REPUBLIK ÖSTERREICH
DATENSCHUTZKOMMISSION

A-1010 Wien, Hohenstaufengasse 3
Tel. ++43-1-531 15/0
Fax: ++43-1-531 15/2690
e-mail: dsk@dsk.gv.at
DVR: 0000027

K054.101/0002-DSK/2010

An das
Bundesministerium für Finanzen
Abteilung VI/1

per E-Mail: e-recht@bmf.gv.at

Betrifft: Entwurf eines Bundesgesetzes über eine Transparenzdatenbank (Transparenzdatenbankgesetz – TDBG); **Stellungnahme der Datenschutzkommission**

Die Datenschutzkommission nimmt zu dem im Betreff genannten Entwurf wie folgt Stellung:

Zu § 1:

Bei der Transparenzdatenbank handelt es sich um eine Datenanwendung gemäß § 4 Z 7 Datenschutzgesetz 2000 (DSG 2000). Dementsprechend darf ein Eingriff gemäß § 1 Abs. 2 DSG 2000 in das Recht auf Geheimhaltung der Betroffenen nur im überwiegenden Interesse eines Dritten erfolgen, wobei dieser Eingriff in einem Gesetz hinreichend determiniert vorgesehen sein muss. In datenschutzrechtlicher Hinsicht ist es geboten, dass der Zweck der Datenanwendung, die datenschutzrechtliche Rollenverteilung, die Inhalte der Datenbank sowie allfällige Empfänger der Daten bereits im Gesetz klar definiert werden.

Lediglich den Erläuterungen ist zu entnehmen, dass der Leistungsempfänger Zugriff auf verschiedene Datenbanken (darunter die neu zu errichtende Transparenzdatenbank) erhalten soll, um eine Übersicht über sein Einkommen und über Leistungen zu erhalten, die ihm von unterschiedlichen Stellen gewährt wurden. Dies soll der Vereinfachung von Behördenwegen dienen. Aus dem allgemeinen Teil der Erläuterungen ergibt sich weiters, dass für die politischen Entscheidungsträger die Transparenzdatenbank mit bereits vorhandenen Datenbanken ein Controllinginstrument sein soll, mit dem unter anderem vorhandene Doppelförderungen analysiert werden können und ein Überblick über gewährte Leistungen erfolgen kann. Aus der Zusammenschau mit dem Gesetzestext kann dies nur die vorgesehenen statistischen Auswertungen von anonymisierten und aggregierten Daten betreffen, da ansonsten keinerlei Zugriffsrechte (außer des Betroffenen selbst) oder Ähnliches vorgesehen werden.

Es sollte auch aus dem Gesetz klar hervorgehen, dass außer dem Betroffenen selbst niemand Zugriff auf (direkt) personenbezogene Daten der Transparenzdatenbank hat. Vielmehr wird im Hinblick auf den Verhältnismäßigkeitsgrundsatz und das gelindeste zum Ziel führende Mittel angeregt, eine Speicherung in indirekt personenbezogener Form vorzusehen. Dies wäre ausdrücklich im Gesetz festzulegen.

Weiters sollte im Gesetz klar geregelt werden, wer als Auftraggeber gemäß § 4 Z 4 DSG 2000 fungiert bzw. wer als Dienstleister im Sinne des § 4 Z 5 DSG 2000 eingesetzt wird. Nur so kann festgelegt werden, wer welche Pflichten, die sich aus dem DSG 2000 ergeben, zu erfüllen hat. Offenbar ist die Bundesregierung als Auftraggeberin hinsichtlich der Transparenzdatenbank und des Transparenzportals eingerichtet (da von „beauftragen“ die Rede ist). Aus § 21 ergibt sich in weiterer Folge, dass die BRZ GmbH als Dienstleisterin fungiert. Dies sollte eindeutig zum Ausdruck kommen.

Die Datenschutzkommission regt daher an, die notwendigen Determinierungen vorzunehmen.

