen und Fachanwendungen handelt, welche ihrer technischen Bereitstellung entsprechend ausschließlich dienstlicher Natur sind, und andererseits, ob es Daten sind, die sich auf allgemeinen Ablagesystemen oder IT-Geräten befinden, welche hinsichtlich ihrer inhaltlichen Datennatur eine Gemengelage bilden.

So werden in Aktensystemen die Daten ihrem Inhalt nach exakt der Vertraulichkeitsstufe und dem Sicherheitsbedarf entsprechend gespeichert, wohingegen in allgemeinen Ablagesystemen eben eine Gemengelage an Daten vorliegt. Es handelt sich dabei meist um Datenkonglomerate aus:

- dienstlichen Daten
- Personaldaten
- persönlichen Daten[1]
- mitunter sensiblen Daten oder
- in besonderen Fällen auch klassifizierten Daten.

[1] Vgl. IKT-Nutzungsverordnung, BGBl. II Nr. 281/2009.

Derartige Datenkonglomerate sind u.a. gespeichert auf:

- allgemeinen elektronischen Dateiablagen (techn. "Fileshare")
- PCs und Notebooks
- Tablets und Smartphones
- E-Mailboxen

Die IKT-Nutzungsverordnung regelt die Nutzung dieser Instrumente durch Bundesbedienstete auch für private Zwecke – im eingeschränkten Ausmaß – und bildet für die rechtskonforme Speicherung die Grundlage.

Das eigentliche Verwaltungshandeln, so auch in Kabinetten, findet daher, soweit es technisch unterstützt wird, im weitaus überwiegenden Ausmaß in elektronischen Akten (z.B. ELAK, elektronischer Personalakt) bzw. in für bestimmte Vollzugsgebiete speziell erstellten Fachanwendungen (z.B. Förderungen) seinen inhaltlichen Niederschlag. Bei diesen Systemen wird weitestgehend technisch sichergestellt, dass wesentliche rechtliche Grundlagen (u.a. das Bundessarchivgesetz) eingehalten werden.

Archivrelevantes Schriftgut liegt daher in der Regel entweder in entsprechend gekennzeichneter Papierform, elektronisch im ELAK oder in für die Archivierung aufbereiteten Datenbeständen von Fachanwendungen vor. Für den ELAK bestehen entsprechende Vorgaben (z.B. Skartierung oder Übertragung an das Österreichische Staatsarchiv), die großteils automationsunterstützt umgesetzt werden.

Folgende Vorschriften finden dabei Anwendung:

- Bundesarchivgesetz, BGBl. I Nr. 162/1999
- Denkmalschutzgesetz, BGBl. Nr. 533/1923
- Bundesarchivgutverordnung, BGBl. II Nr. 367/2002
- Büroordnung 2004
- Datenschutz-Grundverordnung (EU) 2016/679 (DSGVO)
- Datenschutzgesetz (DSG), BGBl. I Nr. 165/1999

Grundlegend festgehalten wird daher, dass Daten, die im Aktensystem ELAK auf Servern hinterlegt sind, nicht mehr durch Benutzerinnen und Benutzer gelöscht werden können.

Zeitgemäßes Arbeiten – v.a. zu komplexen Themenstellungen – verlangt in den meisten Fällen die Zusammenarbeit einer Vielzahl von Expertinnen und Experten sowie Organisationen, sodass im Vorfeld einer tatsächlichen Schriftguterstellung, die letztlich im Aktenwege zu verwalten ist, unterschiedliche Arbeitsversionen und Hilfsdarstellungen erzeugt bzw. benötigt

werden. Diese Hilfsdarstellungen von Expertinnen und Experten stellen sohin in der Regel fragmentarische und z.T. auch wieder verworfene Arbeitsversionen dar, die eben gerade nicht die Grundlage des späteren Verwaltungshandelns bilden.

Im Gegensatz zu den für den Gesetzesvollzug vorgesehenen Schriftgütern, Konzepten und Dokumenten werden diese Hilfsdarstellungen daher auch nicht im Aktensystem, sondern meist auf persönlichen elektronischen Ablagen zusammen mit allgemeinen Dateien (z.B. Texte, Tabellenkalkulationen) gespeichert.

Bei einem Wechsel dieser Speichermedien (z.B. Austausch bzw. Ausscheiden eines Notebooks) bzw. bei einem Benutzer- oder Regierungswechsel wird daher der konkrete Umgang mit den gespeicherten Daten anlassfallbezogen abgestimmt, sodass die Einhaltung rechtlicher Grundlagen (z.B. Bundesarchivgesetz, DSGVO, Informationssicherheitsgesetz, Verträge) im Detail sichergestellt werden kann.

1.2. Systemverwaltete Daten

Systemverwaltete Daten sind für die einwandfreie Funktionsweise von IT-Lösungen und IT-Geräten unerlässlich, erlauben aber in der Regel keinen Zugriff durch die Benutzerinnen und Benutzer. Die Daten selbst sind inhaltlich stets redundant mit originären Daten (z.B. Dokumenten, Eingaben, Schriftstücken) und sind mit systeminternen Informationen wie z.B. Netzadressen, Plattensektoren, Verarbeitungsreihenfolge und Datenbankindices angereichert.

Zu den systemverwalteten Daten gehören auch Sicherungskopien zur Wiederherstellung bei etwaigen Datenverlusten, da diese einem direkten Zugriff durch Benutzerinnen und Benutzer entzogen sind. In modernen Rechenzentren wie z.B. der Bundesrechenzentrum GmbH bilden die systemverwalteten Daten den weitaus überwiegenden Speicheranteil. Diese Daten werden aufgrund der sachlich-inhaltlichen 100-prozentigen Redundanz (da es sich nicht um originäre Daten handelt) nicht dem Österreichischen Staatsarchiv übergeben. Die im Rechenzentrumsbetrieb befindlichen systemverwalteten Daten unterliegen gesonderten hohen Sicherheitsauflagen. Das heißt im Konkreten, dass diese Daten soweit möglich verschlüsselt oder in nicht lesbaren internen Speicherformaten abgespeichert werden und nur von gesondert autorisiertem IT-Personal (Administratoren) gewartet werden können (z.B. Zurücksetzen, Kopieren, Löschen).

