

REPUBLIK ÖSTERREICH  DATENSCHUTZRAT

BALLHAUSPLATZ 2, A-1014 WIEN
GZ • BKA-817.208/0002-DSR/2015
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:

Christoph.Schlager@bmf.gv.at
e-Recht@bmf.gv.at

Betrifft: **Entwurf eines Bundesgesetzes, mit dem das Bankwesen (Bankwesengesetz – BWG) geändert, das Bundesgesetz über die Einrichtung eines Kontenregisters (Kontenregistergesetz – KontRegG), das Bundesgesetz über die Meldepflicht von Kapitalabflüssen (Kapitalabfluss-Meldegesetz) und das Bundesgesetz zur Umsetzung des gemeinsamen Meldestandards für den automatischen Austausch von Informationen über Finanzkonten (Gemeinsamer Meldestandard-Gesetz – GMSG) erlassen, das EU-Amtshilfegesetz und das Amtshilfe-Durchführungsgesetz geändert werden**

Stellungnahme des Datenschutzrates

Der **Datenschutzrat** hat in seiner **225. Sitzung am 9. Juni 2015 einstimmig** beschlossen, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

1) Allgemeines

Durch die **Änderungen im Bankwesengesetz** soll der **Zugang zu durch das Bankgeheimnis geschützten Informationen erleichtert werden**, indem festgelegt werden soll, unter welchen Voraussetzungen diese Informationen den Abgabenbehörden, den Finanzstrafbehörden, den Staatsanwaltschaften oder den Strafgerichten zu erteilen sind. Durch die **Erweiterung der Durchbrechung des Bankgeheimnisses um abgabenrechtliche Verfahren, durch**

Meldeverpflichtungen von Kapitalabflüssen und durch den Aufbau eines Kontenregisters sollen die Abgabenbehörden künftig rasch die für das Abgabeverfahren notwendigen Informationen erhalten. Durch diese Änderungen sollen beispielsweise Schwarzgeldumsätze künftig leichter und zeitnah entdeckbar sein.

Weil derzeit im Hinblick auf die Verfolgung von Finanzvergehen das Bankgeheimnis nur dann durchbrochen ist, wenn ein Strafverfahren eingeleitet worden ist, dürfen Banken derzeit keine entsprechenden Informationen an die Abgabenbehörden herausgeben. Daher sollen ab 1. Jänner 2016 die Banken die von den Abgabenbehörden für Zeiträume ab dem 1. März 2015 angeforderten Informationen an diese herausgeben dürfen.

Derzeit gibt es auch – anders als in vielen anderen europäischen Staaten – kein zentral geführtes Register über alle Bankkonten/Depots, die in Österreich geführt werden. Daher erhalten derzeit Behörden und Gerichte in einigen bestimmten Fällen (zB in Verlassenschaftsverfahren) diese Auskunft nur über anlassfallbezogenes Verbandsabfrageverfahren. Dieses Verbandsabfrageverfahren ist nur bis zu einer gewissen Fallanzahl einsetzbar und stößt danach an seine Kapazitätsgrenze. Abgabenbehörden haben daher derzeit keine Möglichkeit diese Information zu erhalten. **Es sollen zukünftig daher Staatsanwaltschaften, Strafgerichte, Finanzstrafbehörden, das Bundesfinanzgericht und Abgabenbehörden des Bundes Zugriff auf ein zentral geführtes Register über alle Bankkonten/Depots, die in Österreich geführt werden, haben.**

Derzeit besteht keine Möglichkeit zu verhindern, dass im Hinblick auf die Erweiterung der Befugnisse der Staatsanwaltschaften, Strafgerichte, Finanzstrafbehörden, des Bundesfinanzgerichts und der Abgabenbehörden des Bundes zur Erlangung von bankspezifischen Informationen Kapital in größeren Beträgen von Privatkunden abgezogen wird. **Ein Ziel wäre daher, wenn Privatkunden ab dem 1. März 2015 keine größeren Beträge von ihren österreichischen Bankkonten und -depots abziehen können, ohne dass der Vorgang dem Bundesministerium für Finanzen gemeldet wird.**

Weiters ist seit dem 1.1.2015 Österreich zum automatischen Informationsaustausch im Verhältnis zu den EU-Mitgliedstaaten in Bezug auf bestimmte Kategorien von Einkünften (z.B. Vergütungen aus unselbständiger Arbeit bzw. Ruhegehälter)

verpflichtet. Eine Verpflichtung zum Austausch von Informationen über Finanzkonten mit anderen Staaten als den USA besteht derzeit nicht.

