REPUBLIK ÖSTERREICH DATENSCHUTZRAT

BALLHAUSPLATZ 2, A-1014 WIEN
GZ ● BKA-817.413/0002-DSR/2010
TELEFON ● (+43 1) 53115/2527
FAX ● (+43 1) 53115/2702
E-MAIL ● DSRPOST@BKA.GV.AT
DVR: 0000019

An das
Bundesministerium für Finanzen

Per E-Mail:
e-Recht@bmf.gv.at

Betrifft: Bundesgesetz über eine Transparenzdatenbank (Transparenzdatenbankgesetz – TDBG)

Stellungnahme des Datenschutzrates

Der **Datenschutzrat** hat in seiner 199. Sitzung am 28. September 2010 **mehrheitlich – mit einer Gegenstimme beschlossen** – zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

1) Vorbemerkungen:

Vorweg ist zu bemerken, dass die primäre Aufgabe des Datenschutzrates darin besteht, die Bundesregierung in rechtspolitischen Fragen des Datenschutzes zu beraten (§ 41 Abs. 2 DSG 2000). Dem Datenschutzrat obliegt aber keine darüber hinaus gehende Beurteilung von Gesetzesvorhaben hinsichtlich derer politischen Notwendigkeit und Zweckmäßigkeit. Gegen die im Entwurf vorgesehene Einführung einer Transparenzdatenbank bestehen aus Sicht des Datenschutzrates dann keine Einwände, wenn die nachstehenden datenschutzrechtlichen Determinanten eingehalten werden, die sich insbesondere aus der europäischen Datenschutz-Richtlinie 95/46/EG und aus dem DSG 2000 ergeben.

2) Datenschutzrechtlich relevante Bestimmungen:

Gegen die im Entwurf vorgesehene Einführung einer Transparenzdatenbank bestehen aus Sicht des Datenschutzrates dann keine Einwände, wenn die datenschutzrechtlichen Determinanten eingehalten werden.

Insbesondere werden folgende Punkte zu berücksichtigen sein:

Die vorgesehene gesetzliche Regelung ist in mehrerer Hinsicht zu unbestimmt, um überhaupt beurteilen zu können, ob die Datenverwendung im Lichte des Grundrechts auf Datenschutz und der gemäß § 1 Abs. 2 DSG 2000 zulässigen Ausnahmen gerechtfertigt ist.

Zudem merkt der Datenschutzrat vorweg an, dass die Bundesregierung offenbar als Auftraggeberin hinsichtlich der Transparenzdatenbank und des Transparenzportals eingerichtet (arg. „beauftragen“) wird. Aus § 21 ergibt sich in weiterer Folge, dass die BRZ GmbH als Dienstleisterin fungiert. Dies sollte in der Textierung eindeutig zum Ausdruck kommen.

Der Datenschutzrat weist jedoch darauf hin, dass die Bundesregierung in diesem Fall die Pflichten des Auftraggebers treffen würde, die sich nicht nur aus dem DSG 2000, sondern auch als „für die Verarbeitung Verantwortlicher“ („Auftraggeber“ iSd DSG 2000) aus der Datenschutz-Richtlinie 95/46/EG ergeben.

Die gesamte Bundesregierung wäre somit für die Rechte der Betroffenen auf Auskunft, Richtigstellung, Löschung und Widerspruch (§§ 26 ff DSG 2000) verantwortlich. Eventuelle Beschwerden gemäß § 31 DSG 2000 an die Datenschutzkommission, würden sich daher gegen die Bundesregierung richten.

Der Datenschutz regt daher in diesem Zusammenhang an, dass die Bundesregierung hinsichtlich der Auftraggeberfunktion eine andere Konstruktion wählen sollte, die die Betroffenenrechte gemäß § 26 ff DSG 2000 besser wahren kann.

Fraglich ist, **welcher Zweck** mit der Transparenzdatenbank genau verfolgt werden soll: Aus dem vorliegenden Gesetzestext ergibt sich jedenfalls, dass der Leistungsempfänger Zugriff auf die Datenbank erhalten soll, um insbesondere eine Übersicht über Leistungen zu erhalten, die ihm von unterschiedlichen Stellen gewährt wurden. Überdies sind nach § 4 des Entwurfes Auswertungen möglich, wobei es sich – wie auch in den Erläuterungen ausgeführt wird – hier um die Auswertung von Daten in aggregierter und anonymisierter Form handelt.