Eine besonders sicherheitsrelevante Kategorie von systemverwalteten Daten bilden diejenigen Daten, die Benutzerinnen und Benutzern (nicht IT-Personal) und hausfremden Drittpersonen (z.B. Reinigungspersonal, Handwerker, Lieferanten) dezentral zugänglich sind.

Derartige Daten befinden sich insbesondere auf PCs und Notebooks, Tablets und Smartphones sowie Multifunktionsgeräten.

In diesen Fällen bedarf es deutlich erhöhter sicherheitstechnischer Maßnahmen, um insbesondere die Datensicherheit zu gewährleisten. Aus sicherheitstechnischer Sicht sind dabei grundsätzlich auch potenzielle Angriffs- und Bedrohungsszenarien zu berücksichtigen, beispielsweise durch etwaige Manipulation, bei Verlust, bei Zugang durch unautorisierte Personen oder in Zusammenhang mit Cyberattacken. Es wird daher auch in diesen Fällen durch Klärung der jeweils konkreten Situation mit dem Benutzer oder der Benutzerin eine individuelle Beurteilung einer Bedrohungslage vorgenommen und darauf basierend die entsprechenden Sicherheitsmaßnahmen vereinbart.

Jedenfalls werden die Daten routinemäßig gelöscht, bei entsprechender Beurteilung wird auch individuell mit den Benutzerinnen und Benutzern die Vernichtung des gesamten Speichermediums oder IT-Gerätes erwogen und gegebenen Falles durchgeführt (siehe Löschung von Daten).

Ein Löschen dieser Daten kann softwaretechnisch unter Nutzung entsprechender Programme erfolgen oder durch Vernichtung des Speichermediums bzw. des gesamten IT-Gerätes (Schreddern).

Die internationale Expertendiskussion, insbesondere in Zusammenhang mit der DSGVO, und die einschlägige Fachliteratur zeigen bei der Löschung von Daten durchaus differenzierte Ansätze und Meinungen auf. Klare Position der Lehre ist, dass softwaretechnisches Löschen keine endgültige Vernichtung darstellt und ein Restrisiko einer späteren Lesbarkeit immer bestehen bleibt (vgl. körperlich Vernichten: Oberster Gerichtshof vom 13. September 2012, 6 Ob 107/12x; Artikel im Kurier vom 31. Juli 2019 – Unterschätztes Risiko: Was Drucker verraten).

Dieses Restrisiko steigt insbesondere durch den rasanten technischen Fortschritt – einerseits durch immer leistungsfähigere Instrumente zur Datenwiederherstellung, andererseits im Bereich der verfügbaren Speichervolumina in IT-Geräten. Im letzten Jahrzehnt haben sich die Speicherkapazitäten in IT-Geräten etwa um den Faktor 1.000.000 vergrößert. Daten können sich daher – abhängig von der Art und Menge der Nutzung – über Monate und Jahre in einem Gerät befinden, ohne vom System selbst überschrieben zu werden. Eine endgültige Sicherheit bzw. Vertraulichkeit ist daher nur mittels physischer Vernichtung zu gewährleisten.

1.3. Multifunktionsgeräte

Im gegenständlichen Fokus der Fragen stehen systemverwaltete Daten auf internen Speichern von Multifunktionsgeräten, die in den Kabinetten von Bundeskanzler Kurz und Bundesminister Blümel standen.

Nach den mir vorliegenden Informationen befinden sich auf internen Speichern von Multifunktionsgeräten die erforderlichen temporären Datenkopien, die für die Durchführung des jeweiligen Prozesses (Drucken, Kopieren oder Scannen) erforderlich sind. Auf diese Datenkopien können die Benutzerinnen und Benutzer nicht direkt zugreifen – sie unterliegen daher keiner willentlichen Speicherung, Bearbeitung oder Löschung mit gerätefremder Software. Sohin wäre z.B. ein Speichern von Videos oder ein für forensische Zwecke geeignetes Löschen durch Benutzerinnen oder Benutzer nicht möglich. Da diese (systemverwalteten) Daten lediglich temporäre technische Kopien darstellen, sind sie kein Schriftgut im Sinne des Bundesarchivgesetzes, weshalb dieses auch nicht anwendbar ist. Die Bezeichnung z.B. als Kabinettsarchivalien ist daher nicht korrekt.

Wie oben dargestellt, bilden auch die Daten auf internen Speichern von Multifunktionsgeräten ein Konglomerat aus:

- dienstlichen Daten
- Personaldaten
- persönlichen Daten
- mitunter sensiblen Daten oder
- in besonderen Fällen auch klassifizierten Daten,
- darüber hinaus waren im konkreten Fall auf Grund der Ministerzuständigkeit mutmaßlich auch Sicherheitsdaten (im Zuge von Ausdrucken) gespeichert.

Vor diesem Hintergrund ist die rechtskonforme Behandlung der Daten im Sinne der DSGVO und des Informationssicherheitsgesetzes besonders zu beachten (z.B. "need to know-Prinzip").

Die Bedrohungsintensität bei Kenntniserlangung der Daten durch unbefugte Personen muss aufgrund ihrer inhaltlichen Natur als hoch beurteilt werden. Eine Übergabe der Daten gemäß Bundesarchivgesetz scheidet aus, da es sich um vollständig redundante Daten, also lediglich temporäre technische Kopien handelt. Eine Archivierung der Inhalte kommt bei den Originaldaten (jenen Dateien, für die ein Multifunktionsgerät zum Ausdruck, Kopieren oder Einscannen genutzt wurde) in Frage.

Eine Löschung dieser internen Speicher ist jedenfalls sowohl im Sinne der Datenminimierung (Grundsatz der DSGVO) als auch im Sinne der IT-Sicherheit geboten.

Die physische Vernichtung (Schreddern) der Datenträger aus Multifunktionsgeräten ist nach den mir vorliegenden Informationen ein – basierend auf der individuellen Klärung der Bedrohungsvektoren mit den Benutzerinnen bzw. Benutzern – durchaus üblicher und rechtskonformer Vorgang und unter bestimmten Rahmenbedingungen sogar zwingend.

