738/AB XXIII. GP

Eingelangt am 26.06.2007

BM für Finanzen

Anfragebeantwortung

Frau Präsidentin
des Nationalrates
Mag. Barbara Prammer
Parlament
1017 Wien

Wien, am Juni 2007

GZ: BMF-310205/0039-I/4/2007

Sehr geehrte Frau Präsidentin!

Auf die schriftliche parlamentarische Anfrage Nr. 730/J vom 26. April 2007 der Abgeordneten Dr. Graf und Kollegen, betreffend Vernichtung von relevanten Unterlagen für die Untersuchungsausschüsse betreffend Finanzmarktaufsicht, BAWAG, Hypo Alpe-Adria und weiterer Finanzdienstleister sowie hinsichtlich der Beschaffung von Kampfflugzeugen durch das BMF, beehre ich mich Folgendes mitzuteilen:

Zu 1. - 4.:

Gemäß einem von Herrn Prof. Reinhard Posch ausgearbeiteten Merkblatt „Daten in politischen Büros“ liegt es im Ermessen der politischen Ebene, welche ihrer Daten nach Ende einer Amtsperiode gelöscht werden sollen. Dieses Merkblatt, nach welchem im Bundesministerium für Finanzen vorgegangen wird, lege ich zur Information meiner Anfragebeantwortung bei.

Es wurden alle Daten der Mitarbeiterinnen und Mitarbeiter im Büro meines Amtsvorgängers sowie im Büro dessen Staatssekretariates gelöscht. Diese Löschung schließt die Festplatten aller Arbeitsplatzcomputer, Notebooks und der dazugehörigen Netzwerkserver (File-, Print-

und Mail-Services) mit ein. Akten des Bundesministeriums für Finanzen waren davon selbstverständlich nicht betroffen.

In diesem Zusammenhang möchte ich darauf hinweisen, dass ein derartiger Auftrag erstmals vom seinerzeitigen Finanzminister Rudolf Edlinger bzw. von seinem Kabinett erfolgt ist. Diese Praxis wurde seit damals beibehalten.

Zu 5, 8. und 9.:

Wie bereits erwähnt, wurden keine Akten des Bundesministeriums für Finanzen gelöscht. Dies wäre auch aufgrund des elektronischen Aktes (ELAK), wie er im Bundesbereich verwendet wird, technisch gar nicht möglich. Alle angeforderten Akten und offiziellen Unterlagen des Bundesministeriums für Finanzen, die von den Untersuchungsgegenständen der beiden Untersuchungsausschüsse umfasst werden, wurden dem Parlament übermittelt. Im Übrigen verweise ich auf meine Beantwortung der Fragen 1. - 4.

Zu 6. und 7.:

Alle Festplatten aus den Servern und die dazugehörigen Datensicherungsmedien sowie die Festplatten der Arbeitsplatzcomputer bzw. Notebooks, die im Ministerbüro und Büro des Herrn Staatssekretär im Einsatz waren, wurden im Auftrag des seinerzeitigen Kabinettschef von der BRZ GmbH einer unwiderruflichen und protokollierten Vernichtung zugeführt.

Zu 10. und 11.:

Da keine Akten oder sonstige offizielle Dokumente des Bundesministeriums für Finanzen gelöscht wurden, erübrigen sich allfällige weitere Veranlassungen.

Mit freundlichen Grüßen

Anlage:

CHIEF INFORMATION OFFICE
Stabsstelle IKT-Strategie des Bundes

Daten in politischen Büros

Ziele

Für das Umfeld der Kabinette/Büros von Regierungsmitgliedern ist eine IT-Situation vorzuschlagen, die folgende Aspekte beachtet und deren Umsetzung im Auftrag der politischen Büros durch entsprechendes Bewusstsein ermöglicht. Diese Notwendigkeit entsteht dadurch, dass Daten der persönlichen politischen Sphäre mit dem Schriftgut des Amtsträgers gemeinsam bzw. auf den gleichen Einrichtungen verarbeitet werden und ohne geeignete Sorgfalt eine spätere Trennung nicht bzw. nunr unter besonderen Aufwendungen möglich ist.

- **Gesetzliche Randbedingungen:** Bundesarchivgesetz und Bundesarchivgutverordnung entsprechen: §6 Abs. 3 des Bundesarchivgesetzes BGBL 162/1999 regelt, dass *Schriftgut* aus den politischen Büros dem Österreichischen Staatsarchiv zu übergeben ist. Die Archivwürdigkeit derartiger Schriftgüter wird in der Bundesarchivgutverordnung Pkt. 5 der Anlage zu §2 Abs.1 nochmals betont.