Zum Evaluierungszeitpunkt ist der automatische Austausch von Informationen über Finanzkonten entsprechend den Vorgaben der Richtlinie 2014/107/EU und des Regierungsübereinkommens vom 29. Oktober 2014 umgesetzt.

Die entsprechenden Daten werden von Österreich zeitgerecht und inhaltlich vollständig übermittelt.

Das Vorhaben umfasst hauptsächlich folgende Maßnahmen:

Maßnahme 1: Erweiterung der Ausnahmebestimmungen vom Bankgeheimnis

Im Hinblick auf die Verfolgung von Finanzvergehen war das Bankgeheimnis bisher nur dann durchbrochen, wenn ein Strafverfahren eingeleitet worden ist. In Zukunft soll u.a. bereits im abgabenbehördlichen Verfahren die Möglichkeit bestehen, dass die Abgabenbehörde auf ein Auskunftersuchen Konto- und Bankinformationen erhält.

Maßnahme 2: Einrichtung eines Kontenregisters

Mit der Einrichtung eines zentral verwalteten Kontenregisters erhalten Staatsanwaltschaften, Strafgerichte, Finanzstrafbehörden, das Bundesfinanzgericht und Abgabenbehörden des Bundes die Möglichkeit einen Überblick darüber zu bekommen, über welche Bankkonten/Depots eine Person verfügt bzw. welche Personen Zugriff auf ein bestimmtes Konto/Depot haben.

Maßnahme 3: Einführung einer Meldepflicht von Kreditinstituten über größere Geldbewegungen

Es besteht die Gefahr von Kapitalabflüssen aufgrund der Ausweitung der Möglichkeiten der Abgaben-, Strafbehörden und Gerichte bankbezogene Informationen zu erhalten. Um zu verhindern, dass vor dem Wirksamwerden der geplanten Maßnahmen Kapital abgezogen wird, müssen Kreditinstitute Kapitalabflüsse über 50.000 Euro ab dem 1. März 2015 dem Bundesministerium für Finanzen melden.

Maßnahme 4: Erweiterung des automatischen Informationsaustausches in Steuersachen auf Informationen über Finanzkonten

Jedes betroffene österreichische Finanzinstitut wird verpflichtet, seinem zuständigen Finanzamt für jedes Konto einer natürlichen oder juristischen Person aus einem anderen EU-Mitgliedstaat oder einem Vertragsstaat des Regierungsübereinkommens vom 29. Oktober 2014 die vorgeschriebenen Daten über den Kontoinhaber sowie bestimmte Kontodaten zu melden. Das Bundesministerium für Finanzen leitet diese Daten einmal pro Jahr gesammelt für das vorangegangene Kalenderjahr der zuständigen Behörde des anderen EU-Mitgliedstaates oder des Vertragsstaates des Regierungsübereinkommens vom 29. Oktober 2014 weiter.

2) Datenschutzrechtliche Anmerkungen

I. Datenschutzrechtliche Vorbemerkungen

Einleitend merkt der Datenschutzrat an, dass ein zentrales Kontenregister bereits in vielen europäischen Ländern eingerichtet ist und einen internationalen Standard darstellt. Im Gegensatz zu entsprechenden Regelungen in anderen EU-Mitgliedstaaten wird durch dieses Gesetz der Zugriff auf dieses Register auf die Staatsanwaltschaften, Strafgerichte, Finanzstrafbehörden, das Bundesfinanzgericht und Abgabenbehörden des Bundes beschränkt.

In anderen EU-Mitgliedstaaten – wie in Deutschland – können eine Vielzahl von Behörden (z.B. neben Finanzbehörden und Abgabenbehörden auch Sozialbehörden, Jobcenter, Gerichtsvollzieher) derartige Kontenzugriffe durchführen. Dies führte in Deutschland zu ausufernden Bankkontenabrufen, die durch den Bundesdatenschutzbeauftragten heftig kritisiert wurden. Die Einschau in Konten und Bankunterlagen selbst ist in Europa unterschiedlich geregelt, meist mit richterlicher Genehmigung.