Die Multifunktionsgeräte im Bundeskanzleramt sind den mir vorliegenden Informationen zufolge in ein internes Drucknetzwerk eingebunden und können grundsätzlich von allen Mitarbeiterinnen und Mitarbeitern angesteuert bzw. genutzt werden, da keine technischen Zugangsbeschränkungen bestehen. Es gibt daher auch keine Multifunktionsgeräte, die explizit bzw. ausschließlich einer bestimmten Organisationseinheit oder Anwenderinnen- oder Anwender-Gruppe zur Verfügung stehen. Beschränkungen können lediglich hinsichtlich der physischen Zutrittsmöglichkeiten zu den Gebäudeabschnitten bestehen, in denen sich u.a. auch Multifunktionsgeräte befinden. In der Praxis werden von den Mitarbeiterinnen und Mitarbeitern des Bundeskanzleramtes jene Multifunktionsgeräte genutzt, die dem jeweiligen Arbeitsplatz räumlich am nächsten liegen.

2. Spezifische technisch-organisatorische Themenstellungen im Bereich IKT für einen Regierungswechsel Zug-um-Zug

Im Fokus der Betrachtung steht der Zeitraum von 20. Mai bis 3. Juni 2019. Im Gegensatz zum üblichen Ablauf bei Regierungswechseln (z.B. nach Neuwahlen) war die Vorbereitungszeit – neben Feiertagen und Wochenenden – für technische und organisatorische Maßnahmen auf rund 2 Arbeitswochen begrenzt.

<u>Retrospektive auf den politischen Ablauf in diesem Zeitraum:</u>

- Misstrauensvotum gegen den damaligen Bundeskanzler Kurz steht im Raum
- Ausweitung des Misstrauensvotums gegen die gesamte Bundesregierung steht im Raum
- Erfolgreiches Misstrauensvotum im Nationalrat
- Bundespräsident enthebt Bundesregierung
- Bundespräsident betraut Bundesregierung (kurzfristig)
- Bundespräsident stellt die zukünftige Bundeskanzlerin Bierlein vor und beauftragt diese mit der Bildung einer Expertenregierung
- Zukünftige Bundeskanzlerin Bierlein stellt das Experten-Ministerkabinett vor
- Expertenregierung wird vom Bundespräsidenten angelobt
- Bildung der internen Büros und Kabinette

Um unter den Rahmenbedingungen des dargestellten Zeitablaufes und Zeitdruckes die erforderlichen technischen und organisatorischen Vorbereitungsmaßnahmen zu treffen, war

nach den mir vorliegenden Informationen die IKT des Hauses mit enormen Herausforderungen in inhaltlicher, personeller und zeitlicher Hinsicht konfrontiert.

Trotz dieser Umstände, insbesondere hinsichtlich eines konkreten zeitlichen und inhaltlichen Ausgangs des Misstrauensvotums, waren für den Fall des Aussprechens des Misstrauens durch den Nationalrat rechtzeitig alle Vorbereitungen für einen umgehenden Wechsel ZUG-UM-ZUG (Abgang der bisherigen Regierungsmitglieder samt Kabinetten und Einzug bzw. Arbeitsaufnahme der neuen Regierungsmitglieder samt Kabinetten) zu treffen.

Betroffen davon waren v.a. Maßnahmen in Zusammenhang mit Räumlichkeiten, der Rücknahme und Ausgabe individueller Geräteausstattungen (Notebooks, Telefone), der Rückgabe und Neuausstellung von Dienstausweisen, das Entziehen und die Neuvergabe von Berechtigungen, die Archivierungen und etwaige Löschung von persönlichen Daten sowie Parkmöglichkeiten.

In all diesen Fällen war insbesondere auch die IKT-Gruppe des Hauses technisch und organisatorisch mit Aufgaben und Leistungen gefordert bzw. war in die Bewältigung dieser Aufgabenstellungen involviert. Eine besondere Herausforderung stellte dabei die Gewährleistung der im Rahmen der IKT vielfältigen und komplexen Sicherheitsaspekte dar. Zu diesem Zwecke war es zwingend erforderlich – über Abteilungsgrenzen hinweg – u.a. mit hausinterner IT, Cybersicherheit, Informationssicherheit, Personalmanagement, Datenschutz und Gebäudemanagement abgestimmt zu handeln.

Nach den mir vorliegenden Informationen wurde vor dem Hintergrund der zeitlichen Herausforderungen diese Koordinationsaufgabe unmittelbar von der Gruppenleitung I/C wahrgenommen bzw. wurde seitens der Gruppenleitung I/C direkt mit Mitarbeiterinnen und Mitarbeitern unterschiedlicher Abteilungen u.a. im Rahmen einer Taskforce zusammengearbeitet.

Bei den vom Wechsel unmittelbar betroffenen Bereichen und Personen wurden insbesondere auch unter Berücksichtigung des Zeitdruckes von der IKT möglichst Standardprozesse zur Anwendung gebracht bzw. deren Anwendung empfohlen und mit dem in den Kabinetten von Bundeskanzler Kurz und Bundesminister Blümel für IT-Koordination und Sicherheitsfragen zuständigen Kabinettsmitglied besprochen.

Hinsichtlich der Rückgabe der individuellen Ausstattungen wurde nach den mir vorliegenden Informationen grundsätzlich eine umfangreiche und detaillierte Ausarbeitung von der IKT schriftlich zur Verfügung gestellt.

In diesem Zusammenhang wurde daher auch das Vorgehen mit den gegenständlich relevanten Multifunktionsgeräten in den Räumlichkeiten der Kabinette von Bundeskanzler Kurz und Bundesminister Blümel behandelt.

Die einzelnen Fragen beantworte ich nach den mir von den zuständigen Organisationseinheiten des Bundeskanzleramtes bereitgestellten Informationen wie folgt:

Zu Frage 1:

- *Wann genau und durch wen erfuhren Sie von der "Schredder-Aktion" des Kurz Mitarbeiters?*

Vom konkreten, in der Frage angesprochenen Sachverhalt habe ich aus der medialen Berichterstattung erfahren.

Zu Frage 2:

- *Wie ist der Name des Mitarbeiters, der die Festplatte vernichten ließ?*

Ich ersuche um Verständnis, diese Frage aus Gründen des Datenschutzes nicht beantworten zu können.