  Nicht davon betroffen sind persönliche Unterlagen wie beispielsweise Aufzeichnungen und Notizen (§ 2 Z 2 BundesarchivG) und Schriftgut gemäß Verordnung über Nicht archivwürdiges Schriftgut des Bundes (BGBl. II 366/02)

- **Verantwortlichkeit wahren:** Der vorliegende Text ist ein Vorschlag zur Handhabung der IT-Situation in politischen Büros dar, der helfen sollte ohne spezielles IT-Wissen in den Büros Bewusstsein und Sensibilität zu erzeugen und geeignte IT-Umgebungen umzusetzen. Der Text stellt daher primär Informationsmaterial dar, das erst auf Wunsch des jeweiligen politischen Büros zur Handlungsanweisung wird.

- **Vertraulichkeit sicherstellen:** In den politischen Büros entsteht eine zum Amtsgebrauch unterschiedliche teilweise auf Personen bezogene Vertraulichkeitsanforderung. Diese Vertraulichkeit und die damit betroffenen Informationen gehen demgemäß nicht unmittelbar auf den Amtsnachfolger über. Die bestehende IT-Situation, die mit den neuen Technologien verbundene Vernetzung und vor allem die Sicherung von Daten tragten diesem Umstand nicht ausreichend Rechnung.

- **Laufender Betrieb und Wechsel der Amtsträger:** Die Vertraulichkeit und die damit verbundenen Anforderungen treten meist erst mit dem Wechsel der Amtsträger ins Bewusstsein. Zu diesem Zeitpunkt ist es teilweise nahezu unmöglich nachträglich die Vertraulichkeit sicherzustellen, auf jeden Fallaber mit besonderen Aufwendungen und Belastungen für den restlichen Betrieb verbunden. Um dem entgegenzusteuern, ist daher die Vertraulichkeitssituation laufend und bereits mit Amtsantritt umzusetzen.

Aufgaben

In den politischen Büros sind generell zwei Datenarten zu verarbeiten und zu übermitteln, die eine unterschiedliche Situation erfordern.

Prof. Dr. Reinhard Posch http://www.cio.gv.at e-Mail: Reinhard.Posch@cio.gv.at

- **Daten des normalen Aktenlaufes**
  Dies sind Daten, die auch in den regulären Aktenlauf oder in die gewöhnliche Kommunikation mit der Beamtenebene eingebunden sind. Diese Daten besitzen einen klaren Bedarf, gleich wie die übrigen Daten der Beamtenebene behandelt, übermittelt und gesichert (auf Sicherungskopien ausgelagert) zu werden.
  Eine Trennung und insbesondere ein Entfernen dieser Daten nach Ende der Amtszeit ist nicht vorzusehen, da diese einen wesentlichen Bestandteil der ordentlichen Amtsführung bilden. Es sind für diese Datenkategorien die gleichen Vertraulichkeitsmechanismen zu wählen wie auf Beamtenebene.
  Daten,die ohne den Hinweis einer besonderen Vertraulichkeit von bzw. zur Beamtenebene kommuniziert werden fallen jedenfalls auch in diese Kategorie.
  Daten, die als Schriftgut einzustufen sind, sind jedenfalls als Daten des normalen Aktenlaufes einzustufen, auch dann, wenn es sich um vertrauliche Daten handelt.

- **Daten mit besonderer politischer Vertraulichkeit**
  Dies sind Daten, die unter Verantwortung der Leitung des politischen Büros als solche explizit eingestuft wurden. Wenn nicht anders vorgesehen, sind dazu jedenfalls die persönlichen Terminkalender, e-Mails und damit auch die Mailboxen und die persönlichen Notizen sowie sonstige persönliche Dokumente zu zählen sein.
  In diese Kategorie zählen auch Daten, die auf die EDV des politischen Büros gelangen, aber der Persönlichkeitssphäre des Amtsträgers zuzuordnen sind.

Vorgehensweise

Der vorliegende Text ist als einfaches Merkblatt für die politischen Büros und deren Dienstleister zu sehen, das die Umsetzung und Anforderungswünsche an die IT-Infrastruktur der politischen Büros erleichtern sollte. Dies erscheint beim erhöhten Moblilitätsbedarf der betroffenen Kategorie wichtig.

Ob die beiden Kategorien von Daten überhaupt getrennt organisiert werden, oder ob alle Daten in die Standardverarbeitung eingebunden werden, wird eine Entscheidung der aufzubringenden Ressourcen sein. Dieses Dokument stellt daher nicht eine Vorgabe sondern primärer eine Entscheidungsgrundlage dar auf Basis derer in bewusster Weise und zu Beginn einer Legislaturperiode die EDV eines politischen Büros geeignet organisiert werden kann.

Maßnahmen

1. **Das Schriftgut ist in der Form gemäß §4 (2) Bundesarchivgutverordnung (auf elektronischem Datenträger gemäß EDIAKT-Spezifikationen) dem Österreichischen Staatsarchiv anzubieten.**[1]

2. Die Daten des normalen Aktenlaufes sind in die Archivierungsmechanismen des Ressorts zu einzubinden.

3. Die Daten der Kategorie „besonders politisch vertraulich“ sind vom Amtsantritt an in Verantwortung und auf Risiko des Amtsträgers getrennt zu behandeln. Sie dürfen (auch nicht temporär) mit den Daten des normalen Aktenlaufes mit gesichert werden. Sofern diese aus prozeduralen Gründen gemeinsam mit anderen Daten verarbeitet werden (z.B. eMail und Mailboxen sowie Logfiles) ist nachweislich sicherzustellen, dass diese Daten nicht im Wege der Sicherung offengelegt werden und gegebenenfalls einem getrennten Sicherungsmechanismus unterstellt werden bzw. gelöscht werden.

4. Zusätzlich sind die Daten der Kategorie politisch vertraulich personenbezogen durch den Amtsträger zu archivieren. Das Medium (z.B. CD), welches in einem längerfristig auswertbaren Format zu erstellen ist wird durch den Amtsträger in dessen persönlichksitessphäre erstellt und verbleibt in dessen Persönlichkeitssphäre. Archivierte Daten dieser Kategorie sind regelmäßig – jedenfalls mit Ablauf der

1 Es wird daher darauf zu achten sein, dass das Schriftgut auch im elektronsichen Fall so entsteht, dass es im Wege der EDIAKT schnittstelle zu einem späteren Zeitpunkt übergeben werden kann.

Amtsperiode und einem damit verbundenen Wechsel des Amtsträgers - zu löschen. Sofern es scih um Schriftgut handelt, ist dieses zuvor dem Staatsarchiv anzubieten. Zu diesem Zeitpunkt müssen auch alle Sicherungskopien, die diese Daten enthalten könnten gelöscht werden bzw. dem Staatsarchiv angeboten worden sein.

5. Nicht besonders eingestufte Daten sind als Daten des normalen Aktenalufes zu betrachten und entsprechend zu behandeln. Die Einstufung erfolgt explizit oder nach Kategorien durch den betroffenen verantwortlichen Amtsträger unter Beachtung der Bundesarchivordnung.

6. Durch den Dienstleister ist eine Arbeitsanweisung zu erstellen, die diesen Grundsätzen Rechnung trägt. Die Arbeitsanweisung sollte durch Dritte geprüft werden.

Besondere Vertraulichkeit von einzelnen Dokumenten

Zur Umsetzung der besonderen Vertraulichkeit der Dokumente aus dem Bereich besonderer politischer Vertraulichkeit wird eine hinreichend starke Verschlüsselung vorgeschlagen, die ausschließlich dem politischen Büro zugänglich ist und damit die operativen Einheiten in der Verantwortung entlastet.

- Diese Daten können in abgeschlossenen Filebereichen (z.B. Laufwerke) oder in Verschlüsselungscontainer im Fall von einzelnen Dokumenten gehalten werden.

- In jedem Fall ist zur Sicherung gegen den Datenverlust sicherzustellen, dass der Entschlüsselungsschlüssel nicht in Verlust geraten kann. In der Regel wird dies durch Ausdruck des Schlüssels oder brennen des Schlüssels auf eine CD-ROM und Aufbewahrung in einem versiegelten Kuvert in einem dafür geeigneten Safe geschehen können.

Wien, 10.01.03

Dr. Reinhard Posch

Prof. Dr. Reinhard Posch http://www.cio.gv.at e-Mail: Reinhard.Posch@cio.gv.at

Merkblatt für den Systembetreiber (politisches Büro)

INSTALLATION

☐ Einrichtung der Standardkomponenten für das Ressort

☐ Einrichten des Mailkontos in einem für des politische Büro abgetrennten Datenbereich. Dies muss sowohl für die Server- als auch für die Clientkomponente geschehen.