In datenschutzrechtlicher Hinsicht ist festzuhalten, dass es sich beim Kontenregister und den daraus resultierenden Meldeverpflichtungen um **Datenanwendungen** iSd § 4 Z 7 DSG 2000 und damit um einen **Eingriff in das Grundrecht auf Datenschutz** nach § 1 Abs. 1 DSG 2000 handelt. Somit bedarf es nach § 1 Abs. 2 DSG 2000

eines **überwiegenden berechtigten Interesses** an diesem Eingriff, der **in einem Gesetz hinreichend bestimmt geregelt sein muss**.

Ein solcher gesetzlich normierter Eingriff muss somit im **Interesse der Allgemeinheit** (Art. 8 Abs. 2 EMRK) gelegen sein bzw. dem **Gemeinwohl** dienen und **verhältnismäßig** sein (siehe u.a. **EuGH-Urteil** vom 8.4.2014, verbundene Rechtssachen C-293/12 und C-594/12 zur Prüfung der Richtlinie über die **Vorratsspeicherung von Daten** (RL 2006/24/EG)).

Die **Bekämpfung von Abgabenhinterziehung und Steuerbetrug – und damit die Sicherstellung der Gleichmäßigkeit der Besteuerung – dient dem Gemeinwohl**, womit Eingriffe in das Grundrecht auf Datenschutz für diesen Zweck unter bestimmten Voraussetzungen rechtlich zulässig sind. **Um Missbrauch hintanzuhalten sind jedoch Kontrollen, ein ausreichender Rechtsschutz der Betroffenen sowie Informationsverpflichtungen sicherzustellen**.

Wie in anderen Materiengesetzen (zB beim ELGA-Gesetz) sollte die gesetzliche Festlegung von eigenen **abschreckenden gerichtlichen Strafbestimmungen** geprüft werden und zwar unter dem Blickwinkel, ob die bestehenden strafrechtlichen Bestimmungen (zB Abgabenrechtliche Geheimhaltungspflicht) ausreichen.

Im Hinblick auf die sich aus dem DSG 2000 ergebenden **Pflichten** (zB Meldepflichten nach den §§ 17 f DSG 2000, Wahrung der Rechte des Betroffenen nach den §§ 26 ff DSG 2000) muss die **Rollenverteilung** der einzelnen Akteure definiert werden. Es muss sohin bei **jeder** im Entwurf geregelten Datenanwendung klar erkennbar sein, wer **Auftraggeber** (§ 4 Z 4 DSG 2000) und wer allenfalls **Dienstleister** (§ 4 Z 5 DSG 2000) ist.

Des Weiteren wird darauf hingewiesen, dass im gesamten Entwurf keine **Datensicherheitsmaßnahmen** (§ 14 DSG 2000) festgelegt werden. Es wäre – zumindest in Grundzügen – auf gesetzlicher Ebene zu regeln, welche konkreten **Datensicherheitsmaßnahmen** jeweils ergriffen werden müssen. Insbesondere sollte die **Protokollierung** der Abfragen als Teil der Datensicherheitsmaßnahmen bereits im Gesetz festgeschrieben werden. **Denkbar ist auch eine Verordnungsermächtigung im Gesetz**, ähnlich wie im Meldegesetz (siehe etwa § 10 des Meldegesetzes 1991 – MeldeG, BGBl. Nr. 9/1992, oder § 19 Abs. 4 des Vereinsgesetzes 2002 – VerG, BGBl. I Nr. 66/2002). Kontodaten müssen jedenfalls

wirksam vor Missbrauchsrisiken sowie vor jedem unberechtigten Zugang zu ihnen und jeder unberechtigter Nutzung geschützt werden.

Nach der geltenden Rechtslage (§ 38 Abs. 2 Z 1 BWG) besteht die Verpflichtung zur Wahrung des Bankgeheimnisses im Zusammenhang mit einem Strafverfahren aufgrund einer gerichtlichen Bewilligung (§ 116 StPO) gegenüber den Staatsanwaltschaften und Strafgerichten und mit eingeleiteten Strafverfahren wegen vorsätzlicher Finanzvergehen ausgenommen Finanzordnungswidrigkeiten gegenüber den Finanzstraßbehörden **nicht**. § 38 Abs. 2 Z 2 bis 9 regelt weitere Ausnahmen vom Bankgeheimnis.

