DIE ÖSTERREICHISCHEN RECHTSANWÄLTE

Bundesministerium für Inneres
Sektion III/1-Legistik
Herrengasse 7
1014 Wien

per E-Mail: begutachtungsverfahren@parlament.gv.at
bmi-III-1@bmi.gv.at
begutachtung@bmi.gv.at

Zl. 13/1 12/131

BMI
BG, mit dem das Personenstandsgesetz 2013 erlassen sowie das Staatsbürgerschaftsgesetz 1985, das Meldegesetz 1991 und das Namensänderungsgesetz geändert werden und das Personenstandsgesetz aufgehoben wird
BMI-LR1365/0015-III/1/2012

Referent: Dr. Günther Leissler, Rechtsanwalt in Wien

Sehr geehrte Damen und Herren!

Der Österreichische Rechtsanwaltskammertag (ÖRAK) dankt für die Übersendung des Entwurfes und erstattet dazu folgende

S t e l l u n g n a h m e :

Allgemein:

Der Entwurf eines Personenstandsgesetzes 2013 sieht unter anderem die Einrichtung eines „Zentralen Personenstandsregisters“ (ZPR) und eines „Zentralen Staatsbürgerschaftsregisters“ (ZSR) vor. Diese Register sollen die lokale Bücherstruktur in Personenstandsachen ersetzen. Beide Register sollen als Informationsverbundsysteme iSd § 4 Z 13 DSG betrieben werden. Aus der Sicht des ÖRAK begegnet der Entwurf tiefgehenden **datenschutzrechtlichen Bedenken**:

- Fehlende Vorschriften zu Datensicherheitsmaßnahmen

Der Gesetzesentwurf regelt umfangreich die Verwendung der in den Registern gespeicherten Daten. Dabei fällt sofort ins Auge, dass die bezughabenden Bestimmungen **nicht einmal ansatzweise** Regelungen zur **Datensicherheit**

beinhalten. Dies ist zutiefst verwunderlich. Die Zentralisierung von Datensätzen bedeutet nicht nur Verwaltungsvereinfachung und Kostenreduktion. Die Kehrseite der Medaille ist die der **verminderten Datensicherheit**: Dringt jemand in unzulässiger Weise in lokale, begrenzte Systeme ein, so sind naturgemäß nur die Daten dieses begrenzten Systems betroffen. Dringt aber jemand in einen Informationsverbund ein, so ist das Schadenspotential aufgrund der Masse der betroffenen Daten und der Dichte der Datenvernetzung um ein Vielfaches größer. Zudem enthält das ZPR Daten über eingetragene Partnerschaften. Diese Informationen lassen auf die sexuelle Ausrichtung der Betroffenen schließen. Bei diesen Informationen handelt es sich um besonders schützenswerte Daten, nämlich um **sensible Daten** iSd § 4 Z 2 DSG. Unbefugte Abfragen dieser Daten, deren unzulässige Weitergabe, das illegale „Absaugen" dieser (und natürlich auch anderer) Daten aus dem Register – all das kann für die Betroffenen zu schwerwiegenden und irreversiblen Konsequenzen führen.

Diesen Überlegungen trägt der Gesetzesentwurf nur durch den lapidaren Hinweis in § 44 Abs 4 des vorgeschlagenen Personenstandsgesetzes 2013 Rechnung, wonach der Bundesminister für Inneres die notwendigen Maßnahmen zur Sicherung der „Datenqualität" zu ergreifen hat. Eine einzurichtende „Clearingstelle" ist mit der Durchführung „qualitätssichernder Maßnahmen" zu beauftragen. Anforderungen, welche diese Clearingstelle zu erfüllen hat, werden ebenso wenig determiniert wie die „qualitätssichernden Maßnahmen" näher umschrieben werden. Stattdessen ermächtigt das Gesetz den Bundesminister dazu, „näheres" über die Datensicherheitsmaßnahmen durch Verordnung festzulegen. Die Erläuterungen halten diesbezüglich fest, dass durch diese Bestimmung in jenen Fällen, in denen die Behörden unterschiedliche Datensätze anlegen, sichergestellt werden soll, dass im System letztlich nur ein Datensatz vorhanden ist. Der Betreiber übernehme die Funktion der „Datenpflege" im Informationsverbund.

