3800/AB
vom 26.08.2019 zu 4052/J (XXVI.GP)

Bundeskanzleramt

bundeskanzleramt.gv.at

Dr. Brigitte Bierlein
Bundeskanzlerin

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: BKA-353.110/0091-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. **4052/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[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.

1.1. 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. 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.

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.

<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:

- *Welche Aufgaben hatte Arno M. im BKA?*

Ich darf auf meine Beantwortung der Frage 9 der parlamentarischen Anfrage Nr. 4016/J vom 22. Juli 2019 verweisen.

Zu Frage 2:

- *M. verfügt über eine nachweisbare Qualifikation: Fotograf. Über welche Qualifikationen im Umgang mit Festplatten verfügt er?*

Nach den mir vorliegenden Informationen verfügt M. nicht zuletzt durch seine umfassenden Kenntnisse im Bereich der Bildbearbeitung und der Betreuung von Social-Media-Kanälen über herausragende Kompetenzen im EDV-Bereich und ist nicht nur im Umgang mit zahlreichen Anwenderprogrammen, sondern auch mit Computer-Hardware besonders versiert.

Zu Frage 3:

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

Es darf darauf hingewiesen werden, dass M. keinen Auftrag zum Ausbau der internen Speicher der Multifunktionsgeräte hatte und diese daher auch nicht ausgebaut hat.

Zur Frage der Vernichtung darf ich auf meine Beantwortung der Fragen 10, 11, 16, 17, 18 und 24 der parlamentarischen Anfrage Nr. 4016/J vom 22. Juli 2019 verweisen.

Zu den Fragen 4 und 5:

- *In welcher Weise waren Bundeskanzler KURZ bzw. der Kanzleramtsminister BLÜMEL an der Erteilung dieses Auftrags beteiligt?*
- *Wann wurden BK KURZ bzw. Minister BLÜMEL über die erfolgreiche Vernichtung der Festplatten informiert?*

Es gab den mir vorliegenden Informationen zufolge keinen Auftrag an M. zum Ausbau der Festplatten, und Bundeskanzler a.D. Kurz und Bundesminister a.D. Blümel waren nicht in den Ablauf zum Ausbau und der Vernichtung der Festplatten involviert.

Zu Frage 6:

- *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 meine Beantwortung der Fragen 10, 11, 16, 17, 18 und 24 der parlamentarischen Anfrage Nr. 4016/J vom 22. Juli 2019 verweisen.

Zu Frage 7:

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

Die Entscheidungen des Genannten wurden nach den mir vorliegenden Informationen in dessen Verantwortungsbereich getroffen.

Zu Frage 8:

- *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?*

Nein, in diesem Verhältnis besteht kein Weisungszusammenhang.

Zu Frage 9:

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

M. hat sich nach den mir vorliegenden Informationen aus Eigenem angeboten, die Vernichtung der Festplatten vorzunehmen.

Zu den Fragen 10 und 11:

- *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?*
- *Hat A. formellen Protest gegen diese Vorgehensweise eingelegt?*

Eine Vernichtung von Daten außer Haus ist per se nicht vorschriftswidrig, sondern eine mögliche Variante zur rechtskonformen Löschung und in der Informationstechnologie auch ein durchaus übliches Vorgehen.

Grundsätzlich werden Datenträger wie z.B. Festplatten (PCs, Laptops, Server, Multifunktionsgeräte) oder USB-Sticks nach den mir vorliegenden Informationen seit Frühjahr 2015 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. Es werden auch defekte Festplatten aus PCs oder Laptops, die nicht mehr im geordneten Weg unlesbar gemacht werden können, einbehalten und einer Verschredderung zugeführt.

Zu Frage 12:

- *Welcher Tätigkeit gehen PICHLMAYER und A. gegenwärtig nach?*

Herr Pichlmayer ist gegenwärtig Mitarbeiter im Kabinett des Bundesministers für EU, Kunst, Kultur und Medien, Mag. Schallenberg.

A. ist Leiter der Gruppe I/C und der Abteilung I/7.

Zu den Fragen 13 bis 15:

- *Warum hat M. den Schredder-Auftrag unter falschem Namen durchgeführt?*
- *Warum ist der Firma Reisswolf verheimlicht worden, dass es sich um fünf Festplatten des BKA handelt?*
- *Hat M. diesen Auftrag im Rahmen seines Unternehmens durchgeführt?*

Diese Fragen sind nicht Gegenstand der Vollziehung.