So kann nach dem Finanzstrafgesetz ein Eingriff in das Bankgeheimnis ohne richterliche Genehmigung jetzt bereits vorgenommen werden, wenn die Straftat fahrlässig begangen wurde oder der hinterzogene Betrag die Wertgrenze von 100.000 Euro nicht überschreitet (unter 50.000 Euro in Zollstrafsachen).

Mit dem vorliegenden Gesetzesentwurf, durch den das Bankgeheimnis in mehreren Fällen durchbrochen wird, ergeben sich – nicht zuletzt aufgrund höchstrichterlicher Rechtsprechung – datenschutzrechtliche Problemstellungen, die zu lösen sind.

Im Lichte der datenschutzrechtlichen Vorgaben nach dem DSGVO 2000 ist der vorliegende Entwurf zu überarbeiten. Kontrollen, ein ausreichender Rechtsschutz und gezielte Information der Betroffenen sind in dieser sensiblen Materie wesentliche Elemente einer effektiven Anti- Missbrauchsstrategie, die jeder Rechtsstaat fordert. Eigene Sonderstrafbestimmungen sind aus Sicht des Ressorts derzeit nicht vorgesehen, wobei auf bestehende strafrechtliche Geheimhaltungsbestimmungen verwiesen wurde. Weiters hält der Datenschutzrat fest, dass ein informierter Vertreter des BMF in der Sitzung des Datenschutzrates – unter Hinweis auf die öffentliche Erklärung des Bundesministers für Finanzen Dr. Hans Jörg Schelling im Nationalrat – zugesichert hat, dass angemessene Kontrollinstrumente sowie ein Vier-Augen-Prinzip gesetzlich vorgesehen werden. Überdies wurde von den informierten Vertretern zugesichert, dass Auskunftsbegehren der Behörden begründet werden.

II. Artikel 1 (Änderung des Bankwesengesetzes (BWG))

Zu Z 1 (§ 38 Abs. 2 BWG):

Nach dem vorliegenden Gesetzesentwurf (§ 38 Abs. 2 Z 11) genügen allein „Bedenken gegen die Richtigkeit der Abgabenerklärung“ durch die Abgabenbehörde, um das Bankgeheimnis zu durchbrechen. Diese Voraussetzung, die nicht näher begründet werden muss, ist gegenüber Staatsanwaltschaften und Gerichten eine Besserstellung, die aus sachlichen Gründen als nicht gerechtfertigt erscheint. Überdies können Missbrauchsrisiken nicht ausgeschlossen werden. Auch im Sinne des Determinierungsgebotes des Art. 18 B-VG sollte hier eine Neuformulierung angestrebt werden.

In diesem Zusammenhang verweist der Datenschutzrat auf die Erläuterungen zu diesem Gesetzesvorhaben. Es sollte auch im Gesetzestext – oder zumindest in den Erläuterungen – eine diesbezügliche Klarstellung getroffen werden, dass es im Rahmen einer routinemäßigen Steuerveranlagung (Arbeitnehmer-Einkommenssteuer- Veranlagung und andere) zu keiner Einsichtnahme in die Konten von Abgabepflichtigen kommt. Vom informierten Vertreter wird zugesichert, dass dies in der Regierungsvorlage konkreter ausgeführt wird.

Aus Sicht des Datenschutzrates stellt die elektronische Übermittlung bzw. die Einschau von Daten im Zuge der Öffnung eines Kontos oder Depots an die Abgabenbehörden des Bundes einen weitreichenden Eingriff in das Grundrecht auf Datenschutz dar.

Die Beauskunftung solcher Daten sollte daher besonderen Voraussetzungen (vgl. etwa § 99 Abs. 3a FinStrG idF des Steuerreformgesetzes 2015/2016) unterliegen und nur dann erfolgen, wenn die Einsichtnahme in die Daten **unbedingt erforderlich** ist und **im konkreten Fall kein gelinderes Mittel** zur Erreichung des Zwecks zur Verfügung steht.