Zu § 2:

Der Zugriff auf die in der Transparenzdatenbank gespeicherten Leistungen soll gemäß Abs. 1 für den Betroffenen nach Eingabe einer „elektronischen Zugangskennung“ erfolgen, wobei nicht bestimmt ist, um welche Art der Zugangskennung es sich handeln soll. In § 22 Abs. 2 Z 1 wird zwar der Bundesminister für Finanzen ermächtigt, im Einvernehmen mit dem Bundeskanzler die Gewährung einer Zugangskennung festzulegen, die den Voraussetzungen des § 3 des E-Government-Gesetzes (E-GovG) entspricht.

Im elektronischen Verkehr mit Auftraggebern des öffentlichen Bereichs dürfen gemäß den Bestimmungen des E-GovG Zugriffsrechte auf personenbezogene Daten, an welchen ein schutzwürdiges Geheimhaltungsinteresse im Sinne des § 1 Abs. 1 DSG 2000 besteht, nur dann eingeräumt werden, wenn die eindeutige Identität desjenigen, der zugreifen will, und die Authentizität seines Ersuchens nachgewiesen sind. Die eindeutige Identität ist die Bezeichnung der Nämlichkeit eines Betroffenen durch ein oder mehrere Merkmale, wodurch die unverwechselbare Unterscheidung von allen anderen bewirkt wird. Für die Feststellung der eindeutigen Identität bedarf es eines Elements, wodurch diese unverwechselbare Unterscheidung bewirkt wird. Dazu dient die Bürgerkarte mit ihrer qualifizierten digitalen Signatur. Zusätzlich zur eindeutigen Identität muss auch die Authentizität des Ersuchens nachgewiesen werden. Dies erfolgt durch die qualifizierte elektronische Signatur.

In diesem Zusammenhang wird angemerkt, dass der Bürgerkarte (inkl. Handy-Signatur) aus Sicherheitsgründen gegenüber Username/Passwort-Lösungen der Vorzug zu geben ist. Username/Passwort-Lösungen können nämlich wesentlicher leichter kompromittiert werden als Lösungen, die auf der Bürgerkarte aufbauen. Es sollte daher auch für den Zugang zur

Transparenzdatenbank sichergestellt werden, dass nicht von Hackern auf fremde Daten zugegriffen werden kann.

Zu Abs. 2 wird angemerkt, dass die „Haushaltsbetrachtung“ bei Verwendung der Bürgerkarte auch ohne weitere Eingabe einer Zugangskennung möglich wäre, indem Leistungsempfänger, die gemeinsam die erhaltenen Leistungen abfragen wollen, gleichzeitig gemeinsam mit der jeweiligen Bürgerkarte eine Abfrage vornehmen.

Das Abstellen auf die „Haushaltsbetrachtung“ scheint allerdings aus datenschutzrechtlicher Sicht nicht unproblematisch, da bei zusammenlebenden Personen nicht automatisch davon auszugehen ist, dass sie damit einverstanden sind, dass die anderen Mitbewohner ihre Daten einsehen. Grundsätzlich gilt das Grundrecht auf Datenschutz auch zwischen Familienmitgliedern oder anderen miteinander lebenden Personen. Dass es sich bei der „gemeinsamen Eingabe“ einer Kennung immer um eine datenschutzrechtliche Zustimmung nach § 4 Z 14 DSG 2000 handelt, bei der (die auch von der RL 95/46/EG [„EG-Datenschutz-Richtlinie“] geforderte) hinreichende Freiwilligkeit gegeben ist, kann bezweifelt werden.