Zu den Fragen 3, 4, 5, 7 und 9:

- *Seit wann und wie lange war diese Person in welcher Position im Bundeskanzleramt tätig?*
- *War der Mitarbeiter (auch) im Kabinett des Bundeskanzlers beschäftigt?*
- *Wie lange war der Mitarbeiter im BKA beschäftigt?*
- *Wo ist der Mitarbeiter ab 23. Mai 2019 im BKA tätig gewesen?*
- *Welches Aufgabenprofil hatte dieser Mitarbeiter genau im BKA?*

Nach den mir vorliegenden Informationen war der Mitarbeiter in der Zeit von 19. Dezember 2017 bis 3. Juni 2019 im Kabinett meines Amtsvorgängers und als Referent in der Abteilung „Social Media" tätig. Er war für die Betreuung der Social-Media-Kanäle, der Produktion und Erstellung von Livestreams, der Erstellung von Reportagefilmen und -fotografien sowie für die Erstellung von Animationen und Grafiken zuständig.

Zu den Fragen 6 und 8:

- *Wann wechselte der Mitarbeiter zur ÖVP?*
- *Wo ist der Mitarbeiter zum Zeitpunkt der Anfragebeantwortung tätig?*

Ich ersuche um Verständnis, dass ressortfremde Tätigkeiten keinen Gegenstand der Vollziehung des Bundeskanzleramtes betreffen und somit nicht dem parlamentarischen Interpellationsrecht unterliegen.

Zu den Frage 10, 11, 16, 17, 18 und 24:

- *Wann wurde von wem die Entscheidung getroffen die Festplatte vernichten zu lassen und aus welchen Erwägungen wurde dies entschieden?*
- *Auf wessen Anordnung oder mit wessen Genehmigung wurde die Festplatte vernichtet?*
- *Wenn es sich, wie seitens der ÖVP kommuniziert, beim Schreddern der Festplatte um einen "üblichen Vorgang" handelt, warum wurde die Festplatte dann nicht offiziell seitens des BKA einer Vernichtung zugeführt?*
- *Wurde eine Vernichtung seitens des BKA selbst erwogen?*
  a. *Wenn ja, warum entschied man sich gegen eine Vernichtung seitens des BKA selbst?*
  b. *Wenn nein, warum segneten die Vorgesetzten des Mitarbeiters die Vernichtung auf privatem Wege ab?*
- *Laut Kurier wurde die Vernichtung von den Vorgesetzten abgesegnet. Laut Standard sagte Kanzler Kurz, der Mitarbeiter habe zwar "schlampig agiert", sich aber mittlerweile entschuldigt – und die offene Rechnung beglichen. Was stimmt nun? Wurde die Vernichtung von dessen Vorgesetzten abgesegnet oder hat er „schlampig agiert" und auf eigene Faust agiert?*
- *Weswegen wurden die Festplatte nicht wie sonst üblich von der BKA IT-Abteilung auf offiziellem Weg vernichtet?*

Nach den mir vorliegenden Informationen sind Amtsübergaben nach einer Wahl und den darauffolgenden Regierungsverhandlungen üblicherweise zeitlich einschätzbar, sodass deren Abwicklung Wochen bzw. Monate im Voraus geplant, vorbereitet und durchgeführt werden kann. In derartigen Fällen wird der Ausbau der Festspeicherplatten durch den Leasinggeber der Multifunktionsgeräte im Beisein von internem IT-Personal der Gruppe I/C und die anschließende Vernichtung im Zentralen Ausweichsystem des Bundes (ZAS) in St. Johann im Pongau vorgenommen. Eine Vernichtung durch externe Dienstleister wurde in diesem Zusammenhang immer wieder erwogen, da dies in der Informationstechnologie ein übliches Vorgehen darstellt.

Die Amtsübergabe hat, wie unter Punkt 2. der einleitend aufbereiteten Grundlagen dargestellt, unter besonderen Umständen stattgefunden. Vor diesem Hintergrund musste nach den mir vorliegenden Informationen rasch mit den Vorbereitungsarbeiten für eine vollständige Amtsübergabe begonnen werden. Dafür wurden Verantwortliche bestimmt, insbesondere auch ein verantwortlicher Mitarbeiter für die Kabinette von Bundeskanzler Kurz und Bundesminister Blümel.

Den mir vorliegenden Informationen entnehme ich, dass im Rahmen der üblichen Arbeitsabläufe sodann, wie eingangs ausgeführt, eine physische Vernichtung der internen Speicher aus den Multifunktionsgeräten als eine mögliche, in der Vergangenheit bereits praktizierte Variante zur bestmöglichen Wahrung der Vertraulichkeit und Sicherheit von Daten zwischen dem Leiter der Gruppe I/C und dem verantwortlichen Mitarbeiter für die beiden Kabinette besprochen wurde. Letzterer hat sich nach Erörterung der aus seiner Sicht vorliegenden Datensensibilität für die Option der physischen Vernichtung entschieden.

Nach den mir vorliegenden Informationen wurden nach dem planmäßigen Ausbau der internen Speicher der Multifunktionsgeräte dem verantwortlichen Kabinettsmitarbeiter die Speichermedien vom anwesenden Personal der Gruppe I/C ausgehändigt. Da die Zeit für den standardisierten Ablauf im ZAS zur Vernichtung der Festspeicherplatten nicht ausreichend war, hat der verantwortliche Kabinettsmitarbeiter in Folge den Gruppenleiter I/C telefonisch darüber informiert, dass entgegen der ursprünglichen Planung die Vernichtung der Festspeicherplatten nicht durch hausinternes IT-Personal und nicht im Wege des ZAS zu erfolgen hat. Die Festspeicherplatten wurden vom verantwortlichen Kabinettsmitarbeiter in Folge einem Mitarbeiter der Social Media Abteilung übergeben, der die Vernichtung bei einem externen Dienstleister veranlasst hat. Die zerstörten Speichermedien wurden vom zuständigen Kabinettsmitarbeiter der Gruppenleitung I/C übergeben und sind derzeit bis zur endgültigen Entsorgung sicher in der Abteilung I/9 des Bundeskanzleramtes verwahrt.

Zu Frage 12:

- *Welche Vorgesetzten des Mitarbeiters waren von dieser Absicht im Vorhinein informiert (sofern keine konkreten Namen genannt werden können bitte um exakte Angabe des Postens und der Bewertung innerhalb des BKA)?*

Es darf auf die Beantwortung der Fragen 10, 11, 16, 17, 18 und 24 verwiesen werden.