Aus datenschutzrechtlicher Sicht muss sohin ein Verfahren festgelegt werden, wie die Einschau in den Konten gestaltet wird, welche Rechte den Betroffenen (zB Informations- und Auskunftsrecht) zukommen und an welche Einrichtung (kommissarischer oder gerichtlicher Rechtschutz) sich die Betroffenen mit allfälligen Beschwerden richten können. Es wäre zu überlegen, ob auch der Datenschutzbehörde in diesem Bereich gesonderte Kontrollbefugnisse zukommen. Weiters muss daher für die Einschau in Konten eine **ausreichende Begründung** (zB ein konkreter Verdachtsgrund) und eine **Benachrichtigung des**

Betroffenen vorgesehen werden, sofern dadurch die Ermittlungen nicht gefährdet werden.

Der Datenschutzrat merkt an, dass die bisherigen Erhebungen der Abgabenbehörden bei der Konteneinsicht aufwendig waren, während die richterliche Genehmigung vergleichsweise rasch erledigt wäre.

Die grundlegenden Voraussetzungen für die Einschau in Konten **müssen auch für alle im Gesetz normierten Berechtigten gleich ausgestaltet sein.** Es darf auch zu **keiner Sonderstellung der Abgabenbehörde (Finanzbehörden) kommen.** Diesbezüglich ist auch die geplante Novelle zu § 116 StPO abzuwarten.

Derartige Eingriffe verlangen überdies auch besondere **Datensicherheitsmaßnahmen** nach § 14 DSG 2000, so vor allem hinsichtlich der **Beschränkung** und der **Protokollierung** des Zugriffs sowie der **Löschung** der Daten. Zu prüfen ist, ob die **Datenübermittlung** entsprechend dem Stand der Technik **verschlüsselt** vorgenommen werden kann. Diesbezüglich wäre zu prüfen, ob das Modell der Durchlaufstelle verwendet werden kann. Zudem sollte eine jährliche **Berichtspflicht** an den Nationalrat vorgesehen werden.

III. Artikel 2 (Bundesgesetz über die Einrichtung eines Kontenregisters (Kontenregistergesetz – KontRegG))

Zu § 1:

Nach den Erläuterungen soll die **Einrichtung eines Kontenregisters** dem Grundsatz der Sparsamkeit, Wirtschaftlichkeit und Zweckmäßigkeit im Rahmen der Durchführung von gerichtlichen Strafverfahren, verwaltungsbehördlichen Finanzstrafverfahren sowie der Erhebung der Abgaben des Bundes dienen.

Nach § 1 Abs. 1 DSG 2000 hat jedermann Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit er daran ein schutzwürdiges Interesse hat. Beschränkungen dieses Grundrechtes sind nach dem Gesetzesvorbehalt des § 1 Abs. 2 DSG 2000 (abgesehen von lebenswichtigen Interessen des Betroffenen an der Verwendung personenbezogener Daten oder

seiner Zustimmung hinzu) bei Eingriffen einer staatlichen Behörde nur auf Grund von Gesetzen zulässig, die aus den in Art. 8 Abs. 2 EMRK genannten Gründen notwendig sind und die ausreichend präzise, also für jedermann vorhersehbar, regeln, unter welchen Voraussetzungen die Ermittlung bzw. die Verwendung personenbezogener Daten zulässig ist.

Aufgrund des Verhältnismäßigkeitsgrundsatzes dürfen jedoch Eingriffe in das Grundrecht auf Datenschutz jeweils nur in der **gelindesten, zum Ziel führenden Art** vorgenommen werden und nur solche Daten verwendet werden, die für die Erreichung des Zwecks auch tatsächlich **erforderlich** sind.

Hinsichtlich der Frage der **Rollenverteilung** wird auf die Ausführungen in den datenschutzrechtlichen Vorbemerkungen verwiesen.

Zu § 2:

Es ist unklar, ob es sich beim Kontenregister um eine Datenbank mit **indirekt oder direkt personenbezogenen Daten** (§ 4 Z 1 DSG 2000) handelt, dies insbesondere vor dem Hintergrund, dass einerseits das bereichsspezifische Personenkennzeichen (bPK) und andererseits der Vorname, Zuname und das Geburtsdatum bei natürlichen Personen verarbeitet werden.

Soweit in einer Datenbank **sowohl indirekt als auch direkt personenbezogene Daten** verarbeitet werden, können sich im Lichte des § 29 DSG 2000 Unterschiede bei der Handhabung der **Rechte der Betroffenen** ergeben, da die durch die §§ 26 bis 28 DSG 2000 gewährten Rechte nicht geltend gemacht werden können, **soweit nur indirekt personenbezogene Daten** verwendet werden. Für diesen Fall ist unklar, ob und wie der Betroffene **Auskunft** über seine verarbeiteten Daten und die **Richtigstellung unrichtiger Daten** (etwa fälschlicherweise angeführte Konten) erwirken kann.