Zunächst fällt auf, dass der Gesetzgeber die Begriffe der „Datenqualität" und der „Datensicherheit" durcheinander zu bringen scheint. So beziehen sich § 44 Abs 4 Personenstandsgesetz 2013 wie auch die Materialien primär auf Aspekte der Datenpflege und der Datenqualität. So wird im Gesetz die Sicherung der Datenqualität postuliert und in den Materialien dazu erläutert, dass Mehrfachdatensätze vermieden werden sollen. Im letzten Satz des § 44 Abs 4 wird dies plötzlich mit Fragen der Datensicherheit verknüpft (Arg: „**Näheres**" über die Datensicherheitsmaßnahmen ist mit Verordnung festzulegen). Die Begriffe der Datenqualität und der Datensicherheit haben nichts miteinander zu tun. Die Datenqualität beschreibt die Aktualität, Vollständigkeit und Richtigkeit von Daten, die Datensicherheit beschreibt deren sichere Verwendung und Verwahrung. Insofern ist es unrichtig, diesen Themenkomplex derart zu verknüpfen, wie es der Gesetzgeber in § 44 Abs 4 des Personenstandsgesetzes 2013 tut.

Führt man sich diese begriffliche Trennung vor Augen, so wird evident, dass der Gesetzgeber vollends auf inhaltliche Vorgaben zur Datensicherheit **verzichtet** hat. Die im Gesetz lapidar vorgesehene Ermächtigung, „näheres" über die Datensicherheitsmaßnahmen durch Verordnung festzulegen, ist derart unbestimmt, dass dies im Lichte des Art 18 B-VG **bedenklich** erscheint. Auch inhaltlich ist nicht nachvollziehbar, wieso das Thema der Datensicherheit derart stiefmütterlich behandelt wird. Im Gesetzesentwurf wird nicht einmal auf die – rudimentären –

Datensicherheitsbestimmungen des § 14 DSG referenziert. Tatsächlich wäre angesichts der Fülle der in den Registern verwahrten Daten, deren Vernetzungsdichte und der hohen Zahl geplanter Zugriffsermächtigungen **detaillierte Sicherheitsvorkehrungen** auf gesetzlicher Ebene zu determinieren, für deren Einhaltung der Bundesminister für Inneres als Registerbetreiber und die Personenstands- und Evidenzbehörden Sorge zu tragen haben. Die an die Sicherheitsvorkehrungen zu stellenden Anforderungen wären speziell auf die sicherheitsrelevanten Aspekte des ZPR bzw ZSR abzustimmen. Auch wenn dies Investitionen bedeuten mag, die das Bild der zu erwartenden Verwaltungseinsparungen trüben könnten, darf die Sicherheit der Daten nicht außer Acht gelassen werden.

- Ermächtigung zum Führen lokaler Personenstandsregister

In § 45 des vorgeschlagenen Personenstandsgesetzes 2013 findet sich eine Ermächtigung, wonach die Personenstandsbehörden „**andere**“ Daten in einem „**lokalen Personenstandsregister**, das **im Rahmen des ZPR** geführt wird“ zu verarbeiten. In den Erläuterungen wird dazu ausgeführt, dass diese „anderen“ Daten so zu speichern sind, dass sie nur für die „eigene Behörde“ sichtbar sind. Von anderen Personenstandsbehörden können die Daten nur eingesehen werden, wenn die Daten für die Ausübung der von der gesetzlichen Aufgabe dieser Behörden umfassten Tätigkeit notwendig sind.