Äußerst unklar ist insbesondere, was in § 4 Abs. 1 letzter Satz gemeint ist, dass der jeweilige Bundesminister „im Rahmen seines Wirkungsbereiches über Daten verfügen“ kann. Sofern geplant sein sollte, die Daten auch für andere Zwecke als für Auswertungen zu verwenden bzw. bestimmten Stellen eine personenbezogene Abfrage zu ermöglichen, wie etwa die Möglichkeit der Einschau einer leistenden Stelle in die Datenbank, ob für die Person bereits eine bestimmte Förderung gewährt wurde, damit eine doppelte Auszahlung vermieden wird, müsste dies **explizit gesetzlich verankert** werden. Sollten derartige Möglichkeiten angedacht werden, müsste insbesondere der **Grundsatz der Verhältnismäßigkeit** – wobei Engriffe in das Grundrecht auf Datenschutz nur jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden dürfen - berücksichtigt werden.
Insbesondere ist etwa die **Einrichtung einer umfassenden Datei über einzelne Personen beim Bundesministerium für Finanzen, aus der ein „Profil“ der jeweiligen Person erstellt werden könnte, aus datenschutzrechtlicher Sicht strikt abzulehnen**, da nicht sichergestellt ist, dass nicht aus verschiedenen Verwaltungsbereichen Daten unzulässigerweise personenbezogen verknüpft werden könnten und somit die datenschutzrechtlichen Vorgaben nicht mehr eingehalten werden. Es wäre daher der Entwurf entsprechend zu schärfen, um diesen nicht wünschenswerten Fall klar auszuschließen.

Zu § 1:

In datenschutzrechtlicher Hinsicht ist grundsätzlich festzuhalten, dass es sich bei Transparenzportal und Transparenzdatenbank trotz der fehlenden Zugriffsrechte für andere als die Betroffenen dennoch um Datenanwendungen im Sinn des § 4 Z 7 Datenschutzgesetz 2000 (DSG 2000) und damit um einen Eingriff in das Recht auf

Geheimhaltung der von einer Datenverwendung Betroffenen nach § 1 Abs. 1 DSG 2000 handelt. Somit bedarf es nach § 1 Abs. 2 DSG 2000 eines überwiegenden berechtigten Interesses an diesem Eingriff, der darüber hinaus in einem Gesetz hinreichend bestimmt vorgesehen sein muss. Speziell zum Transparenzportal ist darauf hinzuweisen, dass die Verwendung von Daten auch ohne Speicherung einen Eingriff bedeutet (so zB auch die Echtzeitüberwachung nach § 50a Abs. 4 Z 3 DSG 2000).

Im Hinblick auf die hinreichende Bestimmtheit ist aus datenschutzrechtlicher Sicht zunächst von besonderer Bedeutung, dass die Rollenverteilung der einzelnen Akteure klar definiert wird, dh es muss im Gesetzestext deutlich definiert 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. Denn nur so kann festgelegt werden, wer welche Pflichten, die sich aus dem DSG 2000 ergeben, zu erfüllen hat.

Weiters kann dem Gesetzestext der Zweck der Errichtung des Transparenzportals bzw. der Transparenzdatenbank nicht klar entnommen werden. Lediglich den Erläuterungen ist zu entnehmen, dass der Leistungsempfänger Zugriff auf verschiedenen 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 (Servicezwecke). Aus dem allgemeinen Teil der Erläuterungen ergibt sich weiters, dass für die politischen Entscheidungsträger die Transparenzdatenbank mit bereits vorhanden 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. **Sollten solche weiteren Zugriffsrechte jedoch in weiterer Folge aufgenommen werden, wäre dies ausdrücklich im Gesetz zu verankern und einer neuerlichen Verhältnismäßigkeitprüfung im Sinne des DSG 2000 zu unterziehen.**

Der Datenschutzrat regt an, dass im Gesetz ergänzt wird, nach welchen Kriterien die Auswertungen vorgenommen werden.