Im Übrigen sollte im Gesetzestext selbst geregelt werden, ob das bPK in **verschlüsselter oder unverschlüsselter Form** verwendet wird.

Hinsichtlich der in § 2 Z 3 vorgesehenen Aufnahme von Daten vertretungsbefugter Personen, Treugeber und wirtschaftlicher Eigentümer in das Kontenregister sollte näher erläutert werden, inwiefern diese Datenverarbeitung zur Erreichung des angestrebten Ziels erforderlich ist.

Weiters sollte die **Benachrichtigung des Betroffenen**, wenn ein Auskunftersuchen gestellt wird, sowie eine **jährliche Berichterstattung** an den Nationalrat vorgesehen werden.

Zu den §§ 3, 4 und 6:

Die §§ 3 und 4 sehen eine **elektronische Übermittlung** von Daten bzw. **Einsicht in Daten** im Kontoregister vor. Diesbezüglich hat der Bundesminister für Finanzen mit Verordnung nach § 6, das Verfahren und die Auskunftserteilung einschließlich ihrer Dokumentation in organisatorischer und technischer Hinsicht näher zu regeln.

Der Zugang der nach diesem Gesetzesentwurf berechtigten Stellen zu den Kontodaten (Kontoeinschau) soll aus datenschutzrechtlicher Sicht vorweg durch ein Gericht oder einen Rechtsschutzbeauftragten geprüft werden, wobei deren Entscheidung eine Schranke für den Zugang zu diesen Daten darstellt und die Nutzung der Daten auf das zur Erreichung des verfolgten Ziels auf das absolut Notwendige beschränkt wird.

Die in § 6 vorgesehene Verordnungsermächtigung ist nicht ausreichend konkret. Vielmehr müssten die organisatorischen und technischen Vorgaben – wozu insbesondere auch die **Datensicherheitsmaßnahmen** (siehe etwa § 10 des Meldegesetzes 1991 – MeldeG, BGBl. Nr. 9/1992) zählen – zumindest **in Grundzügen auf gesetzlicher Ebene** determiniert und in der Folge auf **Verordnungsebene konkretisiert** werden, um die zu ergreifenden **Sicherheitsmaßnahmen beim Register** abzusichern.

Zu § 4 Z 3 wird angemerkt, dass eine verfahrensunabhängige, im Gesetz nicht näher geregelte Zugriffsmöglichkeit der Abgabenbehörden des Bundes und des Bundesfinanzgerichts auf das Kontenregister aus datenschutzrechtlicher Sicht nicht unbedenklich erscheint. So ist es im Lichte des Verhältnismäßigkeitsgrundsatzes keinesfalls ausreichend, dass die Auskunft im Interesse der Abgabenerhebung bloß „**zweckmäßig und angemessen**“ sein muss. Vielmehr dürfte die Auskunft nur dann in Betracht kommen, wenn sie zur Erreichung des Zweckes **unbedingt erforderlich** ist und das **gelindeste Mittel** darstellt.

Unklarheiten bestehen auch dahingehend, unter welchen Voraussetzungen die Auskunft nach § 6 zu erteilen ist. Die vorliegende Formulierung lässt den Schluss zu, dass der Zugriff auf die Daten im Kontenregister **ohne Kenntnis der Bank und des**

Kunden erfolgen kann. Diesbezüglich wird auf die Informationsregelung in § 5 Abs. 2 DSGVO hingewiesen. Aus datenschutzrechtlicher Sicht wäre es notwendig, **Anforderungen** für eine Auskunftserteilung, eine **Begründung** des Auskunftersuchens sowie grundlegende **Informations- und Protokollierungs- sowie Dokumentationspflichten** beim Zugriff auf das Kontenregister und datenschutzkonforme **Auskunftsrechte** der Betroffenen vorzusehen.

Wie bereits ausgeführt, ist grundsätzlich noch zu entscheiden, ob ein kommissarischer oder gerichtlicher Rechtsschutz vorgesehen wird. Der Datenschutzrat empfiehlt eine Regelung vorzusehen, die die Zulässigkeit des Dateneingriffes prüft sowie in Folge eine nachträgliche Kontrolle durchführt.