Zu § 4:

Auch an dieser Stelle wäre auf eine klare datenschutzrechtliche Rollenverteilung zu achten. Auftraggeberin der Auswertungen soll – wie schon oben ausgeführt – offenbar die Bundesregierung sein (und nicht die im zweiten Satz zur Speicherung ermächtigte BRZ GmbH – siehe zur Rolle der BRZ GmbH bei Auswertungen aber die nachstehenden Ausführungen). Daher kann die BRZ GmbH als Dienstleisterin ihr nicht Daten „übermitteln“ (sondern allenfalls „rücküberlassen“, vgl. § 4 Z 11 DSG 2000). In diesem Zusammenhang sollte klargestellt werden, dass die Bundesregierung – obwohl sie datenschutzrechtlicher Auftraggeber ist – keinen Zugriff auf (direkt) personenbezogene Daten der Betroffenen hat. Dies wäre allerdings am besten dadurch zu gewährleisten, dass die Daten bereits indirekt personenbezogen in die Transparenzdatenbank einfließen. Auf der anderen Seite wäre – sofern die Datenbank direkt personenbezogene Daten beinhaltet – der Auftraggeber für die Gewährung von Betroffenenrechten (Auskunfts-, Richtigstellungs- und Löschungsrecht) verantwortlich und hätte dementsprechend auch die Verfahren abzuwickeln. Insofern fragt es sich, ob das vorgeschlagene Konzept, die Bundesregierung als Auftraggeber für die Transparenzdatenbank fungieren zu lassen, überhaupt zielführend ist.

Für die in Abs. 1 zweiter Satz vorgesehene Speicherung von Daten sollten konkrete, über das DSG 2000 hinausgehende Datensicherheitsmaßnahmen im Gesetz normiert werden.

Unklar scheint, was damit gemeint ist, dass der jeweilige Bundesminister „im Rahmen seines Wirkungsbereiches über Daten verfügen“ kann. Die Formulierung ist insofern missverständlich, als sie auch derart verstanden werden könnte, dass der Bundesminister generell ohne nähere gesetzliche Ermächtigung zur Verwendung personenbezogener, in seinem Ressort

vorhandener Daten (samt Vornahme von Auswertungen) ermächtigt wird, was viel zu unbestimmt und daher mit § 1 Abs. 2 DSG 2000 nicht vereinbar wäre, wenn es sich um personenbezogene Daten handelt. Insbesondere wäre die Einrichtung einer umfassenden Datei über einzelne Personen, bei der Daten aus verschiedenen Verwaltungsbereichen verknüpft werden, bei einzelnen Bundesministern unzulässig. Wenn mit dem letzten Satz des Abs. 1 bloß ausgedrückt werden soll, dass sich durch die Übermittlung von Daten an die Transparenzdatenbank durch diesen Bundesminister nichts an dessen Stellung als datenschutzrechtlicher Auftraggeber für andere Datenanwendungen ändert, dann sollte der Entwurf entsprechend präzisiert werden.

Zu den §§ 15 bis 17:

In § 16 Abs. 2 wäre der Ausdruck „Zurverfügungstellen“ durch den datenschutzterminologisch richtigen Ausdruck „Übermittlung“ zu ersetzen.

Weiters scheint es im Lichte des Verhältnismäßigkeitsgrundsatzes als ausreichend, diese Übermittlung anonymisiert bzw. nur mit verschlüsselten bPK vorzunehmen.

Die Treffsicherheit bei der Abfrage von Datenbanken ist Grundvoraussetzung für eine korrekte Zuordnung der Daten zur Person. Bei Verwendung von Namen und Geburtsdatum als Suchkriterien in Datenbanken ist diese korrekte Zuordnung nicht möglich. Auch eine Verwendung der Sozialversicherungsnummer (wie in § 17 Abs. 1 Z 3 normiert) als Suchkriterium ergibt – wie es die Praxis gezeigt hat – besonders bei einer Abfrage über mehrere Verwaltungsbereiche in einer Vielzahl von Fällen nicht zulässige Falschzuordnungen. Es sind daher die Suchkriterien Namen und Geburtsdatum sowie Sozialversicherungsnummer abzulehnen, da Mehrfachtreffer oder Falschzuordnungen denkbar sind. In diesem Zusammenhang wird auch auf die Stellungnahme des Datenschutzrates vom 25. Februar 2010 verwiesen, in der festgehalten wird, dass eine Verwendung der Sozialversicherungsnummer für Bereiche, die nicht in der Ingerenz der Sozialversicherung liegen, aus datenschutzrechtlicher Sicht abzulehnen und den E-Government-Lösungen des Bundes unter Gewähr der höchstmöglichen Datensicherheitsmaßnahmen der Vorzug zu geben ist. Die Verwendung von bPK stellt (wie bereits im Rahmen der Registerzählung erfolgt) das gelindere Mittel bei der Verwendung der personenbezogenen Daten dar, da diese nur mehr indirekt personenbezogen und damit für den Auftraggeber und Dienstleister nicht auf konkrete Personen rückführbar sind. Es wird daher empfohlen, entsprechend der E-Government-Strategie des Bundes für die Zuordnung zu Personen bPK zu verwenden.