Zu Frage 13:

- *Wer im BKA hatte sonst noch Kenntnis von der Vernichtung der Festplatte (sofern keine konkreten Namen genannt werden können bitte um exakte Angabe des Postens und der Bewertung innerhalb des BKA)?*

Über die durchgeführte externe Vernichtung der internen Speicher wurden nach den mir vorliegenden Informationen neben den unter Frage 11 genannten Personen noch der Leiter der Sektion I, der Leiter der Gruppe I/B, der Leiter der Abteilung I/9 sowie weitere Mitarbeiterinnen und Mitarbeiter dieser Abteilung in Kenntnis gesetzt.

Zu Frage 14:

- *Wurde dem Mitarbeiter angeordnet, die Festplatte unter Angabe eines falschen Namens schreddern zu lassen?*
  a. *Wenn nein, waren die Vorgesetzten von dieser Vorgehensweise informiert?*
  b. *Wenn Vorgesetzte davon informiert waren, aus welchem Grund haben sie dem zugestimmt?*

Weder eine derartige Anordnung noch eine entsprechende Information sind bekannt.

Zu Frage 15:

- *Wurde die, laut Kurier mittlerweile beglichene, Rechnung vom BKA bezahlt?*
  a. Wenn nein, von wem wurde die Rechnung bezahlt?
  b. Wenn ja, weshalb wurde die Rechnung vom BKA bezahlt?

Ich ersuche um Verständnis, dass die Frage, von wem die Rechnung bezahlt wurde, nicht Gegenstand der Vollziehung ist; sie wurde jedenfalls nicht vom Bundeskanzleramt beglichen.

Zu den Fragen 19 und 38:

- *In wessen Eigentum befand sich Festplatte?*
- *Welchen Wert hatte die Festplatte?*

Nach den mir vorliegenden Informationen wurden die gegenständlichen Multifunktionsgeräte, die in den Räumlichkeiten der Kabinette von Bundeskanzler Kurz und Bundesministers Blümel aufgestellt waren, geleast und befanden sich dementsprechend nicht in Bundeseigentum.

Die internen Speicher wurden durch den beim Dienstleister im Betrachtungszeitraum beauftragten Ausbau in das Eigentum des Bundes übergeführt. Der Wert eines Speichermediums bei Neuanschaffung ist mit rd. 600 Euro (inkl. USt.) festzusetzen.

Zu den Fragen 20, 21, 22 und 39:

- *Laut Kurier hieß es seitens der ÖVP, es sei "nicht die Absicht des Mitarbeiters gewesen, nicht rechtskonform zu handeln". Die Vernichtung wurde jedoch laut diesem Bericht auch von Vorgesetzten abgesegnet. War irgendeiner der beteiligten Personen im BKA bzw dem BKA bewusst, dass es sich bei der mechanischen Vernichtung einer im Eigentum des Bundes stehenden Sache möglicherweise um eine Straftat handelt?*
- *Wurde eine Schadenersatzforderung gegen den betroffenen Mitarbeiter gerichtet?*
  a. Wenn nein, warum nicht?
- *Wurden oder werden disziplinarrechtliche Schritte gegen den betroffenen Mitarbeiter oder die die Vorgehensweise genehmigenden Vorgesetzten eingeleitet?*

a. Wenn ja, welche Schritte wurden eingeleitet?
b. Wenn nein, warum nicht?

- *Wurde diese Causa auch vom BKA zur Anzeige gebracht?*
  a. Wenn ja, wann, durch wen und bei welcher Behörde?

Wie bereits mehrfach ausgeführt und speziell unter den Punkten 1.2. und 1.3. der einleitend aufbereitenden Grundlagen dargelegt, ist die Vernichtung von bestimmten Festplatten unter bestimmten Umständen ein rechtskonformer Vorgang, der auch in der Vergangenheit wiederholt praktiziert wurde. Der spezifische Vorgang ist Gegenstand eines strafrechtlichen Ermittlungsverfahrens, weshalb keine der angeführten Schritte bis dato notwendig waren.

Zu Frage 23:

- *Welche Informationen hat das BKA hinsichtlich der Frage weshalb die Festplatte vernichtet wurde (um detaillierte Erläuterung wird ersucht)?*

Es darf auf die unter Punkt 1.2. der einleitend aufbereiteten Grundlagen hinsichtlich system-verwalteter Daten und im Konkreten auf den Umgang mit diesen auf Multifunktionsgeräten (vgl. Punkt 1.3.) verwiesen werden.

Zu Frage 25:

- *Wurde jemals zuvor im BKA die mechanische Vernichtung einer Festplatte von einem Mitarbeiter unter Angabe eines falschen Namens durchgeführt?*
  a. Wenn ja, wann und wie oft kam das vor?

Derartige Vorgänge sind nicht evident.

Zu Frage 26:

- *Wie lauten BKA-internen Regeln zur Vernichtung von Akten, Schriftstücken und digitalen Datenträgern (um detaillierte Erläuterung wird ersucht)?*

Es darf auf die einleitend aufbereiteten Grundlagen zur Behandlung von Daten und auf die erforderliche Differenzierung zwischen Akten, Schriftstücken und digitalen Datenträgern verwiesen werden.

Mit Bezug auf die Ausführungen in den Punkten 1.1., 1.2. und 1.3. der einleitend aufbereiteten Grundlagen darf an dieser Stelle festgehalten werden, dass sich auf den internen Speichern von Multifunktionsgeräten temporäre Daten und kein Schriftgut im Sinne des Bundesarchivgesetzes befinden, weshalb dieses auch nicht anwendbar ist. Daher ist eine

Löschung dieser internen Speicher sowohl im Sinne der Datenminimierung (Grundsatz der DSGVO) als auch im Sinne der IT-Sicherheit geboten.

Akten dienen der Dokumentation des Verwaltungshandelns. Akten dürfen nur gemäß der Skartierungsfrist (nach mindestens 10 Jahren) ausgesondert werden (vgl. § 25 und § 26 Büroordnung 2004). Diese Regeln gelten für die gesamte Bundesverwaltung.

Schriftstücke, die nicht Teil von Akten sind (z.B. Entwürfe, Notizen, Kopien), können von den Sachbearbeiterinnen und Sachbearbeitern selbst gelöscht werden.

Sofern ein elektronischer Akt bzw. ein physisches Geschäftsstück als nicht archivwürdiges Schriftgut nach der Verordnung der Bundesregierung BGBl. II Nr. 366/2002 gilt, kann von einer Verständigung des Österreichischen Staatsarchivs abgesehen werden.