Zu § 5:

Es ist fraglich, zu welchem Zweck die erfassten Daten nach Auflösung des Kontos bzw. des Depots zehn Jahre aufbewahrt werden müssen und weshalb nicht mit einer kürzeren Frist das Auslangen gefunden werden kann.

Zu § 7:

Hinsichtlich der in § 7 festgelegten Strafbestimmungen wird angemerkt, dass entsprechende Strafandrohungen für das **rechtswidrige Abfragen der Daten** sowie den **Missbrauch der Daten aus dem Kontenregister** fehlt. Dies sollte nochmals geprüft werden.

IV. Artikel 3 (Bundesgesetz über die Meldepflicht von Kapitalabflüssen (Kapitalabfluss-Meldegesetz))

Zu § 3:

Es erscheint unklar, zu welchem **Zweck** die Meldepflicht vorgesehen wird und weshalb das angestrebte Ziel nur mit einer Meldepflicht von Beträgen von mindestens 50 000 Euro erreicht werden kann bzw. weshalb nicht etwa mit einer höheren Wertgrenze das Auslangen gefunden werden kann. Dies sollte in den Erläuterungen näher dargelegt werden. **Im Übrigen erscheint eine verdachtsunabhängige und routinemäßige Pflicht zur Meldung von Kontenflüssen unverhältnismäßig.**

Unklar erscheint auch, wie in der Praxis festgestellt wird, ob zwischen „mehreren Vorgängen“ eine Verbindung gegeben ist bzw. ob das Kreditinstitut diesbezüglich zu weiteren Nachforschungen und Datenerhebungen verpflichtet ist, um den „offenkundigen“ Zusammenhang feststellen zu können. Jedenfalls muss sichergestellt sein, dass **ausreichende Kriterien** für das Bestehen einer derartigen Verbindung gegeben sind, um eine Meldepflicht nach § 3 auszulösen.

Hinsichtlich der Verwendung des bPK einerseits und des Namen andererseits wird auf die Anmerkungen zu Artikel 2 § 2 verwiesen.

Zu § 5:

Hinsichtlich der vorgesehenen Verordnungsermächtigung wird sinngemäß auf die datenschutzrechtlichen Anmerkungen zu Art. 2 §§ 3, 4 und 6 verwiesen.

Zu § 6:

Hinsichtlich der Strafbestimmungen wird auf die datenschutzrechtlichen Anmerkungen zu Art. 2 § 7 verwiesen.

V. Artikel 4 (Bundesgesetz zur Umsetzung des gemeinsamen Meldestandards für den automatischen Austausch von Informationen über Finanzkonten (Gemeinsamer Meldestandard-Gesetz – GMSG))

Zu § 3:

Es sollte – zumindest in den Erläuterungen – näher dargelegt werden, welchen **Zweck** die automatische Meldepflicht nach § 3 erfüllt. Zudem wäre zu prüfen, ob tatsächlich alle in § 3 genannten Datenarten zur Erreichung dieses Zwecks „automatisch“ – und somit in jedem Fall – notwendig sind.

Zu § 4:

Hinsichtlich der vorgesehenen Verordnungsermächtigung wird sinngemäß auf die datenschutzrechtlichen Anmerkungen zu Art. 2 §§ 3, 4 und 6 verwiesen.

Zu § 8:

Es sollte klargestellt werden, ob in dieser Bestimmung ein „Dienstleister“ in datenschutzrechtlicher Hinsicht (§ 4 Z 5 DSG 2000) gemeint ist.

Zu § 12:

Es sollte präziser geregelt werden, in welchen konkreten Fällen sich das meldende Finanzinstitut gemäß § 12 nicht auf die Belege nach § 11 verlassen kann.

Zu § 30:

Es sollte vor dem Hintergrund des Verhältnismäßigkeitsgrundsatzes konkreter in der Gesetzesbestimmung dargelegt werden, welche Daten im Rahmen der Selbstauskunft benötigt werden. Daten, die zur Erreichung des Zwecks nicht erforderlich sind, dürfen auch im Rahmen einer Selbstauskunft nicht verarbeitet werden.

11. Juni 2015
Für den Datenschutzrat
Der Vorsitzende:
MAIER

Elektronisch gefertigt