

 Bundeskanzleramt

bundeskanzleramt.gv.at

Dr. Brigitte Bierlein
Bundeskanzlerin

Herrn
Mag. Wolfgang Sobotka
Präsident des Nationalrats
Parlament
1017 Wien

Geschäftszahl: BKA-353.110/0084-IIM/2019

Wien, am 26. August 2019

Sehr geehrter Herr Präsident,

die Abgeordneten zum Nationalrat Mag. Leichtfried, Kolleginnen und Kollegen haben am 23. Juli 2019 unter der Nr. **4029/J** an mich eine schriftliche parlamentarische Anfrage betreffend „Operation Reißwolf“ durch Altkanzler Sebastian 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 Daten¹
- 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 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. 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.

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 von den zuständigen Organisationseinheiten des Bundeskanzleramtes bereitgestellten Informationen wie folgt:

Zu Frage 1:

- *Hat Ihr Amtsvorgänger Sebastian Kurz bei der Amtsübergabe Akten an Sie übergeben?*

Nein, mein Amtsvorgänger hat mir keine Akten übergeben.

Zu den Fragen 2 und 3:

- *Wenn dies nicht der Fall ist, hat Ihr Amtsvorgänger Sebastian Kurz, wie bei Regierungsübergaben üblich, Akten an das Staatsarchiv übergeben? Wenn ja, in welcher Form wurden sie übergeben (Datenträger, Papier) und worauf bezogen sich die Daten?*
- *Sollte dies nicht geschehen sein, warum wurden dem Staatsarchiv keinerlei Akten übergeben?*

Mein Amtsvorgänger hat Schriftgut im Sinne des § 6 Abs. 3 Bundesarchivgesetz an das Österreichische Staatsarchiv übergeben.

Zu den Fragen 4 und 5:

- *Gibt es nach Ihrer Erkenntnis relevante Akten, die weder Ihnen noch dem Staatsarchiv übergeben wurden?*
- *Gibt es betreffend Inhalte dieser Akten aktuell Nachfragen von Staatsanwaltschaft, Polizei oder Rechnungshof?*

Nein, Derartiges ist mir nicht bekannt. Anfragen von Staatsanwaltschaft, Polizei oder Rechnungshof liegen meines Wissens nicht vor.

Zu den Fragen 6 und 7:

- *Von wieviel Datenträgern, die von Sebastian Kurz oder seinem Kabinett verwendet wurden, wurden Informationen gelöscht?*
 - *Wie viele davon wurden im Haus, also durch Mitarbeiter des BKA, gelöscht bzw. vernichtet?*
 - *Wie viele davon wurden extern gelöscht bzw. vernichtet?*
 - *Wie viele wurden vom betreffenden Mitarbeiter zur Firma Reisswolf gebracht?*

Wie hoch war die Gesamtkapazität der vernichteten Festplatten?

- *Von wieviel Datenträgern, die von Gernot Blümel oder seinem Kabinett verwendet wurden, wurden Informationen gelöscht?*
 - *Wie viele davon wurden im Haus, also durch Mitarbeiter des BKA, gelöscht bzw. vernichtet?*
 - *Wie viele davon wurden extern gelöscht bzw. vernichtet?*
 - *Wie viele wurden vom betreffenden Mitarbeiter zur Firma Reisswolf gebracht?*
 - *Wie hoch war die Gesamtkapazität der vernichteten Festplatten?*

Es darf auf die einleitend aufbereiteten Grundlagen zu benutzerverwalteten bzw. systemverwalteten Daten (vgl. Punkte 1.1. und 1.2.) verwiesen werden.

Im gegenständlichen Fall wurden interne Speicher aus Multifunktionsgeräten ausgebaut, um die darauf enthaltenen Daten zu löschen. Detailinformationen zur verbrauchten Kapazität der vom Leasinggeber ausgebauten internen Speicher liegen nicht vor.

In Zusammenhang mit allfälligen weiteren Datenträgern wird angemerkt, dass diese bei verteilten Applikationen auf unterschiedlichen Speichermedien unterschiedlicher Systeme liegen. Daher ist eine Beantwortung dieser Fragen nicht möglich, da es – abgesehen von Akten – der Benutzerin bzw. dem Benutzer obliegt, Daten zu löschen.

Zu Frage 8:

- *Welche Festplatten von welchen Druckern (Benutzer, Seriennummer) wurden konkret entfernt?*

Es wird 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.

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. Eine Zuordnung von Benutzerinnen oder Benutzern zu Druckern ist im Bundeskanzleramt nicht vorgesehen.