☐ Sofern auf der Serverseite Mailkonten mit de üblichen Ressortwerkzeugen betrieben werden, ist darzustellen
(a) Mit welchen Werkzeugen regelmäßig die Separation der Daten durchgeführt wird.
(b) In welchen Intervallen diese Separation durchgeführt wird.
(c) Die Art des Protokolls, welches über diese Arbeiten geführt wird.

☐ Einrichten des Kalenders und der Notizwerkzeuge sowie allfälliger PDA - Abgleichwerkzeuge in einem für des politische Büro abgetrennten Datenbereich.

☐ Sofern auf der Serverseite Kalender, Notizen und PDA-Abgleich mit den üblichen Ressortwerkzeugen betrieben werden, ist darzustellen
(a) Mit welchen Werkzeugen regelmäßig die Separation durchgeführt wird.
(b) In welchen Intervallen diese Separation durchgeführt wird.
(c) Art des Protokolls, welches über diese Arbeiten geführt wird.

☐ Einrichtung der elektronischen Signatur und der Mailverschlüsselung mit einem Wirkungsbereich der Organisationseinheit, der dem politischen Büro entspricht. Alle Erzeugungsschlüssel sind zur Archivierung zu übergeben.

☐ Einrichtung eines für das politische Büro (allenfalls gemeinsamen) Filebereiches der auf starker Verschlüsselung basiert. Export der Zertifikate mit privaten Schlüsseln. Löschen und Reimport ohne die Möglichkeit eines weiteren Exports. Übergabe der gesicherten (exportierten) Zertifikate zur Versiegelung und Archivierung im Safe.

☐ Einschulung in verschlüsselte und signierte Mail und Ablegen in ressortinternen bzw. für das politische Büro verschlüsselten Bereichen.

Datum, durchführende Person.

Prof. Dr. Reinhard Posch http://www.cio.gv.at e-Mail: Reinhard.Posch@cio.gv.at

Merkblatt für den Betrieb

☐ Es ist vom Dienstleister ein Protokoll der Sicherungen, die die Daten (Mailboxen, Kalender,Filebereiche etc..) betreffen zu führen und durch die durchführende Person zu unterfertigen. Dieses Protokoll hat die Art und Kennung des Datenträgers sowie den Aufbewahrungsort zu enthalten.

☐ Es ist vom Dienstleister ein Protokoll der Einrichtung und nach Beendigung der Amtsperiode des Abschlusses zu führen. Das Abschlußprotokoll hat zu enthalten:
(a) Wann und mit welchen Werkzeugen wurde eine abschließende Sicherung mit anschließendem Löschen der Datenbereiche besonderer politischer Verrtraulichkeit durchgeführt. Vor der Löschung ist aus der Backupkopie der Entschlüsselungsschlüssel (Safe) eine Sicherungskopie zu erstellen. Der Amtsträger ist auf die getrennte Aufbewahrung aus Sicherheitsgründen hinzuweisen und es sind beide Kopien auszuhändigen. Auf Wunsch des Amtsträgers kann anlässlich des Abschlusses auch eine Klartextkopie erzeugt werden, die unmittelbar auszuhändigen ist.
(b) Wann und in welcher Form wurden sämtliche Datensicherungen des politischen Bereiches an den Amtsträger ausgehändigt und der Nachweis der Funktionalität (mit dem Backupschlüssel entschlüsselbar) geführt.

☐ Mailzugänge sind zu schließen und eine Beendigungsnotiz ist automatisch zu versenden. Alternativ kann auch für eine vereinbarte und protokollierte Zeit eine automatisches Forward zu einer anderen Adresse nach Angabe des Amtsträgers durchgeführt werden. Bei Absenden darf die Adresse nicht mehr eingebunden werden.

☐ Das Abschlußprotokoll ist von der durchführenden Person und vom Amtsträger zu fertigen und wird in zweifacher Ausfertigung erzeugt.

Bei Verwendung mobiler Geräte (Laptops, PDAs ..) ist besonders auf die Vertraulichkeit zu achten. Bei Laptops sind zumindest folgende Rgeln zu beachten:

☐ Es ist ein Start-Up Passwort auf Bios-Ebene einzurichten.

☐ Die Rückkehr aus Suspend- bzw. anderen Powerdown-Modi ist ebenfalls mit einem Passwort abzusichern.

☐ Persönliche Daten auf den Festplatten sind mit Verschlüsselung auf Fileebene abzusichern.

