

2404/AB XXI.GP  
Eingelangt am: 06.07.2001  
BM für Finanzen

Auf die schriftliche parlamentarische Anfrage der Abgeordneten Mag. Cordula Frieser und Kollegen vom 10. Mai 2001, Nr. 2426/J, betreffend Datenzugriffe auf das Abgaben - Informationssystem (AIS) des Finanzministeriums, beehre ich mich Folgendes mitzuteilen:

Zu 1.:

Im Abgaben - Informationssystem (ATS) der Finanzverwaltung werden folgende Informationen über Steuerpflichtige gespeichert:

- a) *Subjekt*daten: Das sind personenbezogene Daten wie Name, Adresse, Geburtsdatum, Familienstand oder Bankverbindung.
- b) *Verfahrens*daten: Das sind für die Steuererhebung relevante Daten wie Art der Veranlagung (z.B. Betrieb bzw. Arbeitnehmer), Betriebsgröße, Branche, zu erhebende Abgaben oder Bevollmächtigte.
- c) *Einhebungs*daten: Das sind die zeitgeordneten Buchungen auf dem Abgabekonto.
- d) *Bescheid*daten: Das sind die in den Abgabenbescheiden enthaltenen Daten wie Bemessungsgrundlagen (z.B. Einkünfte bzw. Umsätze), Steuerbeträge oder Vorsollbeträge.

Darüber hinaus können - sofern derartige Maßnahmen gesetzt wurden - auch noch Informationen über folgende Vorgänge gespeichert sein:

- Durchführung einer Betriebsprüfung
- Einbringungsmaßnahmen
- Finanzstrafverfahren
- Auszahlungen von Familienbeihilfe

Hinsichtlich der Informationsebene kann festgehalten werden, dass nur der Zugriff auf die Subjektdaten, die Verfahrensdaten und die Einhebungsdaten bundesweit für alle Finanzbediensteten möglich ist, während alle anderen Daten lediglich von Bediensteten der zuständigen Abteilung des zuständigen Finanzamtes sowie den jeweiligen Oberbehörden (Finanzlandesdirektion und Bundesministerium für Finanzen) abgefragt werden können.

Zu 2.:

Da alle Zugriffe auf das AIS mittels "Log - Files" protokolliert und sequentiell gespeichert werden, kann ermittelt werden, wer wann auf welche Daten zugegriffen hat.

Zu 3. und 4.:

Technische Vorkehrungen zur Verhinderung von unerlaubter Daten - Weitergabe bzw. der Verletzung des Steuergeheimnisses werden insbesondere im Bereich des Zugangsschutzes getroffen. Abfragen im AIS können daher nur nach entsprechender persönlicher Identifikation des Bediensteten (USER - ID und Passwort) erfolgen.

Dienstrechtliche Vorkehrungen zur Hintanhaltung von disziplinärem bzw. strafrechtlich relevantem Verhalten sind durch die einschlägigen gesetzlichen Bestimmungen getroffen worden. Ziel dieser Regelungen ist es, Fehlverhalten von Bediensteten zu verhindern und das Ansehen und die Leistungsfähigkeit der Bundesbediensteten zu gewährleisten.

- Bei Mitarbeitern, die in einem öffentlich - rechtlichen Dienstverhältnis stehen, ist bei jedem begründeten Verdacht einer Dienstpflichtverletzung nach den Bestimmungen des § 109ff des Beamten - Dienstrechtsgesetzes 1979 vorzugehen.

Die dienstrechtlichen Folgen eines unerlaubten Zugriffes bzw. der Weitergabe von Daten an Dritte ist disziplinär zu verfolgen und kann je nach den Umständen des Einzelfalles und nach genauer Prüfung der einschlägigen Rechtsvorschriften verschieden geahndet

werden:

Einerseits kann der Dienstvorgesetzte eine Ermahnung oder Belehrung aussprechen, andererseits kann die Dienstbehörde eine Disziplinaranzeige bei der Disziplinar - kommission erstatten, woraufhin ein formelles Disziplinarverfahren durchgeführt wird, das mit Freispruch oder Verurteilung zu einer Geldbuße oder Geldstrafe oder der Entlassung enden kann.

- Bei Vertragsbediensteten sind - je nach der Schwere der Dienstpflichtverletzung - seitens des Dienstgebers die §§ 32 (Kündigung) und 34 (vorzeitige Auflösung des Dienstverhältnisses) des Vertragsbedienstetengesetzes 1948 anzuwenden.

Darüber hinaus normiert § 46 Beamten - Dienstrechtsgesetz 1979 die Amtsverschwiegenheit in Ausführung des verfassungsrechtlichen Gebotes der Amtsverschwiegenheit gemäß Art. 20 Abs. 3 B - VG.

Wird der Verdacht einer von Amts wegen zu verfolgenden strafbaren Handlung bekannt, die den gesetzmäßigen Wirkungsbereich der Behörde betrifft, so hat diese bei Beamten und Vertragsbediensteten nach § 84 Strafprozessordnung (StPO) (Anzeige an die Staatsanwaltschaft oder die Sicherheitsbehörde - Ausnahmen sind in Abs. 2 normiert) vorzugehen.

Zu 5.:

Daten, die sich als falsch erwiesen haben, werden selbstverständlich korrigiert. Allerdings ist darauf hinzuweisen, dass „falsche Daten“, die in eine Erledigung (z.B. Bescheid) eingeflossen sind, lediglich im Zuge der entsprechenden verfahrensrechtlichen Bestimmungen (siehe §§ 243 ff. BAO) richtig gestellt werden können.

Zu 6.:

Pro Jahr werden im AIS ca. 420 Mio. Datentransaktionen durchgeführt.

Zu 7.:

Bereits am 8. November 2000 habe ich eine Arbeitsgruppe zwecks Erarbeitung von Maßnahmen zur Verhinderung unerlaubter Zugriffe auf das AIS eingesetzt. Dabei war aber auch zu berücksichtigen, dass der Arbeitsablauf durch neue Datensicherheitsvorschriften nicht behindert wird.

Als wesentliches Ergebnis dieser Überlegungen soll künftig folgender zusätzlicher Überwachungsmechanismus eingesetzt werden: Den leitenden Funktionären in den Finanzämtern wird wöchentlich eine automationsunterstützt erstellte Liste übermittelt, auf der nach dem Zufallsprinzip ausgewählte Datenabfragen der Mitarbeiter erfasst sind, die jeweils auf ihre Ordnungsmäßigkeit zu überprüfen sind. Dadurch erwarte ich mir eine entsprechende Präventionswirkung.

Zu 8.:

Sollte ein Abgabepflichtiger einen Schaden durch eine vorsätzliche Verletzung der Verpflichtung zur abgabenrechtlichen Geheimhaltung erlitten haben und diesen auch nachweisen können (beispielsweise schlechtere Bankbonitäten), so wäre dieser Schaden im Wege der Finanzprokurator im Amtshaftungsverfahren geltend zu machen.

Zu 9.:

Eine umfassende Aufzählung der wesentlichen gesetzlichen Verpflichtungen aufgrund der gemäß § 48a Abs. 4 lit. b BAO eine Offenbarung von Daten, die grundsätzlich der abgabenrechtlichen Geheimhaltungspflicht unterliegen, dennoch zulässig ist, findet sich im Kommentar der Bundesabgabenordnung (2. Auflage, Wien 1999) von Dr. Christoph Ritz unter § 48a Tz 24 und Tz 28 eine Kopie dieser Bestimmungen liegt in der Anlage bei.