XXIII. GP.-NR
1125 /AB
23. Aug. 2007
zu 1229 /J

REPUBLIK ÖSTERREICH

DR. ALFRED GUSENBAUER
BUNDESKANZLER

An die
Präsidentin des Nationalrats
Mag[a] Barbara PRAMMER
Parlament
1017 W i e n

GZ: BKA-353.110/0122-I/4/2007

Wien, am 22. August 2007

Sehr geehrte Frau Präsidentin!

Die Abgeordneten zum Nationalrat Mag. Maier, Kolleginnen und Kollegen haben am 6. Juli 2007 unter der **Nr. 1229/J** an mich eine schriftliche parlamentarische Anfrage betreffend Einsatz von Überwachungssoftware in öffentlichen Dienststellen gerichtet.

Diese Anfrage beantworte ich wie folgt:

Zu Frage 1:

- *In welcher Form und in welchem Umfang wurde in Ihrem Ressort dem Anliegen und den Anregungen des Datenschutzrates seit 2004 Rechnung getragen?*

Der Datenschutzrat hat in seiner Sitzung am 21. Juli 2004 im Wesentlichen empfohlen, in der Bundesverwaltung eine zwischen den Ressorts abgestimmte bundeseinheitliche und datenschutzrechtlich korrekte Vorgangsweise beim Einsatz von Überwachungssoftware festzulegen.

In Entsprechung dieser Anregung des Datenschutzrates wurde im Herbst 2004 seitens des Bundeskanzleramtes eine ressortübergreifende Umfrage zu dieser Problematik durchgeführt. Aufgrund des Ergebnisses dieser Umfrage, die zeigte, dass es in diesem Bereich eine sehr unterschiedliche Handhabung und Regelungsdichte gibt, sowie auf Initiative der Gewerkschaft Öffentlicher Dienst wurde im Jänner 2005 eine Plattform "Datenschutz im öffentlichen Dienst - Verhaltensregeln betreffend den Ge-

brauch der IT-Ausstattung" eingerichtet. Zweck dieser Arbeitsgruppe ist es, unter Einbindung von Experten und den Ressorts Richtlinien für den Umgang mit sensiblen Daten zu erarbeiten, die in Form einer Empfehlung des Bundeskanzleramtes an alle Zentralstellen zu einer einheitlichen Vorgangsweise beitragen sollen. Ihre Anfrage habe ich zum Anlass genommen, eine Intensivierung der Tätigkeit dieser Arbeitsgruppe zu veranlassen.

Zu Frage 2:

- *Welche Vorkehrungen wurden bislang getroffen, damit die technischen Möglichkeiten, die mit zugekaufter kommerzieller Software zur Mitarbeiterüberwachung gegeben sind, nicht oder nur unter besonders strengen gesetzlichen Kontrollen angewendet werden?*

Im Hinblick auf die Richtlinie über die Mindestvorschriften bezüglich der Sicherheit und des Gesundheitsschutzes bei der Arbeit an Bildschirmgeräten 90/270/EWG, ABl. L 156 vom 21.06.1990, S. 14 wurde in § 79c des Beamtendienstrechtsgesetzes 1979, in § 29n des Vertragsbedienstetengesetzes 1948 und in § 76g des Richterdienstgesetzes die Einführung und Verwendung von Kontrollmaßnahmen und technischen Systemen, welche die Menschenwürde berühren im Bundesdienst für unzulässig erklärt.

Im Vergleich dazu verbietet § 96 Abs. 1 Z 3 Arbeitsverfassungsgesetz nicht generell derartige Kontrollmaßnahmen und technische Systeme zur Kontrolle der Arbeitnehmer. Diese Bestimmung sieht lediglich vor, dass die Einführung von solchen Kontrollmaßnahmen und technischen Systemen der Zustimmung des Betriebsrates bedürfen, wenn diese Maßnahmen (Systeme) die Menschenwürde berühren.

Die im Vergleich zu § 96 Abs. 1 Z 3 Arbeitsverfassungsgesetz größere Restriktivität in den dienstrechtlichen Vorschriften der Bundesbediensteten ist dadurch bedingt, dass jede die Menschenwürde berührende Kontrollmaßnahme als unzulässiger Eingriff des Staates als Dienstgeber in den durch Art. 8 der Europäischen Menschenrechtskonvention geschützten Rechten zu werten ist.