Digitale Datenträger werden nach den mir vorliegenden Informationen dann einer Vernichtung zugeführt, wenn diese nicht mehr funktionsfähig sind, oder – im Falle von Multifunktionsgeräten – um sicherzustellen, dass Daten nachvollziehbar nicht mehr von diesen Datenträgern ausgelesen werden können.

Zu Frage 27:

- *Inwiefern war die Vorgehensweise des Mitarbeiters gerechtfertigt (um detaillierte Erläuterung unter dem Gesichtspunkt des Abgehens von der "Üblichen Vorgehensweise" wird ersucht)?*

Insofern darf auf das anhängige strafrechtliche Ermittlungsverfahren verwiesen werden.

Zu Frage 28:

- *Inwiefern entsprechen diese internen Regeln dem § 6 Abs 3 des Bundesarchivgesetzes, wonach Kabinettsarchivalien entweder dem Staatsarchiv übergeben werden müssen oder im Ressort zu verbleiben haben (um detaillierte Erläuterung wird ersucht)?*
  - *a. Inwiefern entspricht die Vernichtung der Festplatte durch den Mitarbeiter dieser Bestimmung des Bundesarchivgesetzes?*

Es darf auf die einleitend aufbereiteten Grundlagen zur Behandlung von Daten und vor allem auf die erforderliche Differenzierung zwischen Akten, Schriftstücken und digitalen Datenträgern verwiesen werden.

Mit Bezug auf die Ausführungen zu Punkt 1.3. der einleitend aufbereiteten Grundlagen darf an dieser Stelle nochmals festgehalten werden, dass sich auf den internen Speichern von Multifunktionsgeräten temporäre Daten und kein Schriftgut im Sinne des

Bundesarchivgesetzes befinden, weshalb dieses auch nicht anwendbar ist. Die Bezeichnung z.B. als Kabinettsarchivalien ist daher nicht zutreffend.

Zu Frage 29:

- *In welchen Fällen werden Akten, Schriftstücke und digitalen Datenträger im BKA "üblicherweise" vernichtet?*

Es darf auf die einleitend aufbereiteten Grundlagen zur Behandlung von Daten, auf die erforderliche Differenzierung zwischen Akten, Schriftstücken und digitalen Datenträgern und die Ausführungen zu Frage 26 verwiesen werden.

Wie in den einleitend aufbereiteten Grundlagen unter Punkt 1. festgehalten worden ist, werden Datenträger wie z.B. Festplatten (PCs, Laptops, Server, Multifunktionsgeräte) oder USB-Sticks nach den mir vorliegenden Informationen seit Frühjahr 2015 grundsätzlich einer Vernichtung im Wege des Bundeskanzleramtes – ZAS zugeführt.

Zu Frage 30:

- *Ist es üblich, dass Akten, Schriftstücke und digitalen Datenträger im BKA bei "Regierungswechseln" vernichtet werden?*
  a. *Inwiefern entspricht diese Vorgehensweise dem § 6 Abs 3 des Bundesarchivgesetzes, wonach Kabinettsarchivalien entweder dem Staatsarchiv übergeben werden müssen oder im Ressort zu verbleiben haben (um detaillierte Erläuterung wird ersucht)?*

Nach den mir vorliegenden Informationen handelte es sich bei den vernichteten internen Speichern der Multifunktionsgeräte nicht um Kabinettsarchivalien, die dem Bundesarchivgesetz unterliegen.

Es darf auf die einleitend aufbereiteten Grundlagen zur Behandlung von Daten, auf die erforderliche Differenzierung zwischen Akten, Schriftstücken und digitalen Datenträgern und die Ausführungen zu Frage 26 verwiesen werden.

Nach den mir vorliegenden Informationen ist bei nicht dem Bundesarchivgesetz unterliegenden Daten das Löschen von Datenträgern bzw. die Neuinstallation bzw. das Neuaufsetzen von Geräten bei Regierungswechseln ein üblicher Vorgang.

Zu Frage 31:

- *In welchem Umfang und Ausmaß wurden bei Regierungswechseln der letzten 5 Jahre Akten, Schriftstücke und digitalen Datenträger im BKA vernichtet (um eine annäherungsweise Beschreibung der Vorgänge wird ersucht)?*

Es darf auf die einleitend aufbereiteten Grundlagen zur Behandlung von Daten, auf die erforderliche Differenzierung zwischen Akten, Schriftstücken und digitalen Datenträgern sowie auf die Beantwortung der Fragen 33 und 34 verwiesen werden.

Eine generelle Überwachung aller Tätigkeiten der Mitarbeiterinnen und Mitarbeiter (inkl. E-Mails) durch die IKT ist gemäß den §§ 79c ff Beamtendienstrechtsgesetz 1979 verboten. Da eine Nutzung der IKT-Infrastruktur im eingeschränkten Ausmaß für private Zwecke erlaubt ist, würde eine derartige Überwachung bzw. Nachschau ohne gerichtlichen Auftrag auch der DSGVO widersprechen. Technisch ist dazu festzuhalten, dass ein Audit Log auf den Mailboxen aus obigen Gründen nicht aktiv ist. Daher darf und kann auch keine Aussage erfolgen, welche E-Mails von Nutzern gelöscht wurden.

Zu Frage 32:

- *Wurde bei Regierungswechseln der letzten 5 Jahre Akten, Schriftstücke und digitalen Datenträger im BKA entgegen den Bestimmungen (insbesondere des § 6 Abs 3) des Bundesarchivgesetzes vernichtet?*
  a. Wenn ja, wann auf wessen Anordnung und in welchem Ausmaß?

Nach den mir vorliegenden Informationen kann davon ausgegangen werden, dass kein dem Bundesarchivgesetz unterliegendes Schriftgut vernichtet wurde. Auf die Ausführungen in den einleitend aufbereiteten Grundlagen, dass die internen Speicher von Multifunktionsgeräten nicht dem Bundesarchivgesetz unterliegen, wird verwiesen. Es darf ergänzt werden, dass sich die Frage der Anwendbarkeit des Bundesarchivgesetzes stets auf das Original bezieht und es sich bei den vernichteten Daten lediglich um temporäre technische Kopien handelte.