Hinsichtlich der Wichtigkeit der genauen Bestimmung des Zwecks ist auch auf die Schlussanträge zu den verbundenen EuGH-Rechtssachen C-92/09 und C-93/09 betreffend die unionsrechtlich gebotene Publikation von Agrardaten zu verweisen. Dort wird ausgeführt, dass das verantwortliche gesetzgeberische Organ in der Lage sein muss, zu erläutern, weshalb der Eingriff (dort eine – sicherlich eingriffsintensivere – Veröffentlichung) im Hinblick auf das verfolgte spezifische Ziel erforderlich, geeignet und verhältnismäßig ist (vgl. RdNr. 120). Die Verhältnismäßigkeit ist an Hand des angestrebten Endergebnisses zu prüfen (vgl. RdNr. 118).

Des Weiteren sollten die Inhalte der Transparenzdatenbank, die sich wohl nur aus § 15 Abs. 2 erschließen lassen, ebenso klar im Gesetz geregelt werden wie der Grad, in dem eine Speicherung in personenbezogener Form erfolgen soll.

Aus all dem folgt, dass § 1 des Entwurfs aus datenschutzrechtlicher Sicht wohl als zu unbestimmt anzusehen ist und detaillierter ausgestaltet werden sollte.

Die Ausführungen, dass die Transparenzdatenbank der Speicherung der mitgeteilten Leistungen und das Transparenzportal der Darstellung der Leistungen sowie des Einkommens des Leistungsempfängers dienen, ist **nicht ausreichend**, um die **Verhältnismäßigkeit des Grundrechtseingriffs (vgl. § 1 DSG 2000) näher zu erläutern**. Im Hinblick auf den Zweck „Information der Leistungsempfänger“ ist darüber hinaus fraglich, ob bei der Sammlung von Daten durch eine Behörde (die Bundesregierung) dafür tatsächlich von einem überwiegenden berechtigten Interesse ausgegangen werden kann. Schließlich sollte jeder Leistungsempfänger auch selbst in der Lage sein, sich diese Informationen ohne viel Aufwand zu beschaffen. Es handelt sich also um ein reines „vor Augen Führen“.

Zu § 2:

Der vorliegende Entwurf regelt die umfassende Speicherung von Daten und den Zugriff auf definierte Leistungen. Der Zugriff auf diese Leistungen soll gemäß Abs. 1 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; dies scheint aber nicht ausreichend determinierend zu sein.

Vielmehr ist es aufgrund des Umfangs und der Art der in der Transparenzdatenbank gespeicherten Daten unabdingbar, bereits im Gesetz die Art des Zugangs konkret festzulegen.

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 (chipkartenbasierend oder in Form der Handy-Signatur). Zusätzlich zur eindeutigen Identität muss auch die Authentizität des Ersuchens nachgewiesen werden. Dies erfolgt durch die qualifizierte elektronische Signatur.

Anzumerken ist in diesem Zusammenhang noch, dass grundsätzlich der Bürgerkarte bzw. Handy-Signatur aus Sicherheitsgründen gegenüber Username/Passwort-Lösungen (etwa Zugang über eine FinanzOnline-Zugangskennung) 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 aus diesen Erfahrungen profitiert und sichergestellt werden, dass nicht von Hackern auf fremde Daten zugegriffen werden kann.

Zu Abs. 2 ist anzumerken, 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.

Anzumerken ist allerdings, dass der Klammerausdruck (Haushaltsbetrachtung) nicht sachgerecht erscheint, da nach dem in der österreichischen Rechtsordnung verwendeten Begriff privater Haushalt darunter gewöhnlich „*alle in einer Wohnung oder einer sonstigen Unterkunft in einer Wirtschaftsgemeinschaft zusammen lebenden Personen*“ zu verstehen sind. Eine Beschränkung der Abfragemöglichkeit auf jeweils diesen Personenkreis lässt sich dem in § 2 Abs. 2 vorgesehenen Modell der Transparenzportalabfrage in keiner Weise entnehmen. Weiters ist darauf hinzuweisen, dass gerade in Familiensituationen fraglich erscheinen kann, ob die für eine datenschutzrechtliche Zustimmung nach § 4 Z 14 DSG 2000 (als solche wird man die gleichzeitige Eingabe der Zugangskennung zu werten haben) erforderliche Freiwilligkeit gegeben ist. Dies ist vor dem Hintergrund zu sehen, dass schutzwürdige Geheimhaltungsinteressen auch zwischen Personen bestehen, die in einem gemeinsamen Haushalt leben.

Zu § 3:

Es sollte erwogen werden, eine nähere Zweckbestimmung des Transparenzportals vorzunehmen.