Ob eine Kontrollmaßnahme oder ein technisches System zur Kontrolle der Arbeitnehmer die Menschenwürde berührt oder nicht, wird in der Praxis insbesondere an den zu § 96 Abs. 1 Z 3 Arbeitsverfassungsgesetz entwickelten Auslegungsgrundsät-

zen und der Entscheidungspraxis der Einigungsämter bzw. Gerichte und Behörden gemessen.

Da im Bundesdienst aus den angeführten Gründen keine Kontrollmaßnahmen und technische Systeme zur Kontrolle der Arbeitnehmer zulässig sind, die die Menschenwürde berühren, ist aus meiner Sicht keine besondere Kontrolle der Anwendung solcher Software nicht erforderlich.

Mit der Dienstrechts-Novelle 2007 wird ein Einvernehmensrecht der Zentralausschüsse der Personalvertretung des Bundes bei der Einführung von Kontrollmaßnahmen bezüglich des Umgangs von Bediensteten mit automationsunterstützten Datenverarbeitungssystemen geschaffen. Das als stärkstes Mitwirkungsrecht ausgestaltete Einvernehmensrecht der Personalvertretung soll sicherstellen, dass an sich gesetzlich zulässige Kontrollmaßnahmen nicht missbraucht werden.

Zu Frage 3:

- *Wurde kommerzielle Software oder so genannte Behördentrojaner zur Mitarbeiterüberwachung angekauft?*
  Wenn ja, welche Software und welche Behördentrojaner, zu welchen Zwecken?

Es wurde keine derartige Software eingekauft und es ist auch ein derartiger Ankauf nicht beabsichtigt.

Zu Frage 4:

- *Wurde im Ressort ein Datenschutzbeauftragter bestellt, der weisungsungebunden im Interesse der Bediensteten die Einhaltung von Datenschutzvorschriften sicherstellt?*
  Wenn ja, welche Aufgaben hat dieser im Einzelfall wahrzunehmen?

Zur Sicherung der Publizität von Datenverarbeitungen sieht die Richtlinie 95/46 EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Abl. Nr. L 281 von 23.11.1995 S. 31, drei alternative Instrumente vor:

a. Die Meldung von Datenanwendungen an ein Register, das von der unabhängigen Kontrollstelle zu führen ist, oder
b. die Bestellung eines internen Datenschutzbeauftragten, der eine Liste der Datenverarbeitungen des Auftraggebers zu führen hat, oder

c. die Offenlegung von nicht meldepflichtigen Datenverarbeitungen durch den Auftraggeber auf Antrag jedes Interessierten.

Der österreichische Bundesgesetzgeber hat sich für die Variante a. durch die Einrichtung des Datenverarbeitungsregisters im Datenschutzgesetz 2000 entschieden. Ein Datenschutzbeauftragter ist im Datenschutzgesetz 2000 nicht vorgesehen. Im Bundeskanzleramt ist daher kein Datenschutzbeauftragter bestellt.

Zu Frage 5:

➢ *In welchen Fällen wurde seit 2000 mit Organen der Personalvertretung (Dienststellenausschuss, Zentralausschuss) zur Einführung von Systemen zur automationsunterstützten Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten der Bediensteten verhandelt und Einvernehmen erzielt?*

Seit 2000 wurden *pm/sap* und HV/SAP im BKA eingeführt. Die Abstimmung dieser Systeme zur automationsunterstützten Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten erfolgte bundesweit zentral durch die zuständigen Einheiten (Sektion III des BKA bzw. Sektion V des BMF).

Die Organe der Personalvertretung wurden bei der Einführung im BKA von der Personal- und Organisationsabteilung zusätzlich laufend informiert.

Zu Frage 6:

➢ *Unter dem Begriff „Überwachungssoftware" werden in erster Linie legale im Einsatz befindliche Datensicherungs- und Systemfunktionalitätssicherungs-Maßnahmen verstanden. Es handelt sich hierbei vor allem auch um zulässigerweise installierte Kontrollsoftware zur Sicherung der Funktionsführung des EDV-Systems und des Datenschutzes. Unter anderem wurden in der Sitzung vom 21. Juli 2004 der Virenschutz, die Verhinderung des Zugriffs auf Webseiten mit dienstlich unzulässigen, weil illegal oder anstößigem Inhalt, sowie die Fernwartung bzw. das Aufzeichnen von Login-Versuchen, die bei mehreren fehlerhaften Versuchen zum Abbruch führen, angeführt.*
Sind aus Sicht des Ressorts noch weitere Softwarekomponenten gemäß diesem Verständnis anzuführen?
Wenn ja, welche?