Zu den Fragen 16 bis 18:

- *War BK KURZ über diesen Auftrag informiert?*
- *War Minister BLÜMEL über diesen Auftrag informiert?*
- *War Kabinettschef BONELLI über diesen Auftrag informiert?*

Nach den mir vorliegenden Informationen waren die Genannten nicht informiert.

Zu den Fragen 19 bis 22:

- *Wie viele Festplatten mit welchen Seriennummern wurden im Zuge dieser Handlung vernichtet bzw. gelöscht?*
- *Befanden sich Festplatten folgender Hersteller bei den zerstörten Festplatten: Western Digital, Hitachi, Seagate und Toshiba?*
- *Befanden sich Festplatten anderer Hersteller unter den zerstörten Festplatten?*
- *Welche Speicherkapazitäten hatten die zerstörten Festplatten?*

Ich ersuche um Verständnis, dass ich dazu aufgrund des anhängigen strafrechtlichen Ermittlungsverfahrens keine Angaben machen kann.

Zu den Fragen 23 bis 25:

- *In welchen Geräten befanden sich diese Festplatten?*
- *Wie viele dieser Geräte waren Notebooks?*
- *Wer hat diese Geräte ausgebaut?*

Es darf angemerkt werden, dass keine Geräte, sondern interne Speicher aus (Multifunktions-) Geräten ausgebaut wurden. Hinsichtlich des Ausbaus der internen Speicher darf ich auf meine Beantwortung der Frage 17 der parlamentarischen Anfrage Nr. 4029/J vom 23. Juli 2019 verweisen.

Zu Frage 26:

- *Wie lauten die Inventarnummern dieser Geräte?*

Die Anlagenummern der anfragegegenständlichen Multifunktionsgeräte lauten nach den mir vorliegenden Informationen 40000 088 44 65, 40000 101 24 83, 40000 103 81 69, 40000 088 44 43, 40000 078 68 32.

Zu den Fragen 27 bis 30:

- *Welche Mitarbeiter verwendeten diese Geräte?*
- *Befand sich unter diesen Geräten auch das Gerät des damaligen Bundeskanzlers?*
- *Befand sich unter diesen Geräten auch das Gerät des damaligen Kanzleramtsministers?*
- *Befand sich unter diesen Geräten auch das Gerät des Kabinettschefs des damaligen Bundeskanzlers?*

Ich darf auf meine Beantwortung der Frage 9 der parlamentarischen Anfrage Nr. 4029/J vom 23. Juli 2019 verweisen.

Zu den Fragen 31 bis 33:

- *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 meine Beantwortung der Frage 6 der parlamentarischen Anfrage Nr. 4029/J vom 23. Juli 2019 verweisen.

Zu den Fragen 34 und 35:

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

Ich darf auf meine Beantwortung der Fragen 17 und 18 der parlamentarischen Anfrage Nr. 4029/J vom 23. Juli 2019 verweisen.

Zu Frage 36:

- *Wer war Eigentümer der vernichteten Festplatten?*

Ich darf auf meine Beantwortung der Frage 19 der parlamentarischen Anfrage Nr. 4016/J vom 22. Juli 2019 verweisen.

Zu Frage 37:

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

Ich darf auf meine Beantwortung der Frage 24 der parlamentarischen Anfrage Nr. 4016/J vom 22. Juli 2019 verweisen.

Zu Frage 38:

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

Nein, nach den mir vorliegenden Informationen gibt es keine Backups, da sich lediglich die erforderlichen temporären Datenkopien auf internen Speichern von Multifunktionsgeräten befinden, die für die Durchführung des jeweiligen Prozesses (Drucken, Kopieren oder Scannen) erforderlich sind.

Zu den Fragen 39 und 40:

- *Welche Netzwerkaktivitäten im BKA werden von welchen Servern in welcher Form mitprotokolliert?*
- *Wie lange werden diese Daten gespeichert?*

Im Bundeskanzleramt wird den mir vorliegenden Informationen zufolge seit 2016 ein Security Information und Event Management-System (SIEM) betrieben. Dieses SIEM-System erhält Daten zum Netzwerk Traffic von Routern und Firewall. Die Daten werden korreliert und pseudo-anonymisiert. Die SIEM Daten werden für 90 Tage gespeichert.

Es werden dabei keine Inhaltsdaten bzw. Druckerströme analysiert oder aufgezeichnet.

Verbindungsdaten der E-Mailkommunikation werden am Gateway für 1 Jahr und auf den Mail-Servern für 3 Monate gespeichert.

Zu Frage 41:

- *Lassen sich auf Grund dieser Daten Druckaufträge zu bestimmten Zeitpunkten erheben?*

Nein, da Druckjobs nicht aufgezeichnet werden.