In § 17 Abs. 1 Einleitungssatz sollte – den Erläuterungen entsprechend – das Wort „insbesondere“ entfallen und eine taxative Aufzählung aufgenommen werden.

Zu den §§ 20 und 21:

§ 20 erster Satz dürfte davon ausgehen, dass die mitgeteilten Daten und der Inhalt der Transparenzdatenbank stets übereinstimmen. Die Frage der Verantwortung stellt sich – sollte nicht das Konzept der indirekt personenbezogenen Daten aufgegriffen werden – aber gerade in den Fällen, in denen hier Divergenzen auftreten; vor diesem Hintergrund erscheint die Bedeutung des § 20 erster Satz im Zusammenhang mit der Regelung des § 21 Abs. 2 unklar. Für den Betroffenen stellt sich im Zusammenhang mit diesen Regelungen vor allem die Frage, wie und bei wem das Auskunfts- und Richtigstellungs- oder Löschungsrecht geltend gemacht werden kann. Es ist wird daher nochmals auf die Notwendigkeit hingewiesen, die Verantwortung insb. für die Frage der Datenaktualität und -richtigkeit durch eine klare datenschutzrechtliche Rollenverteilung eindeutig festzulegen. Auch im Lichte der EG-Datenschutzrichtlinie ist es geboten, dass für jede Datenanwendung ein Auftrageber („für die Verarbeitung Verantwortlicher“ in der Diktion der Richtlinie) vorhanden sein muss, dem die Rechte und Pflichten nach § 1 Abs. 1 sowie den §§ 24 ff DSG 2000 zugeordnet sind, auch wenn die faktische Erfüllung dieser Rechte und Pflichten teilweise im Innenverhältnis durch einen Dienstleister erfolgt. Datenschutzrechtlich ist der Auftraggeber für die Richtigkeit der verwendeten Daten verantwortlich. Die Formulierung, dass der Dienstleister „vertraglich zur Einhaltung sämtlicher Datenschutzbestimmungen“ verpflichtet werden soll, scheint missverständlich. Vielmehr muss die BRZ GmbH die in § 11 DSG 2000 normierten Dienstleisterpflichten einhalten. Diese datenschutzrechtliche Rollenverteilung und damit verbundenen Verantwortlichkeiten können auch nicht geändert werden. Die Haftungsregelung sollte nicht darauf beschränkt werden, zu normieren, wer für etwas nicht haftet, sondern auszusprechen, wer tatsächlich die Verantwortung trägt.

Zu § 22:

Es wird angeregt, bei den Verordnungsermächtigungen zu Eingriffen in das Grundrecht auf Datenschutz (§ 22 Abs. 1) im Gesetz wesentlich detailliertere Festlegungen vorzunehmen.

Wie oben bereits ausgeführt, sollen grundlegenden Datensicherheitsbestimmungen bereits im Gesetz selbst festgelegt werden. Es wird aber angeregt, eine Verordnungsermächtigung für eine detaillierte Regelung der technischen und organisatorischen Datensicherheitsstandards vorzusehen.

Diese Stellungnahme wird im auch dem Präsidium des Nationalrats zur Kenntnis gebracht.

27. September 2010
Für die Datenschutzkommission
Das geschäftsführende Mitglied:
SOUHRADA-KIRCHMAYER