Bei einem obersten Organ bzw. dessen unmittelbaren Mitarbeiterinnen und Mitarbeitern fällt erfahrungsgemäß eine Vielzahl von persönlichen Aufzeichnungen im Sinne des § 2 Z 2 des Bundesarchivgesetzes an. Dieses Schriftgut fällt nicht unter das Bundesarchivgesetz und kann somit zu jeder Zeit von den Betroffenen vernichtet werden, auch bereits vor dem Ausscheiden aus der Funktion.

Alle in elektronischen Aktensystemen (z.B. ELAK) erfassten Schriftstücke fallen nicht unter die persönlichen Aufzeichnungen, da von der Funktion dieses Systems diese Schriftstücke als amtliche gelten und somit vom Bundesarchivgesetz umfasst sind.

Zu den Fragen 33 und 34

- *Inwiefern wurde das Staatsarchiv im Zuge der Regierungswechsel der letzten 5 Jahre zur fachkundigen Begleitung des Aktenüberganges einbezogen?*
- *Wurde das Staatsarchiv überhaupt im Vorfeld von Regierungswechseln einbezogen?*
  a. Wenn ja, inwiefern?
  b. Wenn nein, weshalb nicht?

Entsprechend der Bestimmung des § 6 Abs. 3 des Bundesarchivgesetzes ist das Schriftgut, das unmittelbar beim Bundeskanzler in Ausübung der Funktion oder in den politischen Büros anfällt und nicht beim Nachfolger verbleiben soll, nach dem Ausscheiden aus der Funktion dem Österreichischen Staatsarchiv zu übergeben. Daher ist davon auszugehen, dass das Österreichische Staatsarchiv im Zuge von Regierungswechseln regelmäßig miteinbezogen worden ist.

Zu Frage 35:

- *Wo genau befindet sich jener Drucker in dem die Festplatte verbaut war?*

Die anfragegegenständlichen Multifunktionsgeräte befinden sich am Ballhausplatz 2, 1. Stock, im Bereich der Kabinette.

Zu Frage 36:

- *Welche Organisationseinheiten des BKA hatten Zugriff auf diesen Drucker und welche Personen und Organisationseinheiten druckten darauf üblicherweise?*

Es darf auf die unter Punkt 1.3. der einleitend aufbereiteten Grundlagen hinsichtlich der Netzwerkeinbindung der Multifunktionsgeräte und der Nutzungsmöglichkeit der Multifunktionsgeräte durch alle Bediensteten des Bundeskanzleramtes verwiesen werden. Wie zu diesem Punkt ausgeführt, werden in der Praxis von den Mitarbeiterinnen und Mitarbeitern des Bundeskanzleramtes jene Multifunktionsgeräte genutzt, die dem jeweiligen Arbeitsplatz räumlich am nächsten liegen.

Zu Frage 37:

- *Wurden auf dem Drucker auch "private" (im Sinne von "nicht behördliche") Dokumente gedruckt?*
  a. Wenn ja, von wem und in welchem Ausmaß?
  b. Wenn ja, ist dies zulässig (um detaillierte Erläuterung wird ersucht)?

Es darf auf die Ausführungen unter Punkt 1. der einleitend aufbereiteten Grundlagen verwiesen werden (vgl. auch Punkt 1.1. in Verbindung mit BGBl. II Nr. 281/2009).

Zu Frage 40:

- *Werden regelmäßig Festplatten im Eigentum des BKA vernichtet?*
  a. *Wenn ja, wie viele Festplatten aus dem Eigentum des BKA wurden seit 1.1.2017 vernichtet?*
  b. *Wenn nein, wie werden Festplatten im BKA üblicherweise behandelt, wenn die Daten vernichtet werden sollen?*

Nach den mir vorliegenden Informationen werden regelmäßig Festplatten vernichtet. Seit 1. Jänner 2017 wurden 371 Festplatten für das Bundeskanzleramt, das Österreichische Staatsarchiv und die Verwaltungsakademie des Bundes im ZAS vernichtet.

Zu Frage 41:

- *Wurde die BKA IT-Abteilung im Zeitraum zwischen 15.5. und 5.6.2019 angewiesen, Festplatten und andere Datenträger aus IT-Geräten auszubauen und zu vernichten bzw sich für solche Tätigkeiten "bereit" zu halten?*
  a. *Wenn ja, auf wessen Anordnungen und Bewilligung geschah dies jeweils?*
  b. *Aus welchen Geräten, welcher Benutzer stammten diese Festplatten bzw Datenträger jeweils?*
  c. *Aus welchem präzisen Grund wurden diese Datenträger jeweils ausgebaut, gelöscht oder vernichtet?*
     i. *Wie viele Festplatten wurden in dem Zeitraum im BKA aus den Geräten ausgebaut?*
     ii. *Wie viele Festplatten wurden in dem Zeitraum im BKA vernichtet?*
     iii. *Wie viele Festplatten wurden in dem Zeitraum im BKA fachkundig gelöscht?*
  d. *Wie wurde sichergestellt, dass sich auf diesen Datenträgern keine Dokumente befanden, deren Übergabe richtigerweise an das Staatsarchiv erfolgen hätte müssen?*

Es darf grundsätzlich auf die unter Punkt 2. beschriebenen Informationen verwiesen werden. Die (vom Leasinggeber) ausgebauten internen Speicher stammten aus Multifunktionsgeräten. Es gibt keine Zuordnung von bestimmten Benutzerinnen und Benutzern zu Multifunktionsgeräten – in diesem Zusammenhang darf auf die detaillierten Ausführungen unter Punkt 1.3. verwiesen werden; jede Benutzerin bzw. jeder Benutzer kann auf jedem Multifunktionsgerät des Hauses ausdrucken.

Am 21. Mai wurden zunächst 34 Festplatten, wie sie regelmäßig zur Vernichtung anfallen (defekte Festplatten bzw. solche aus Altsystemen oder ausgedienten Serverinfrastrukturen), im Wege der üblichen Routinen im ZAS vernichtet. Danach wurden 7 interne Speicher aus Multifunktionsgeräten ausgebaut. Aufgrund der individuellen Beurteilung der Datensensibilität wurden zum einen 5 interne Speicher ausgebaut und, wie bereits ausgeführt, dem verantwortlichen Kabinettsmitarbeiter ausgehändigt; zum anderen wurde ein

Speichermedium für eine allfällige spätere Wiederverwendung vorbereitet und ein weiteres Speichermedium im Juli im ZAS vernichtet.