Im vorliegenden Gesetzesentwurf finden sich keine Regelungen zu allfälligen Streitigkeiten zwischen der Bundesregierung und der an das Transparenzportal übermittelnde Institutionen über die zu übermittelnden Daten.

Der Datenschutzrat hält es daher für sinnvoll, für derartige Fälle eine Schlichtungsstelle im Gesetz vorzusehen.

Zu § 4:

Zunächst ist darauf hinzuweisen, dass der in Abs. 1 erster Satz vorgesehene **„Beschluss der Bundesregierung**“ mehrfache Rechtswirkungen entfaltet. Einmal dürfte er im Sinn einer reinen „Selbstbindung“ Voraussetzung für einen Auftrag an die BRZ GmbH sein. Er ist aber auch Tatbestandsvoraussetzung für die mit einem Eingriff in das Recht auf Geheimhaltung verbundene Gruppierung und Zusammenfassung, so dass auch die Voraussetzungen des Beschlusses näher zu determinieren wären.

Auch an dieser Stelle wäre auf eine klare datenschutzrechtliche Rollenverteilung zu achten.

Auftraggeberin der Auswertungen soll wie schon oben ausgeführt offenbar die Bundesregierung (und nicht die im zweiten Satz zur Speicherung ermächtigte BRZ GmbH) sein. Daher kann die BRZ GmbH als Dienstleisterin ihr nicht Daten übermitteln (sondern allenfalls rücküberlassen, § 4 Z 11 DSG 2000). Mit dem letzten Satz des Abs. 1, wonach die Kompetenz jedes Bundesministers im Rahmen seines Wirkungsbereichs über Daten zu verfügen und Auswertungen von Daten zu beauftragen, soll wohl bloß ausgedrückt werden, dass sich durch die Übermittlung von Daten an die Transparenzdatenbank durch diesen Bundesminister nichts an dessen Stellung als datenschutzrechtlicher Auftraggeber für andere Datenanwendungen ändert. **Die Formulierung erscheint aber missverständlich, sie könnte auch derart verstanden werden, dass der Bundesminister generell ohne nähere gesetzliche Ermächtigung zur Verwendung personenbezogener Daten (samt Vornahme von Auswertungen) in seinem Ressort vorhandenen Daten ermächtigt wird, was viel zu unbestimmt und daher mit § 1 Abs. 2 DSG 2000 nicht vereinbar wäre.**

Weiters ist der Zugriff für derartige Auswertungen auf die Daten aus der Transparenzdatenbank nicht ausreichend geregelt, auch hier scheint eine genauere Determinierung erforderlich. Für die in Abs. 1 zweiter Satz vorgesehene Speicherung von Daten (wohl in personenbezogener Form) erscheinen zusätzliche Datensicherheitsmaßnahmen angebracht.

Aus Sicht des Datenschutzrates ist es erforderlich, hinsichtlich der Sicherheitsmaßnahmen spezielle Regelungen im Gesetz selbst oder durch eine zukünftige Verordnung vorzusehen.

Darüber hinaus wird angeregt, die **Bundesanstalt Statistik Österreich** generell für die Auswertungen als Dienstleister heranzuziehen, da die Statistik Österreich bereits über das erforderliche Fachwissen und die notwendige Infrastruktur verfügt, um diese Auswertungen unter Anwendung des Konzepts der bereichsspezifischen Personenkennzeichen (bPK) und somit datenschutzgerecht anonymisiert und aggregiert durchzuführen. Die Statistik Österreich hat zudem solche Auswertungen

bereits im Rahmen der Volks-, Arbeitsstätten-, Gebäude- und Wohnungszählung auf Grundlage des Registerzählungsgesetzes durchgeführt. Die Heranziehung der Statistik Österreich auf „verwaltungsökonomische Gründe“ (Abs. 2) zu beschränken, ist daher zu eng. Aus Gründen der Zweckmäßigkeit und Einfachheit sollte immer die Statistik Österreich als Dienstleister herangezogen werden.

Außerdem unterliegt die Bundesanstalt Statistik Österreich bei der Wahrnehmung von statistischen Aufgaben den Grundsätzen des § 24 Bundesstatistikgesetzes 2000 und der EU-Verordnung (EG) Nr. 223/2009 über die Gemeinschaftsstatistiken, ABl. Nr. L 87 vom 31.03.2009, S 164, die die erforderliche Objektivität, Sachlichkeit und Qualität der statistischen Auswertungen sowie Vertraulichkeit der Daten gewährleisten. Seitens der EU-Kommission wurden im Rahmen von Benchmarkings alle statistischen Ämter der Mitgliedstaaten geprüft, bei denen die Bundesanstalt Statistik Österreich zuletzt im Jahr 2006 gemeinsam mit dem Statistikamt von Finnland den ersten Rang erreicht hat.