Zu den Fragen 42 bis 44:

- *Welche Daten befanden sich auf diesen Festplatten?*
- *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?*

Zu diesen Fragen darf auf die einleitend aufbereiteten Grundlagen zur Behandlung von Daten, den Unterschied zwischen benutzerverwalteten und systemverwalteten Daten und 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 wäre daher nicht korrekt.

Zu den Fragen 45 bis 49:

- *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?*

Es darf auf die einleitend aufbereiteten Grundlagen zur Behandlung von Daten und den Unterschied zwischen benutzerverwalteten und systemverwalteten Daten 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 internen Speichern von Multifunktionsgeräten die erforderlichen temporären Datenkopien befinden, die für die Durchführung des jeweiligen Prozesses (Drucken, Kopieren oder Scannen) erforderlich sind und eine Gemengelage unterschiedlicher Daten bilden können.

Ob sich Daten oder Datenfragmente zu den nachgefragten Themenbereichen auf den internen Speichern befanden, kann daher nicht beantwortet werden.

Zu Frage 50:

- *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?*

Nach den mir vorliegenden Informationen bieten die genannten IP-Adressen kein SMTP-Service (nach außen) an. Im Firewall Log gibt es keine Verbindungen zwischen den Mailgateways des Bundeskanzleramtes und den betreffenden Adressen.

Es darf darauf hingewiesen werden, dass eine generelle Überwachung aller Tätigkeiten der Mitarbeiterinnen und Mitarbeiter (inkl. E-Mails) durch die IKT gemäß den §§ 79c ff Beamtendienstrechtsgesetz 1979 verboten ist. 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 51:

- *Ist M. verdächtig, durch seine Aktion 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 und daher nicht beantwortet werden kann.

Zu Frage 52:

- *Hat das BKA diesbezüglich Anzeigen bei der WKStA erstattet?*

Das Bundeskanzleramt hat keine Anzeige bei der Wirtschafts- und Korruptionsstaatsanwaltschaft erstattet, zumal der Vorgang bereits Gegenstand eines strafrechtlichen Ermittlungsverfahrens ist.

Zu Frage 53:

- *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?*

Ein aktuelles Datenleak ist nicht bekannt.

Zu den Fragen 54 bis 56:

- *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?*

Nein, ein derartiger Auftrag wurde nicht erteilt, dazu bestand keine Veranlassung.

Zu Frage 57:

- *Ist es richtig, dass PICHLMAYR nach wie vor im Kabinett, das die Agenden von Ex-Minister BLÜMEL wahrnimmt, beschäftigt ist?*

Wie bereits bei Frage 12 ausgeführt, ist der Genannte gegenwärtig Mitarbeiter im Kabinett von Bundesminister für EU, Kunst, Kultur und Medien, Mag. Schallenberg.

Zu Frage 58:

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

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

Zu Frage 59:

- *Bis wann werden Sie die KURZ-V-Männer in den Kabinetten der Mitglieder der Bundesregierung durch parteiunabhängige Personen ersetzt haben?*

Diese Frage ist nicht Gegenstand der Vollziehung.

Zu Frage 60:

- *Altkanzler KURZ hat die Schredderung der fünf Festplatten als „übliche Aktion" bezeichnet. Ist die Vernichtung von Festplatten unter falschem Namen, ohne Bezahlung der Rechnung und gegen die Empfehlung des Leiters der IT-Abteilung im BKA üblich?*

Nein, davon gehe ich nicht aus. Ich darf aber ein weiteres Mal darauf hinweisen, dass, wie in den einleitend aufbereiteten Grundlagen bereits ausgeführt, die physische Vernichtung (Schreddern) der Datenträger aus Multifunktionsgeräten ein durchaus üblicher und rechtskonformer Vorgang und unter bestimmten Rahmenbedingungen sogar zwingend ist.

Zu Frage 61:

- *ÖVP-Generalsekretär NEHAMMER hat in der ZiB2 betont, dass die Festplatten „wieder auch ins Bundeskanzleramt zurückgekommen sind". Welcher Verwendung werden die Festplatten in ihrer neuen Form zugeführt?*

Das geschredderte Material wird keiner weiteren Verwendung zugeführt.

Dr. Brigitte Bierlein

REPUBLIK ÖSTERREICH BUNDESKANZLERAMT AMTSSIGNATUR	Unterzeichner	serialNumber=932783133,CN=Bundeskanzleramt,C=AT
	Datum/Zeit	2019-08-26T14:46:17+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	2019-08-28T10:34:17+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.	