

 **Bundeskanzleramt**

Bundesminister für EU,  
Kunst, Kultur und Medien

[bundeskanzleramt.gv.at](http://bundeskanzleramt.gv.at)

**Mag. Alexander Schallenberg**  
Bundesminister für EU, Kunst, Kultur und Medien

Herrn  
Mag. Wolfgang Sobotka  
Präsident des Nationalrats  
Parlament  
1017 Wien

Geschäftszahl: BKA-353.120/0074-IIM/2019

Wien, am 26. August 2019

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Dr. Pilz, Kolleginnen und Kollegen haben am 25. Juli 2019 unter der Nr. **4053/J** an mich eine schriftliche parlamentarische Anfrage betreffend „Schreddern für Kurz“ 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<sup>1</sup>
- mitunter sensiblen Daten oder
- in besonderen Fällen auch klassifizierten Daten.

---

<sup>1</sup> 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 gekennzeichnete 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.

#### 1.1. 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.

## 1.2. 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. Sogar 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.

## 1. 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.

### Retrospektive auf den politischen Ablauf in diesem Zeitraum:

- 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 Dienstaussweisen, 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 vorliegenden Informationen wie folgt:

**Zu Frage 1:**

- *Wer hat M. den Auftrag zum Ausbau der Festplatten und zu deren Vernichtung erteilt?*

Ich darf auf die Beantwortung der Frage 3 der parlamentarischen Anfrage Nr. 4052/J vom 25. Juli 2019 durch die Bundeskanzlerin sowie der Fragen 10, 11, 16, 17, 18 und 24 der parlamentarischen Anfrage Nr. 4016/J vom 22. Juli 2019 durch die Bundeskanzlerin verweisen.

**Zu Frage 2:**

- *In welcher Weise war Kanzleramtsminister BLÜMEL an der Erteilung dieses Auftrags beteiligt?*

Ich darf auf die Beantwortung der Frage 4 der parlamentarischen Anfrage Nr. 4052/J vom 25. Juli 2019 durch die Bundeskanzlerin verweisen.

**Zu Frage 3:**

- *Wann wurde Minister BLÜMEL über die erfolgreiche Vernichtung der Festplatten informiert?*

Ich darf auf die Beantwortung der Frage 5 der parlamentarischen Anfrage Nr. 4052/J vom 25. Juli 2019 durch die Bundeskanzlerin verweisen.

**Zu Frage 4:**

- *In welcher Weise waren der damalige Referent im Kabinett des Kanzleramtsministers BLÜMEL, Bernd PICHLMAYER, sowie der damalige Leiter der IT-Abteilung im BKA, Erich A., an der Erteilung dieses Auftrags beteiligt?*

Ich darf auf die Beantwortung der Frage 6 der parlamentarischen Anfrage Nr. 4052/J vom 25. Juli 2019 durch die Bundeskanzlerin verweisen.

**Zu Frage 5:**

- *Von wen hat PICHLMAYER seine diesbezüglichen Aufträge erhalten?*

Ich darf auf die Beantwortung der Frage 7 der parlamentarischen Anfrage Nr. 4052/J vom 25. Juli 2019 durch die Bundeskanzlerin verweisen.

**Zu Frage 6:**

- *PICHLMAYER gehörte seit dem 19.12.2017 dem Kabinett BLÜMEL an. War PICHLMAYER als Referent von Minister BLÜMEL befugt, M. als Mitarbeiter der Abt. I/12 „Digitale Kommunikation im BKA“ Weisungen zu erteilen?*

Ich darf auf die Beantwortung der Frage 8 der parlamentarischen Anfrage Nr. 4052/J vom 25. Juli 2019 durch die Bundeskanzlerin verweisen.

**Zu Frage 7:**

- *Wenn nein, wer hat persönlich M. mit der Vernichtung der Festplatten beauftragt?*

Ich darf auf die Beantwortung der Frage 9 der parlamentarischen Anfrage Nr. 4052/J vom 25. Juli 2019 durch die Bundeskanzlerin verweisen.

**Zu Frage 8:**

- *Laut Bericht des „Kurier“ vom 20.07.2019 hat A. die Vernichtung der Daten außer Haus als nicht vorschriftsgemäß bezeichnet. Warum wurde sie dennoch in dieser Art durchgeführt?*

Ich darf auf die Beantwortung der Frage 10 der parlamentarischen Anfrage Nr. 4052/J vom 25. Juli 2019 durch die Bundeskanzlerin verweisen.

**Zu den Fragen 9 und 10:**

- *Befand sich unter den Geräten, deren Festplatten vernichtet wurden, auch ein Gerät des damaligen Kanzleramtsministers?*
- *Wenn ja, um welches Gerät (Drucker, Notebook etc.) handelte es sich?*

Wie schon in den einleitend aufbereiteten Grundlagen zur Behandlung von Daten dargelegt, handelte es sich um interne Speicher von Multifunktionsgeräten in den Kabinetten von Bundeskanzler Kurz und Bundesminister Blümel.

**Zu den Fragen 11 bis 13:**

- *Wurden in diesem Zusammenhang auch Daten, die sich nicht auf den fünf Festplatten befanden, gelöscht?*

- *Wenn ja, um welche Daten handelte es sich?*
- *Wo waren diese Daten gespeichert?*

Ich darf auf die Beantwortung der Fragen 31 bis 33 der parlamentarischen Anfrage Nr. 4052/J vom 25. Juli 2019 durch die Bundeskanzlerin verweisen.