Für die technische Wartung und technische Überwachung von komplexen EDV-Systemen sind entsprechende Werkzeuge erforderlich. Diese unabdingbaren Systemmanagementfunktionen sind bereits im eingesetzten Betriebssystem selbst enthalten oder werden durch zusätzliche Software-Produkte abgedeckt.

Für die technische Systemüberwachung wird im Bundeskanzleramt das Produkt „TNG - Unicenter" von Computer Associates eingesetzt. Dabei werden in unterschiedlichsten Bereichen Log-Dateien geführt, die inhaltlich Auskunft über das System selbst geben. Im Bereich des „Mailings", wo das Systemverhalten vor allem durch die Benutzer bestimmt wird, könnten Hinweise auf das Benutzerverhalten abgeleitet werden. Im Bereich des „Mailings" werden Log-Dateien geführt die ca. 60 Tage aufgehoben werden.

Die Benutzerdaten werden zumindest zwei Mal pro Tag gesichert. Diese Daten werden im Storage-System vorgehalten und in der Folge auf Band gesichert.

Generell ist festzuhalten, dass technisch bedingt jeder User durch Aktivitäten am System „Spuren" hinterlässt, die in sehr unterschiedlicher Form einsehbar, darstellbar und gegebenenfalls mit anderen Informationen verknüpft werden könnten.

Zu Frage 7:

- *Welche Organisationseinheit oder Person entscheidet über die Beschaffung bzw. den Einsatz von solchen Softwareprodukten bzw. wie sieht der diesbezügliche Ablauf aus?*

Die fachliche Entscheidung über die Beschaffung von Software für den Systembetrieb wird grundsätzlich vom Bereichsleiter IKT oder vom Leiter der Abteilung IT-Infrastruktur (Abteilung I/9) getroffen. Bei der Beschaffung von Software, die explizit das Benutzerverhalten beeinflusst (beeinflussen soll), wie z.B. eine URL – Filtering – Software, wird darüber hinaus im Einvernehmen mit der Organisations- und Personalabteilung und dem Leiter der Sektion I des Bundeskanzleramtes vorgegangen.

Zu Frage 8:

- *Sind die Organe der Personalvertretung und/oder der/die Datenschutzbeauftragte in solche Abläufe gemäß Frage 7 eingebunden?*

Vor dem Einsatz von Software, die explizit das Benutzerverhalten beeinflusst, erfolgt eine Einbindung der Personalvertretung durch die Organisations- und Personalabteilung des Bundeskanzleramtes.

Zu Frage 9:

- *Welche Organisationseinheit oder Person entscheidet unter welchen Rahmenbedingungen über die Einsicht in die durch solche Softwareprogramme gesammelten Daten und/oder über die Durchführung von Auswertungen bzw. wie sieht der diesbezügliche Ablauf aus?*

Generell ist eine Einsicht in die durch die angesprochenen Softwareprogramme zwangsläufig anfallenden personenbezogenen Daten nicht vorgesehen. Es ist aber nicht auszuschließen, dass im Zuge von technischen Wartungen und Fehlerbehebungen die betreffenden Techniker Kenntnis von solchen Daten erlangen.

Eine gezielte Einsicht in derartige Daten kommt nur bei hinreichendem Verdacht strafbarer Handlungen zur Beweissicherung in Frage. In diesen Fällen obliegt die Entscheidung dem Leiter der Sektion I des Bundeskanzleramtes.

Zu Frage 10:

- *Sind die Organe der Personalvertretung und/oder der/die Datenschutzbeauftragte in solche Abläufe gemäß Frage 9 eingebunden?*

Die Einbindung der Personalvertretung erfolgt entsprechend den Bestimmungen des Bundes-Personalvertretungsgesetzes.