Nach den mir vorliegenden Informationen lauten die Seriennummern der fünf anfragegegenständlichen Multifunktionsgeräte:

- G436P600124
- G706J600485

- G726JA00197
- G716M930651
- G135PC00236

Zu Frage 9:

- *Welche Benutzer haben auf den betroffenen Geräten gedruckt? Bitte um detaillierte Aufstellung.*

Eine Zuordnung von Benutzerinnen oder Benutzern zu Druckern ist im Bundeskanzleramt nicht vorgesehen; es wird 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. 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 10:

- *An welchen Standorten (Bürräumen) waren die betroffenen Geräte aufgestellt?*

Die Multifunktionsgeräte, bei denen die 5 internen Speicher getauscht wurden, befinden sich am Ballhausplatz 2, 1. Stock, im Bereich der Kabinette.

Zu Frage 11:

- *Wieviel Gigabyte Datenvolumen wurden an Sie bzw. an das Staatsarchiv – wie üblich - weitergegeben, wie viel Gigabyte Datenvolumen (bzw. Festplattenkapazitäten) wurden gelöscht bzw. vernichtet?*

Detailinformationen zur verbrauchten Kapazität der vom Leasinggeber ausgebauten internen Speicher und Medien liegen nicht vor. Zudem ersuche ich um Verständnis, dass ich zur Größe des von meinem Amtsvorgänger an das Österreichische Staatsarchiv übergebenen Schriftgutes über keine Informationen verfüge.

Zu Frage 12:

- *Können Sie ausschließen, dass lt. Gesetz zu archivierende Daten bei den Vorgängen nicht mitvernichtet wurden?*

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

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 das Bundesarchivgesetz auch nicht anwendbar ist. Es kann daher ausgeschlossen werden, dass über die internen Speicher von Multifunktionsgeräten zu archivierende Daten vernichtet werden.

Zu Frage 13:

- *Gibt es ein Backup von den zerstörten Daten? Wenn ja, wurden diese an die Staatsanwaltschaft übermittelt?*

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

Zu Frage 14:

- *Betreffend externer Löschung bzw. Vernichtung der medial kolportierten Druckerfestplatte: Wer hat den Auftrag zur externen Löschung/Vernichtung gegeben?*

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 15:

- *Wurde betreffend der Druckerfestplatte eine Rechnung von der Firma Reisswolf an das Bundeskanzleramt gestellt?*

Nein, nach den mir vorliegenden Informationen wurde keine Rechnung an das Bundeskanzleramt gestellt.

Zu Frage 16:

- *In welcher Abteilung und aufgrund welchen Dienstverhältnisses war der Mitarbeiter, der die Druckerplatte zu Reisswolf brachte, beschäftigt?*

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“ im Rahmen eines Dienstverhältnisses nach dem Vertragsbedienstetengesetz 1948 tätig.

Zu Frage 17:

- *Von wem wurde die Druckerfestplatte aus dem Drucker entfernt?*

Der Tausch der internen Speicher der Multifunktionsgeräte wurde den mir vorliegenden Informationen zufolge auftragsgemäß von einem Techniker des Leasinggebers im Beisein von internem Personal des Bundeskanzleramtes durchgeführt.

Zu Frage 18:

- *Wer gab den Auftrag zur Entfernung dieser Druckerfestplatte? Wurde dies von Experten der zuständigen Abteilung veranlasst?*

Die IT-Abteilung des Bundeskanzleramtes hat den Leasinggeber mit dem professionellen Tausch der internen Speicher beauftragt.

Zu Frage 19:

- *Wer wurde von der Entfernung der Druckerfestplatte bzw. die Intention diese extern zu vernichten informiert?*
- *War der Kabinettschef von Sebastian Kurz über diesen Vorgang informiert?*
- *Welche Kabinettsmitarbeiter bzw. führende Beamte aus dem BKA waren über diesen Vorgang informiert?*

Der Auftrag zum Tausch der internen Speicher der Multifunktionsgeräte und der physischen Vernichtung der ausgebauten internen Speicher im Wege des Zentralen Ausweichsystems (ZAS) wurde auf Basis der Rücksprache mit dem zuständigen Koordinator und Sicherheitsverantwortlichen der Kabinette vom Gruppenleiter I/C an die IT-Abteilung des Bundeskanzleramtes erteilt. Die IT-Abteilung des Bundeskanzleramtes hat daraufhin den Leasinggeber mit dem professionellen Tausch der internen Speicher beauftragt.

Die Entscheidung, die physische Vernichtung nicht im Wege des ZAS durchzuführen, wurde nach den mir vorliegenden Informationen nach dem Ausbau der internen Speicher vom dafür verantwortlichen Mitarbeiter der Kabinette getroffen.