**Zu den Fragen 14 und 15:**

- *Wer hat die Festplatten ausgebaut?*
- *Wer hat dazu den Auftrag gegeben?*

Ich darf auf die Beantwortung der Fragen 34 und 35 der parlamentarischen Anfrage Nr. 4052/J vom 25. Juli 2019 durch die Bundeskanzlerin verweisen.

**Zu Frage 16:**

- *Wer war Eigentümer der vernichteten Festplatten?*

Ich darf auf die Beantwortung der Frage 36 der parlamentarischen Anfrage Nr. 4052/J vom 25. Juli 2019 durch die Bundeskanzlerin verweisen.

**Zu Frage 17:**

- *Warum wurden die Festplatten nicht – wie üblich - von der IT-Abteilung im BKA vernichtet?*

Ich darf auf die Beantwortung der Frage 37 der parlamentarischen Anfrage Nr. 4052/J vom 25. Juli 2019 durch die Bundeskanzlerin verweisen.

**Zu Frage 18:**

- *Waren die so gelöschten Daten durch Back Ups oder auf andere Art gesichert?*

Ich darf auf die Beantwortung der Frage 38 der parlamentarischen Anfrage Nr. 4052/J vom 25. Juli 2019 durch die Bundeskanzlerin verweisen.

**Zu den Fragen 19 und 20:**

- *Befanden sich auf diesen Festplatten Daten, die nach § 6 Abs 3 Bundesarchivgesetz dem Staatsarchiv zu übergeben wären?*
- *Welche Daten befanden sich auf diesen Festplatten, die nicht nach § 6 Abs 3 Bundesarchivgesetz dem Staatsarchiv zu übergeben wären?*

Ich darf auf die Beantwortung der Fragen 43 und 44 der parlamentarischen Anfrage Nr. 4052/J vom 25. Juli 2019 durch die Bundeskanzlerin verweisen.

**Zu den Fragen 21 bis 25:**

- *Welche Daten bzw. Dokumente der ÖVP befanden sich auf den Festplatten?*
- *Befanden sich auf den Festplatten Strategiepapiere für die NRW 2019?*
- *Befanden sich auf den Festplatten Informationen, die in einem Wahlkampf gegen politische Gegner eingesetzt werden konnten?*
- *Befanden sich auf den Festplatten Daten, Mails oder Dokumente des Bundeskanzlers oder des Kanzleramtsministers?*
- *Haben sich unter den gelöschten Daten auch die oben genannten Ibiza-Mails befunden?*

Ich darf auf die Beantwortung der Fragen 45 bis 49 der parlamentarischen Anfrage Nr. 4052/J vom 25. Juli 2019 durch die Bundeskanzlerin verweisen.

**Zu Frage 26:**

- *Haben sich unter den gelöschten Daten Mails, die über den Mailserver mit der IP-Adresse 92.51.182.37 oder 92.51.182.1 versandt wurden, befunden?*

Ich darf auf die Beantwortung der Frage 50 der parlamentarischen Anfrage Nr. 4052/J vom 25. Juli 2019 durch die Bundeskanzlerin verweisen.

**Zu Frage 27:**

- *Ist PICHLMAYER verdächtig, als Beitragstätter Delikte nach § 126 a StGB (1) (Datenbeschädigung) oder § 125 StGB (Sachbeschädigung) begangen zu haben?*

Ich ersuche um Verständnis, dass diese Frage nicht Gegenstand meines Vollziehungsbereiches ist.

**Zu Frage 28:**

- *Haben Sie diesbezüglich Anzeigen bei der WKStA erstattet?*

Das Bundeskanzleramt hat keine Anzeige bei der Wirtschafts- und Korruptionstaatsanwaltschaft erstattet, zumal der Vorgang bereits Gegenstand von kriminalpolizeilichen Ermittlungen ist.

**Zu Frage 29:**

- *Am 9.5.2019 wurde ein Daten-Leak bekannt, durch den Passwörter sowie die dazugehörigen E-Mailadressen mehrerer Minister, darunter Gernot BLÜMEL, an die Öffentlichkeit gelangten. Stehen die Datenvernichtungsaktionen in Zusammenhang mit diesem Daten-Leak?*

Ich darf auf die Beantwortung der Frage 53 der parlamentarischen Anfrage Nr. 4052/J vom 25. Juli 2019 durch die Bundeskanzlerin verweisen.

**Zu den Fragen 30 bis 32:**

- *Haben Sie den Auftrag gegeben, nach Maßgabe der technischen Möglichkeiten die gelöschten Daten wiederherzustellen?*
- *Wenn ja, an wen und auf welche Art?*
- *Bis wann ist in diesem Zusammenhang mit einem Ergebnis zu rechnen?*

Ich darf auf die Beantwortung der Fragen 54 bis 56 der parlamentarischen Anfrage Nr. 4052/J vom 25. Juli 2019 durch die Bundeskanzlerin verweisen.

**Zu Frage 33:**

- *Ist es richtig, dass PICHLMAYR nach wie vor Ihrem Kabinett beschäftigt ist?*

Ja.

**Zu Frage 34:**

- *Ist auszuschließen, dass PICHLMAYR an der Beantwortung der vorliegenden Anfrage mitwirkt?*

Ja. Die Beantwortung der vorliegenden Anfrage erfolgt wie üblich unter Einbindung aller dafür notwendigen Stellen.

Mag. Alexander Schallenberg