Um bei den Auswertungen die notwendige sachliche Autorität, Qualität und Objektivität sicherzustellen, ist es daher angezeigt, die für diese Aufgaben in Europa führende Institution in Österreich, nämlich die Bundesanstalt Statistik Österreich heranzuziehen.

Außerdem können von der Bundesanstalt Statistik Österreich **über bPK unter Wahrung des Datenschutzes** auch Auswertungen mit Haushaltszusammenhang, auf lokaler Ebene usw. durchgeführt werden, was auf eine andere Weise ordnungsgemäß nicht möglich ist, sodass ohne zusätzlichen Aufwand die Daten der Transparenzdatenbank aussagekräftiger ausgewertet werden können. Der Grundsatz der Sparsamkeit, Zweckmäßigkeit und Wirtschaftlichkeit gebietet es daher, dass die Bundesanstalt Statistik Österreich die Auswertungen vornimmt.

Zu § 15:

Nochmals ist an dieser Stelle zu betonen, dass **der Zweck, der Inhalt und die Form der Speicherung von Daten in der Transparenzdatenbank aus dem Entwurf nicht klar hervorgehen, was ihre datenschutzrechtliche Zulässigkeit grundsätzlich in Frage stellt**. Weiters erfolgt keine Regelung, inwieweit auf die Transparenzdatenbank zugegriffen werden darf, um etwa Richtigstellungen bzw. Löschungen (§ 27 DSG 2000) vornehmen zu können.

Zu § 16:

Nach § 16 Abs. 2 haben der Bundesminister für Finanzen, das AMS bzw. der Hauptverband der Sozialversicherung der BRZ GmbH zum Zweck der Erstellung der Auswertungen die dafür erforderlichen Daten aus ihren Datenbanken zur Verfügung zu stellen. Um Unklarheiten zu vermeiden, sollten datenschutzrechtliche Begriffe verwendet werden. Wenn es sich bei diesem „Zurverfügungstellen“ um eine Übermittlung im datenschutzrechtlichen Sinn, also um eine Übermittlung vom Auftraggeber (BMF, AMS, HV) an die Bundesregierung (als Auftraggeberin der Transparenzdatenbank) handelt, sollte dies auch so bezeichnet werden. Weiters stellt sich im Lichte des Verhältnismäßigkeitsgrundsatzes die Frage, ob es ausreichend wäre diese Übermittlung anonymisiert bzw. nur mit verschlüsselten bPK vorzunehmen.

Zu § 17:

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 in vielen Fällen nicht möglich (man denke etwa an die zahlreichen Namensdoubletten). 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. Aus **E-Government-Sicht** sind daher die Suchkriterien Namen und Geburtsdatum sowie Sozialversicherungsnummer abzulehnen, da Mehrfachtreffer oder Falschzuordnungen nicht nur wahrscheinlich sind, sondern in vielen Fällen auch stattfinden werden.

Aus datenschutzrechtlicher Sicht ist die Schlussfolgerung des Datenschutzrates in der Stellungnahme vom 25. Februar 2010 hervorzuheben, 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.