Den mir vorliegenden Informationen zufolge waren in den Kabinetten keine weiteren Mitarbeiterinnen und Mitarbeiter informiert. Im Übrigen darf ich auf meine Beantwortung der

Fragen 10, 11, 12, 13, 16, 17, 18 und 24 der parlamentarischen Anfrage Nr. 4016/J vom 22. Juli 2019 verweisen.

Zu Frage 20:

- *Auf welcher gesetzlichen Grundlage stützte sich der Vorgang, dass eine Druckerfestplatte durch einen Mitarbeiter des Kabinetts des Bundeskanzlers entfernt, aus dem BKA geschafft und danach bei einer externen Firma vernichtet wird?*

Die internen Speicher der Multifunktionsgeräte wurden von Mitarbeitern des Leasinggebers im Beisein von internem Personal der IT-Abteilung des Bundeskanzleramtes ausgebaut und nicht durch einen Mitarbeiter des Kabinetts. Ein Ausschleiden von Gegenständen ist nach den Bestimmungen der Bundesvermögensverwaltungsverordnung, BGBl. II Nr. 51/2012, grundsätzlich zulässig.

Zu den Fragen 21 und 23:

- *Haben die involvierten Mitarbeiter die Verpflichtungserklärung zur „Nutzung der Informations- und Kommunikationstechniksysteme“ des BKA unterzeichnet?*
- *Welche Mitarbeiter des Kabinetts von Sebastian Kurz, des Kabinetts von Minister Gernot Blümel, der Stabstellen bzw. der Regierungssprecher haben diese Erklärung aus Frage 14 unterzeichnet und welche nicht?*

Mitarbeiterinnen und Mitarbeiter, die ihren Dienst im Bundeskanzleramt neu antreten, haben nach den mir vorliegenden Informationen im Zuge ihres Dienstantrittes in der Regel die Verpflichtungserklärung zur „Nutzung der Informations- und Kommunikationstechniksysteme“ zu unterzeichnen. Für Mitarbeiterinnen und Mitarbeiter der Kabinette wurde außerdem am 24. Februar 2018 von 9.00-17.00 Uhr im Bundeskanzleramt ein „Crashkurs für neue Mitarbeiter/innen der Ministerbüros“ abgehalten, der unter anderem das Modul „ELAK & IT-Sicherheit“ enthielt. Sie wurden im Zuge dessen über die Nutzung der Informations- und Kommunikationstechniksysteme informiert und über bestehende Regelungen aufgeklärt. Darüber hinaus gilt für sämtliche Bedienstete des Bundeskanzleramtes die IKT-Nutzungsverordnung, BGBl. II Nr. 281/2009, die diesen in der jeweils gültigen Fassung im Intranet zur Verfügung gestellt wird.

Zu Frage 22:

- *Sieht diese IT-Richtlinie eine externe Vernichtung von Datenträgern, die im Eigentum des BKA stehen vor?*

Die „Verpflichtungserklärung zur Nutzung der Informations- und Kommunikationstechniksysteme des Bundeskanzleramtes“ enthält Richtlinien zur korrekten Nutzung der

Informations- und Kommunikationstechnik-Systeme im Bundeskanzleramt. Auf eine externe Vernichtung von Datenträgern wird in dieser Nutzungserklärung nicht Bezug genommen.

Zu den Fragen 24 bis 26:

- *Wurden mit Stichtag 19. Juli (erstmaliges Erscheinen der „Operation Reißwolf“ im Kurier) sämtliche Diensthandys der Kabinette von Kurz und Blümel sowie der Minister bzw. des Kanzlers selbst an das BKA zurückgegeben?*
- *Wenn nein, warum erfolgte keine ordnungsgemäße Rückgabe an das BKA?*
- *Wurden Diensthandys von Sebastian Kurz, Gernot Blümel bzw. deren Kabinettsmitarbeiter aus dem BKA rausgekauft? Wenn ja, bitte um Bekanntgabe wer sein Diensthandy mit dem Stichtag 19. Juli nicht zurückgegeben bzw. rausgekauft hat.*

Nein, nach den mir vorliegenden Informationen wurden von den Genannten keine Diensthandys erworben; jedoch erfolgte ein Sachgütertausch mit dem Bundesministerium für Inneres, wo eine Person nunmehr beschäftigt ist. Mit Stand 19. Juli 2019 war die Retournierung von zwei Smartphones ausständig. Diese wurden mittlerweile allerdings zurückgegeben. Die Rückholung der Geräte liegt in der Zuständigkeit der Gruppe I/C. Im Übrigen ersuche ich um Verständnis, dass die Bekanntgabe von personenbezogenen Daten aus datenschutzrechtlichen Gründen nicht möglich ist.

Dr. Brigitte Bierlein