Prof. Dr. Reinhard Posch http://www.cio.gv.at e-Mail: Reinhard.Posch@cio.gv.at

Anhang: Gesetzliche Grundlagen

§ 2 Z 2 Bundesarchivgesetz:

2. Schriftgut:
Schriftgut gemäß § 25 Abs. 2 des Denkmalschutzgesetzes, **ausgenommen persönliche Unterlagen wie beispielsweise Aufzeichnungen und Notizen.**

§ 25 Abs. 2 Denkmalschutzgesetz:

(2) Schriftgut sind schriftlich geführte oder auf **elektronischen Informationsträgern** gespeicherte Aufzeichnungen aller Art wie Schreiben und Urkunden samt den damit in Zusammenhang stehenden Karten, Plänen, Zeichnungen, Siegel, Stempel mit deren Anlagen **einschließlich** der Programme, Karteien, Ordnungen und Verfahren, um das Schriftgut auswerten zu können.

Anhang: nicht archivwürdiges Schriftgut des Bundes

BGBL **366.**

Verordnung der Bundesregierung über nicht archivwürdiges Schriftgut des Bundes

Auf Grund des § 5 Abs. 4 des Bundesarchivgesetzes, BGBl. I Nr. 162/1999, wird verordnet:

Geltungsbereich

§ 1. (1) Diese Verordnung gilt für Schriftgut gemäß § 2 Z 2 des Bundesarchivgesetzes, das bei Bundesdienststellenoder bei einer ihrer Vorgängereinrichtungen in Erfüllung ihrer Aufgaben angefallen ist.

(2) Vom Geltungsbereich dieser Verordnung ist Schriftgut ausgenommen, das

1. im Zuge von gerichtlichen Verfahren bei Zivil- und Strafgerichten oder
2. vor dem 1. November 1955

angefallen ist.

Archivwürdigkeit von Schriftgut

§ 2. Das in der **Anlage** angeführte Schriftgut gilt nicht als Archivgut gemäß § 2 Z 3 des Bundesarchivgesetzes.

Verweisungen

§ 3. Soweit in dieser Verordnung auf Bestimmungen des Bundesarchivgesetzes verwiesen wird, sind diese in der Stammfassung anzuwenden.

In-Kraft-Treten

§ 4. Diese Verordnung tritt mit 1. Oktober 2002 in Kraft.

Schüssel Riess-Passer Ferrero-Waldner Gehrer Grasser Strasser Böhmdorfer Scheibner Molterer Haupt Reichhold Bartenstein

Anlage
zu § 2

1. Veröffentlichtes Schriftgut und Kopien;
2. Schriftgut im Rahmen des Bürgerservice und der Auskunftspflicht;
3. Schriftgut der Bibliotheken, Ministerialkanzleidirektionen, Wirtschaftsstellen, Amtsdruckereien, Haus- und Materialverwaltungen, Gebäudeverwaltungen sowie Evidenzstellen;
4. Schriftgut der Buchhaltungen und der Einrichtungen für Informationstechnologie;
5. Schriftgut im Rahmen der Haushaltsverrechnung, Besoldung, Wirtschafts- und Haushaltsangelegenheiten ausgenommen jenes, das die grundsätzlichen und zentralen Belange der Budgeterstellung, des Budgetvollzugs und des Finanzausgleichs betrifft;
6. dienststelleninterne Korrespondenzen, Unterlagen, Rundschreiben und Informationen, Einladungen, Adress- und Anwesenheitslisten und sonstige dienststelleninterne Aufzeichnungen wie Urlaubsscheine, Zeitkarten und vergleichbare Unterlagen;
7. Schriftgut betreffend Beschaffungen und Aufträge bis zum Auftragsvolumen von 200.000 €;
8. Schriftgut des Controllings, der Dienstreisen, des Publikations- und Broschürenmanagements;
9. statistische Unterlagen;
10. Schriftgut der nicht durch Gesetz oder Verordnung eingerichteten Beiräte und Kommissionen, sofern es sich auf interne Verwaltungsvorgänge bezieht;
11. Schriftgut im Zusammenhang mit Zollfreischreibungen, Reise- und Grenzverkehr;
12. Personalakten der Bundesbediensteten (einschließlich der Aus- und Weiterbildung), ausgenommen jener Personalakten gemäß Z 6 der Anlage zu § 2 Abs. 1 der Bundesarchivgutverordnung, BGBl. II

Nr. 367/2002.