Um die gesetzlichen Vorgaben zu erfüllen, soll daher umfassend das **System der bPK** eingesetzt werden, das eine eindeutige Zuordnung der Personen in den jeweiligen Datenbanken garantiert. Da bereits eine Reihe von Behörden ihre Datenbanken (etwa auf Grund der Bestimmungen des Registerzählungsgesetzes) mit bPK ausgestattet hat, ist die Verwendung von bPK nicht nur zu präferieren sondern auch leicht umsetzbar, da die Mechanismen bereits zur Verfügung stehen. Derzeit sind **ca. 68 Mio. direkt und ca. 180 Mio. verschlüsselt mit bPK ausgestattete personenbezogene Datensätze** vorhanden. Für die Behörden, die noch keine bPK-Ausstattung ihrer Datenbank vorgenommen haben, ist diese nachträglich leicht möglich. Dies kann in Form einer sogenannten Gesamtausstattung der Datenbank (allen in der Datenbank vorhandenen natürlichen Personen werden bPK zugeordnet) erfolgen. Falls eine Gesamtausstattung nicht tunlich ist, kann ein Modul zur Integration in das bestehende Formular (zB eines Förderantrags) bereitgestellt werden, um im Hintergrund automatisch eine bPK zu vergeben oder ein elektronisches Service im Rahmen der Datenschnittstelle zur Erstellung von bPK integriert werden. Abschließend wäre in diesem Zusammenhang noch anzumerken, dass durch die Verwendung von bPK eine automatisierte und vor allem anonymisierte Verwendung der personenbezogenen Daten ermöglicht wird. Dies war auch im Bereich der Umgestaltung der seinerzeitigen „Volkszählung“ eine wesentliche Forderung aus datenschutzrechtlicher Sicht, der vom Parlament mit dem Registerzählungsgesetz Rechnung getragen wurde. Dabei werden die Daten an die zentrale Datenbank nicht mit einem Namen übermittelt, sondern mit einer Kennzahl, die nur der Absender, nicht aber der Empfänger entschlüsseln kann. Der Empfänger kann sie aber dann durchaus zusammenführen, statistisch auswerten und Fallprofile erstellen; er weiß aber nie, wie die Person heißt, die sich „hinter der Ziffer verbirgt“. Bisher arbeiten die großen Datenaustauschsysteme auf dieser Basis. Man wird gebotener Weise dieses Verschlüsselungssystem auch bei der Transparenz-datenbank anwenden müssen.

Aus E-Government-Sicht und aus datenschutzrechtlicher Sicht ist daher der Verwendung von bereichsspezifischen Personenkennzeichen gegenüber der Verwendung der Sozialversicherungsnummer der Vorzug zu geben. Die Verwendung von bPK gewährleistet (wie bereits im Rahmen der

Registerzählung erfolgt) eine anonymisierte Verwendung der personenbezogenen Daten.

Zu erinnern ist in diesem Zusammenhang, dass seinerzeit im Gesetzgebungsprozess für das Bundesstatistikgesetz 2000 ursprünglich die Zusammenführung der Daten über die Sozialversicherungsnummer vorgesehen war. Dies wurde sowohl vom Datenschutzrat als auch von der Datenschutzkommission entschieden abgelehnt. Dabei ist noch zu bedenken, dass damals das Instrument der bPK noch nicht zur Verfügung stand. An dieser Haltung ist keine Änderung eingetreten, zumal nunmehr ohne Sozialversicherungsnummer über bPK datenschutzkonform Daten aus unterschiedlichen Quellen zusammengeführt werden können.

Da die anonymisierten Daten der Transparenzdatenbank auch für andere Statistiken von Bedeutung sind, ist es auch aus Gründen einer Reduzierung der Kosten der statistischen Erhebungen und Entlastung der leistenden Stellen erforderlich, in der Transparenzdatenbank zu den Daten und dem bPK für die Transparenzdatenbank das verschlüsselte bPK-AS (Amtliche Statistik) zu führen, um bei statistischen Erhebungen im Anlassfall anonymisiert Daten aus der Transparenzdatenbank und aus anderen Quellen zusammenführen zu können.

Schließlich sollte in § 17 Abs. 1 Einleitungssatz das Wort „insbesondere“ entfallen, da nicht ersichtlich ist, auf Grund welcher Parameter weitere Inhalte verpflichtend in die Mitteilung aufzunehmen wären.

Der Datenschutzrat regt an, dass in der noch mit den Ländern zu schließenden Vereinbarung gemäß Art. 15a B-VG, die Länder dazu verpflichtet werden sollen, bei bestimmten Behörden eigens ermächtigte Organwalter iSd E-GovG vorzusehen, die für Betroffene – insbesondere für Menschen ohne Internetzugang – auf deren Verlangen Verfahrenshandlungen in bürgerkartentauglichen Verfahren setzen können.

Zu § 18:

Abs. 2 normiert, dass eine nachträgliche Änderung unverzüglich nach der Änderung zu übermitteln ist. Fraglich ist, wie die Änderung dann in der Transparenzdatenbank erfolgt bzw. wer diese durchführt.