Im Dunkeln bleibt, welche „anderen“ Daten gemeint sind. Aus dem Gesetz selbst ergeben sich keine Einschränkungen. Da das Gesetz von einem lokalen „Personenstandsregister“ spricht, dürften diese Daten weitere Personenstandsdaten beinhalten. Dadurch ermächtigt das Gesetz die Behörden zum Aufbau einer „**Paralleldatenbank**“, in der, salopp gesagt, unkontrolliert andere Personenstandsdaten eingepflegt werden können. Dies steht im **Widerspruch** zu § 2 des vorgeschlagenen Personenstandsgesetzes, welcher die im ZPR zu speichernden Daten abschließend auflistet. Für die Einspeicherung weiterer Personenstandsdaten in einer „Paralleldatenbank“ besteht somit **kein Raum**.

Das Gesetz besagt zudem, dass dieses lokale Personenstandsregister „im Rahmen des ZPR“ zu führen ist, ohne dies näher zu spezifizieren. Daraus ergibt sich, dass derartige lokale Personenstandsregister im Rahmen des Informationsverbundsystems des ZPR zu führen sind. Dem scheinen zwar die in Materialien zu widersprechen, indem diese festhalten, dass die Daten nur für die „eigene“ Behörde sichtbar seien, jedoch findet diese Ansicht im Wortlaut des Gesetzes **keine Deckung**. Zudem sind die Materialien in sich **widersprüchlich**: So wird weiters ausgeführt, dass diese Daten von anderen Behörden nur eingesehen werden können, wenn dies für deren Aufgabenerfüllung notwendig ist. Wenn nur die „eigene Behörde“ die Daten einsehen kann, wie kann es möglich sein, dass diese Daten dennoch auch von anderen Personenstandsbehörden eingesehen werden können? Weiters: Wer entscheidet, ob der Behördenauftrag diese Dateneinsichtnahme erfordert? Schließlich: Wenn auch andere Personenstandsbehörden auf diese Daten zugreifen können, so ist evident, dass ein „Schatten-ZPR“ im Sinne eines **weiteren Informationsverbundsystems** installiert werden soll, welches keinerlei gesetzlichen Vorgaben unterliegt. So ist alleine schon unklar, welche Daten es beinhaltet. Zugriffsrechte und dergleichen werden nicht

festgelegt. Im Unterschied zum „echten“ ZPR wird für dieses „Schatten-ZPR“ nicht einmal eine Verordnungsermächtigung zur Etablierung von Datensicherheitsmaßnahmen geschaffen, sodass überhaupt keine Sicherheitsvorkehrungen determiniert werden. Aus all diesen Überlegungen ist die in § 45 vorgeschlagene Implementierung eines lokalen Personenstandsregisters zur Gänze **abzulehnen**. Unweigerlich stellt man sich die Frage, welchem Zweck dieses „Schatten-ZPR“ dienen soll. Wenn mit den Datensätzen des „echten“ ZPR nicht das Auslangen gefunden wird, so darf dies jedenfalls nicht durch ein aushilfsweises „Schatten-ZPR“ auszugleichen versucht werden.

Angesichts der zuvor dargelegten Bedenken, vor allem im Hinblick auf das vollständige Fehlen gesetzlicher Datensicherheitsvorgaben, können aus der Sicht des ÖRAK allfällige Detailüberlegungen zur gesetzlichen Ausgestaltung der Register vorerst hintangestellt bleiben. Anders ausgedrückt: Die besten Vorgaben zur Datenverwendung sind nichts wert, wenn nicht für die Sicherheit der verwendeten Daten Sorge getragen wird. Die vom ÖRAK aufgezeigten Bedenken zur Datensicherheit gelten für das ZPR und das ZSR gleichermaßen, sodass der ÖRAK im Lichte dessen eine **grundlegende Überarbeitung** des Gesetzesentwurfs empfiehlt.

Wien, am 30. August 2012

DER ÖSTERREICHISCHE RECHTSANWALTSKAMMERTAG

Dr. Rupert Wolff
Präsident