Die Sicherstellung, dass keine Dokumente, die dem Österreichischen Staatsarchiv zu übergeben sind, enthalten sind, obliegt den jeweiligen Mitarbeiterinnen und Mitarbeitern selbst, die an die Rechtsvorschriften gebunden sind. Durch die IT erfolgt keine weitere inhaltliche Prüfung der Datenträger. Es darf grundsätzlich auf die unter den Punkten 1.1. bzw. 1.2. der einleitend aufbereiteten Grundlagen hinsichtlich benutzerverwalteter bzw. systemverwalteter Daten verwiesen werden.

Zu Frage 42:

- *Hat das BKA Informationen darüber, ob zwischen 15.5 und 5.6 2019 andere Akten, Schriftstücke oder digitale Datenträger außerhalb des oben beschriebenen "üblichen" Weges in Entsprechung der BKA-internen Regelungen vernichtet wurden?*
  a. *Wenn ja, welche Akten, Schriftstücke oder digitalen Datenträger wann und durch wen auf wessen Auftrag?*

Nein, es liegen keine Informationen darüber vor.

Zu Frage 43:

- *Werden Festplatten und andere digitale Datenträger des BKA üblicherweise auch fachkundig gelöscht, um diese nicht jedesmal vernichten zu müssen (um detaillierte Erläuterung wird ersucht)?*

Es darf auf die Punkte 1.1. bzw. 1.2. der einleitend aufbereiteten Grundlagen hinsichtlich benutzerverwalteter bzw. systemverwalteter Daten verwiesen werden.

Bei Übergaben von Geräten (z.B. Laptop) im Sachgüteraustauschverfahren werden die Festplatten fachkundig mittels einer Spezialsoftware gelöscht. Wenn diese Geräte im Haus verbleiben, werden diese neu installiert oder auf die Werkseinstellungen zurückgesetzt.

Zu Frage 44:

- *Welches Unternehmen ist mit der Vernichtung von Akten, Schriftstücken und digitalen Datenträgern des BKA beauftragt?*
  a. *Seit wann ist dieses Unternehmen mit dieser Aufgabe betraut?*
  b. *Welche Kosten waren mit diesem Auftrag seit 1.1.2017 verbunden (um Angabe der Kosten pro Jahr wird ersucht)?*

Es darf auf die Beantwortung von Frage 26 verwiesen werden.

Nach den mir vorliegenden Informationen werden Datenträger bis zu einer bestimmten physischen Größe im Bundeskanzleramt selbst (im Wege des ZAS) vernichtet. Größere Einheiten, wie z.B. ein Notebook oder Smartphones, deren Akku nicht herausnehmbar ist, müssen aus Sicherheitsgründen außer Haus vernichtet werden. Mit der Vernichtung wurde das Unternehmen Reisswolf Österreich GmbH beauftragt.

Im Jahr 2019 wurden nach den mir vorliegenden Informationen vom Bundeskanzleramt 2 Aufträge über die Vernichtung von Datenträgern (1 Laptop und 2 Handys) in der Gesamthöhe von 91,58 Euro an das Unternehmen Reisswolf Österreich GmbH vergeben; für die Jahre 2017 und 2018 sind keine Aufträge vergeben worden.

Zu Frage 45:

- *Wurde das Staatsarchiv in die Vernichtung eingebunden?*

Es darf auf die einleitend aufbereiteten Grundlagen zur Behandlung von Daten, auf die erforderliche Differenzierung zwischen Akten, Schriftstücken und digitalen Datenträgern und die Beantwortung der Frage 26 verwiesen werden.

Zu den Fragen 46 bis 51:

- *Hat das BKA Anhaltspunkte dafür, dass auf der Festplatte Daten in Bezug zur Ibiza-Affäre gespeichert waren?*
  a. Wenn ja, welche Informationen hat das BKA diesbezüglich?
- *Hat das BKA Anhaltspunkte dafür, dass auf der Festplatte Daten in Bezug Parteienfinanzierung gespeichert waren?*
  a. Wenn ja, welche Informationen hat das BKA diesbezüglich?
- *Hat das BKA Anhaltspunkte dafür, dass auf der Festplatte Daten in Bezug auf das Ende der ÖVP/FPÖ Koalition gespeichert waren?*
  a. Wenn ja, welche Informationen hat das BKA diesbezüglich?
- *Hat das BKA Anhaltspunkte dafür, dass auf der Festplatte Daten in Bezug auf die Entlassung von Bundesminister_innen gespeichert waren?*
  a. Wenn ja, welche Informationen hat das BKA diesbezüglich?
- *Hat das BKA Anhaltspunkte dafür, dass auf der Festplatte Daten in Bezug auf den Rücktritt von Bundesminister_innen gespeichert waren?*
  a. Wenn ja, welche Informationen hat das BKA diesbezüglich?
- *Hat das BKA Anhaltspunkte dafür, dass auf der Festplatte Daten in Bezug auf "neue" oder "anzugelobende" Bundesminister_innen gespeichert waren?*
  a. Wenn ja, welche Informationen hat das BKA diesbezüglich?

Es darf auf die Beantwortung der parlamentarischen Anfrage Nr. 4017/J vom 22. Juli 2019 durch den Vizekanzler und Bundesminister für Verfassung, Reformen, Deregulierung und Justiz verwiesen werden.

Zu Frage 52:

- *Welche sonstigen Informationen hat das BKA in Bezug auf den Inhalt jener Daten, die auf der Festplatte gespeichert waren?*

Es darf auf die einleitend aufbereiteten Grundlagen und im Konkreten auf die Punkte 1.2. und 1.3. hinsichtlich systemverwalteter Daten bzw. Daten auf Multifunktions-geräten verwiesen werden.

Dr. Brigitte Bierlein

REPUBLIK ÖSTERREICH BUNDESKANZLERAMT AMTSSIGNATUR	Unterzeichner	serialNumber=932783133,CN=Bundeskanzleramt,C=AT
	Datum/Zeit	2019-08-26T14:30:00+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.bka.gv.at/verifizierung
	Hinweis	Dieses Dokument wurde amtssigniert.

REPUBLIK ÖSTERREICH Parlamentsdirektion SIEGEL	**Unterzeichner**	Parlamentsdirektion
	Datum/Zeit-UTC	2019-08-28T10:32:40+02:00
	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.	