Zu den §§ 20 und 21:

Der erste Satz ist höchst unbestimmt und dürfte außerdem davon ausgehen, dass der Inhalt der abgerufenen Daten und der Inhalt der Transparenzdatenbank stets übereinstimmen. Gerade wenn hier Divergenzen auftreten, stellt sich aber die Frage der Datenaktualität und –richtigkeit sowie der Verantwortung hiefür. Daher ist an dieser Stelle noch einmal anzuraten, diese Verantwortung 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.**

Die Formulierung, dass der Dienstleister „vertraglich zur Einhaltung sämtlicher Datenschutzbestimmungen" verpflichtet werden soll, scheint missverständlich und ist in dieser Form rechtlich äußerst fragwürdig. Vielmehr muss die BRZ GmbH die in § 11 DSG 2000 normierten Dienstleisterpflichten einhalten. **Die datenschutzrechtliche Rollenverteilung und damit verbundenen Verantwortlichkeiten können jedoch nicht geändert werden. So ist datenschutzrechtlich etwa der Auftraggeber für die Richtigkeit der verwendeten Daten verantwortlich. Soweit ersichtlich, agiert die Bundesregierung als Auftraggeber. Dies sollte auch ausdrücklich klargestellt werden.**

Die Haftungsregeln sind unvollständig. Es wird lediglich geregelt, wer NICHT haftet, nicht jedoch wer tatsächlich die Verantwortung trägt. **Die Regelungen zur Auftraggeberhaftung sollten dementsprechend ergänzt bzw. detaillierter ausgeführt werden.**

Der Datenschutzrat regt zur Klarstellung überdies an, dass im Gesetzestext durch eine ausdrückliche Formulierung klargestellt wird, dass die Datenschutzkommission für Beschwerden im Zusammenhang mit der Verwendung von Daten in der Transparenzdatenbank zuständig ist.

§ 21 verweist aber auf den rechtswidrigen Umgang mit Daten im Zusammenhang mit der Transparenzdatenbank und auf die §§ 51 und 52 DSG 2000, nicht jedoch auf die einschlägigen Bestimmungen in §§ 118a ff StGB.

In Anbetracht des Datenvolumens in der Transparenzdatenbank und der Menge an sensiblen Daten sollte aus Sicht des Datenschutzrates zu Präventionszwecken und zur Abschreckung vor Datenmissbrauch (z.B. Identitätsdiebstahl) bzw. rechtswidrigem Umgang mit Daten aus der Transparenzdatenbank eine eigene gerichtliche Strafbestimmung in diesem Gesetz geschaffen werden.

Zu § 22:

Eingriffe in das Grundrecht auf Datenschutz müssen im Gesetz vorgesehen sein (siehe die Verfassungsbestimmung des § 1 Abs. 2 DSG 2000). **Eine Erweiterung der in die Transparenzdatenbank zu übermittelnden Daten durch eine Transparenzdatenbank-Leistungsverordnung ist nicht ohne weiters möglich.**
Ohne entsprechende Determinierung soll die Bundesregierung durch Verordnung zu Eingriffen in das Recht auf Geheimhaltung ermächtigt werden. Eine solche Ermächtigung müsste aber aus datenschutzrechtlichen Gründen schon im Gesetz viel detaillierter vorherbestimmt werden.
In Abs. 2 fehlen nähere Bestimmungen zu Datensicherheitsmaßnahmen.

Da davon auszugehen ist, dass die Festlegungen der Transparenzdatenbank-Betriebsverordnung jedenfalls zu ergehen haben, sollte in Abs. 2 eine verpflichtende Verordnungserlassung normiert werden.

Unklar ist, was mit der Regelung des Abs. 2 Z 2 und 5 jeweils letzter Halbsatz (Zugriff über eine bestimmte geeignete öffentlich-rechtliche oder privatrechtliche Übermittlungsstelle) gemeint ist; dies sollte zumindest in den Erläuterungen näher dargelegt werden.

Zu § 26:

Der Datenschutzrat weist zur Klarstellung darauf hin, dass durch die in § 26 Abs. 3 getroffene Regelung die Rechte des Betroffenen auf Auskunft, Richtigstellung, Löschung und Widerspruch (§§ 26 ff DSG 2000) nicht eingeschränkt werden können.

Hinsichtlich der vorgesehenen Vorgangsweise der Bundesregierung wurde von Dr. Zeger ein Votum Separatum eingelegt. Dieses Votum Separatum wird nachgereicht.

1. Oktober 2010
Für den Datenschutzrat:
Der Vorsitzende:
MAIER

Elektronisch gefertigt