Zu Frage 11:

- *Welche Vorkehrungen werden in Ihrem Ressorts getroffen, damit die technischen Möglichkeiten, die mit zugekaufter kommerzieller Software zur Mitarbeiterüberwachung gegeben sind, nicht oder nur unter Maßgabe der rechtlichen Rahmenbedingungen angewendet werden?*

Bei Dienstantritt im Bundeskanzleramt ist von dem/der zukünftigen Mitarbeiter/In eine Verpflichtungserklärung zur Einhaltung der Bestimmungen des Datenschutzgesetzes 2000 zu unterfertigen.

Die im Bereich der EDV tätigen Bediensteten werden darüber hinaus besonders über den Datenschutz und den dienstrechtlichen Konsequenzen bei dessen Verletzung belehrt. Weiters obliegen den Fachvorgesetzte besondere Kontrollpflichten, um einer missbräuchliche Verwendung von Systemdaten vorzubeugen.

Zu den Fragen 12 und 13:

- *Erfolgt in Ihrem Ressort bei der Verwendung von personenbezogenen Daten für dienstrechtliche oder disziplinarrechtliche Angelegenheiten eine Prüfung, ob die verwendeten Daten rechtmäßig (insbesondere datenschutzkonform) ermittelt, verarbeitet oder übermittelt wurden?*
- *Erfolgt in Ihrem Ressort bei der Verwendung von personenbezogenen Daten für dienstrechtliche oder disziplinarrechtliche Angelegenheiten eine Prüfung, zu welchem Zweck vorhandene Daten ermittelt, verarbeitet oder übermittelt wurden?*

Gemäß den § 280 Abs. 1 des Beamten-Dienstrechtsgesetzes 1979, § 96 Abs. 1 des Vertragsbedienstetengesetzes 1948 und Art. VI Abs. 1 des Richterdienstgesetzes sind die obersten Dienstbehörden ermächtigt, die dienstrechtlichen, besoldungsrechtlichen, ausbildungsbezogenen und sonstigen mit dem Dienstverhältnis in unmittelbarem Zusammenhang stehenden Daten der Bediensteten automationsunterstützt zu verarbeiten.

Grundsätzlich ist davon auszugehen, dass die zuständigen Bediensteten der Personalverwaltung des Ressorts nur in diesem Umfang Daten der Bediensteten erheben. Mir ist kein Fall im Ressort bekannt, dass darüber hinaus Daten erhoben wurden. Eine unzulässige Erhebung von Daten lässt sich nur im Einzel- oder Beschwerdefall feststellen. Sie stellt jedenfalls eine Verletzung von Dienstpflichten dar.

Zu den Fragen 14 und 15:

- *Haben die Bediensteten in Ihrem Ressort die Möglichkeit, sich vollständig darüber zu informieren, welche ihrer Person zugeordneten oder zuordenbare Daten ermittelt, gespeichert, verarbeitet oder übermittelt werden und zu welchem Zweck dies erfolgt?*
  Wie erfolgt diese Information und durch wen?
- *Haben die Bediensteten in Ihrem Ressort die Möglichkeit, die ihrer Person zugeordneten oder zuordenbaren Daten richtig zu stellen oder löschen zu lassen?*
  Wenn ja, wie erfolgt dies und durch wen?

Die Bediensteten haben die Möglichkeit durch eine entsprechende Anfrage bei der Organisations- und Personalabteilung des Bundeskanzleramtes solche Auskünfte gemäß dem Datenschutzgesetz 2000 zu erhalten und durch einen entsprechenden Antrag solche Richtigstellungen zu veranlassen.

Zu Frage 16:

➢ *Werden Sie sich für eine einheitliche und datenschutzrechtlich korrekte Vorgangsweise in der österreichischen Bundesverwaltung einsetzen?*

Selbstverständlich setze ich mich für eine einheitliche und datenschutzrechtlich korrekte Vorgangsweise in der österreichischen Bundesverwaltung ein, wo immer dies in meinem Einflussbereich liegt.

Zu Frage 17:

➢ *Treten Sie dafür ein, dass in Zukunft einheitliche Regelungen über den Einsatz von Software zur Kontrolle der Sicherung der Funktionstüchtigkeit der EDV-Systeme und zur Gewährleistung der Datensicherheit im Bundesbereich geschaffen werden?*

Ich werde dafür eintreten, dass eine ressortübergreifende Arbeitsgruppe sich dieser Themen annimmt.