BUNDESMINISTERIUM FÜR SOZIALE SICHERHEIT
GENERATIONEN UND KONSUMENTENSCHUTZ

XXII. GP.-NR
214 /AB
2003 -05- 14
zu 291 /J

Herrn
Präsidenten des Nationalrates (5-fach)
Parlament
1010 Wien

GZ: 10.001/127-4/2003 Wien, 9. Mai 2003

Sehr geehrter Herr Präsident!

Ich beantworte die an mich gerichtete schriftliche **Anfrage Nr. 291/J der Abgeordneten Mag. Maier und GenossInnen** für den Zuständigkeitsbereich des nunmehrigen Bundesministeriums für soziale Sicherheit, Generationen und Konsumentenschutz wie folgt:

Fragen 1 und 2:

Alle Datenanwendungen werden auf Grund der Bestimmungen des Datenschutzgesetzes 2000 (DSG 2000), BGBl. I Nr. 165/1999, der Datenschutzkommission/ Datenverarbeitungsregister gemeldet.

In den Meldungen der im Wirkungsbereich meines Ressorts durchgeführten Datenverarbeitungen an das Datenverarbeitungsregister sind die verarbeiteten Datenarten einzeln aufgezählt. Die im Ressort verarbeiteten sensiblen Daten sind daher den öffentlich einsehbaren und für jedermann zugänglichen Registrierungen im Datenverarbeitungsregister zu entnehmen, das eben zu diesem Einsichtszweck geführt wird. Aus diesen öffentlich einsehbaren Meldungen sind die Rechtsgrundlagen ersichtlich und es ist der jeweiligen Registrierung auch zu entnehmen, an welche Übermittlungsempfänger die einzelnen Datenarten übermittelt werden bzw. werden dürfen.

Frage 3:

Die für IT-Security im Bund zuständige IKT-Stabsstelle ist im permanenten Dialog mit Microsoft. Der „Beginn eines Government Security Programs" mit Microsoft ist daher nicht erforderlich.

Frage 4:

Fragen der IT-Security werden für den Bund im IKT-Board, dem alle Bundesministerien angehören, gemeinsam behandelt.

Fragen 5 und 6:

Die für die IT-Security zuständigen Stellen des Bundes haben den im Rahmen des Bedarfes der Bundesverwaltung notwendigen mittelbaren Zugriff auf die Quellcodes des Betriebssystems Microsoft Windows. Die Erkenntnisse werden im Rahmen der Sicherheitskonzepte berücksichtigt.

Frage 7:

Es sind all jene Datensicherheitsmaßnahmen vorgesehen, die gemäß § 14 DSG 2000 erforderlich sind.

Fragen 8 und 9:

Bei Daten, die in bestimmten Verarbeitungen mit sehr hohem Geheimhaltungsgrad enthalten sind, ist die verschlüsselte Speicherung vorgesehen. Eine verschlüsselte Übermittlung von Daten in offenen Netzen erfolgt dann, wenn dies aufgrund einer Vereinbarung zwischen den Kommunikationspartnern möglich ist.

Frage 10:

Ja, aufgrund bestehender Rechtsvorschriften.

Fragen 11 und 12:

Diese Fragen sind aus verwaltungsökonomischen Gründen nicht beantwortbar.

Frage 13:

Nein.

Fragen 14, 15 und 16:

Aufgrund der Antwort bei Frage 13 entfällt die Beantwortung dieser Fragen.

Frage 17:

Folgende Microsoft-Produkte werden in meinem Ressort eingesetzt:

Microsoft Windows NT 4.0, Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server, Microsoft Exchange Server 5.5, Microsoft Proxy Server 2.0, Microsoft SQL Server, Microsoft Internet Information Server, Microsoft SNA Manager 4.0, Microsoft Terminal Server, Windows Professional 2000, Microsoft Office 2000, Microsoft Office XP, Microsoft Access 2000, Real Player, Microsoft Visio 2002, Microsoft Front Page 2000, Win TV, Microsoft Map Point, Outlook 2000, Microsoft Windows XP, Microsoft Project 2000, Microsoft Internet Explorer 5.5.

Frage 18:

Es erfolgt keine Übertragung von personenbezogenen oder sensiblen Daten an Microsoft; eine zweckentfremdete Nutzung (Anwenderprofile etc.) wird somit verhindert.

Frage 19:

Ja; ein Sicherheitskonzept wurde erstellt.

Frage 20:

Im e-Government-Projekt der Bundesregierung ist die Einhaltung höchster Datensicherheit ein durchgehendes und vorrangiges Prinzip.

Mit freundlichen Grüßen
Der Bundesminister: