REPUBLIK ÖSTERREICH DATENSCHUTZRAT

BALLHAUSPLATZ 2, A-1014 WIEN
GZ ● BKA-817.354/0002-DSR/2016
TELEFON ● (+43 1) 53115/2527
FAX ● (+43 1) 53115/2702
E-MAIL ● DSRPOST@BKA.GV.AT
DVR: 0000019

An das
Bundesministerium für Finanzen

Per Mail:
Alexander.Peschetz@bmf.gv.at
e-Recht@bmf.gv.at

Betrifft: Entwurf eines Bundesgesetzes, mit dem ein Bundesgesetz zur Verhinderung der Geldwäscherei und Terrorismusfinanzierung im Finanzmarkt **(Finanzmarkt-Geldwäschegesetz – FM-GwG)** erlassen wird und das Alternative Investmentfonds Manager-Gesetz, das Bankwesengesetz, das Betriebliche Mitarbeiter- und Selbständigenvorsorgegesetz, das Börsegesetz 1989, das Bundesgesetz über die Sanierung und Abwicklung von Banken, das Bundesgesetz zur Schaffung einer Abbaueinheit, das Bundeskriminalamt-Gesetz, das Devisengesetz 2004, das Einlagensicherungs- und Anlegerentschädigungsgesetz, das E-Geldgesetz 2010, das Finanzmarktaufsichtsbehördengesetz, das Gemeinsamer Meldestandard-Gesetz, das Glücksspielgesetz, das Investmentfondsgesetz 2011, das Kontenregister- und Konteneinschaugesetz, das Rechnungslegungs-Kontrollgesetz, das Sanierungs- und Abwicklungsgesetz, das Versicherungsaufsichtsgesetz 2016, das Wertpapieraufsichtsgesetz 2007 und das Zahlungsdienstegesetz geändert werden
Stellungnahme des Datenschutzrates

Der **Datenschutzrat** hat in seiner **231. Sitzung am 4. November 2016 einstimmig** beschlossen, zu der im Betreff genannten Thematik folgende Stellungnahme abzugeben:

1) Allgemeines

Laut den Erläuterungen soll mit dem gegenständlichen Gesetzesentwurf die Richtlinie (EU) 2015/849 umgesetzt werden und den internationalen Standards der

FATF entsprochen werden um gezielt dem Missbrauch des Finanzsystems für die Zwecke der Geldwäscherei und Terrorismusfinanzierung entgegenzuwirken.

Darüber hinaus soll für alle Kredit- und Finanzinstitute ein einheitlicher, übersichtlicher gesetzlicher Rahmen geschaffen werden, wodurch eine Vereinfachung bei der Anwendung der neuen Vorschriften bei Unternehmensgruppen und bei der Beaufsichtigung durch die FMA zu erwarten sind.

Zusätzliche Belastungen der Kredit- und Finanzinstitute sollen nach Möglichkeit vermieden werden bzw. sollen auch Maßnahmen gesetzt werden, die die Anwendung der Sorgfaltspflichten erleichtern.

Das Vorhaben umfasst nach Darstellung des BMF hauptsächlich folgende Maßnahmen:

Die bereits bestehenden interministeriellen Strukturen zur Zusammenarbeit der Ministerien und Behörden sollen aufgewertet werden und einen klar definierten gesetzlichen Auftrag erhalten.

Der risikoorientierte Ansatz soll sowohl im Hinblick auf die Anwendung der Sorgfaltspflichten als auch im Hinblick auf die Aufsicht durch die FMA erweitert werden.

Durch die Schaffung des Finanzmarkt-Geldwäschegesetzes (FM-GwG) sollen die Vorschriften für Kredit- und Finanzinstitute in einem Gesetz zusammengefasst werden.

Die Online- Identifizierung durch ein videogestütztes elektronisches Verfahren soll im Rahmen der normalen Sorgfaltspflichten ermöglicht werden, wenn das erhöhte Risiko aufgrund der fehlenden physischen Anwesenheit durch die Auswertung zusätzlicher Daten oder Informationen ausgeglichen wird.

2) Datenschutzrechtlich relevante Bestimmungen

Datenschutzrechtliche Vorbemerkungen

Vorweg wird darauf hingewiesen, dass ab dem 25. Mai 2018 die Verordnung (EU) Nr. 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – DSGVO) zur Anwendung kommt. Die derzeit geltende Form der Meldepflicht an das Datenverarbeitungs-

register (§§ 17 ff DSG 2000) wird aufgrund der Anwendung der DSGVO ab dem 25. Mai 2018 entfallen.

Anstelle des Meldeverfahrens sieht die DSGVO in Art. 35 die Einführung einer Datenschutz-Folgenabschätzung vor. Eine Datenschutz-Folgenabschätzung gemäß Art. 35 Abs. 1 DSGVO ist insbesondere in den Fällen des Abs. 3 erforderlich. Art 35 Abs. 10 DSGVO sieht unter den angeführten Voraussetzungen jedoch eine Ausnahme von der Datenschutz-Folgenabschätzung durch Verantwortliche für Verarbeitungen vor, die auf einer Rechtsgrundlage im Recht des Mitgliedstaates, dem der Verantwortliche unterliegt, beruhen und falls diese Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte.

In diesem Sinne wird – im Falle, dass eine Datenschutz-Folgenabschätzung nach den Vorgaben des Art. 35 DSGVO erforderlich ist – in Übereinstimmung mit dem Bundeskanzleramt-Verfassungsdienst angeregt, bei dem vorliegenden Vorhaben – und allen zukünftigen legistischen Vorhaben des Ressorts – zu prüfen, ob im Rahmen der allgemeinen Folgenabschätzung die Datenschutz-Folgenabschätzung bereits vorweggenommen und dies entsprechend gesetzlich angeordnet werden kann. In den Erläuterungen müsste die Durchführung der Datenschutz-Folgenabschätzung gemäß Art. 35 Abs. 7 DSGVO ausführlich dargelegt werden.

Zu Artikel 2 (Finanzmarkt-Geldwäschegesetz – FM-GwG)

Zu § 3:

Hinsichtlich der im Entwurf vorgesehenen Tätigkeit der Datenschutzbehörde (DSB) im Koordinierungsgremium nach Abs. 1 teilt der informierte Vertreter des Bundesministeriums für Finanzen in der Sitzung des Datenschutzrates mit, dass auf die Aufnahme der Datenschutzbehörde in das Koordinierungsgremium verzichtet wird.

Aus Sicht des Datenschutzrates widerspricht jedenfalls die Festlegung von Aufgaben für die Datenschutzbehörde nach **§ 3 Abs. 3 letzter Absatz eindeutig den unionsrechtlichen Zielsetzungen einer unabhängigen Datenschutzbehörde**. Die Datenschutz-Grundverordnung sieht dafür unmittelbar keine Zuständigkeit vor.

Die in **Abs. 4** vorgesehene Anordnung zur Übermittlung aller für die Erstellung der nationalen Risikoanalyse erforderlichen, den Finanzmarkt betreffenden Daten, Informationen, Analysen und Bewertungen durch die Nationalbank und die FMA ist zu pauschal und **sollte nach Ansicht des Datenschutzrates konkretisiert werden**. Grundsätzlich wäre die Ermächtigung zur Verwendung von konkreten Daten bereits im Zusammenhang mit der Festlegung der Aufgaben der FMA sowie der OeNB zu regeln. Weiters wird darauf hingewiesen, dass das „Verarbeiten von Daten“ gem. § 4 Z 9 DSG 2000 das „Ermitteln“ bereits mitumfasst.

Zu § 6:

Die Identitätsfeststellung einer natürlichen Person erfolgt gemäß **Abs. 2** anhand der im amtlichen Lichtbildausweis festgelegten Kriterien. Einzelne Kriterien (zB Name, Geburtsdatum, Unterschrift der Person) können entfallen, wenn „auf Grund des technischen Fortschritts andere gleichwertige Kriterien eingeführt werden, wie beispielsweise **biometrische Daten**“. **Inwiefern es im vorliegenden Zusammenhang dem Verhältnismäßigkeitsgrundsatz nach § 1 Abs. 2 DSG 2000 entspricht, biometrische Daten der Kunden zu verarbeiten, kann mangels näherer Erläuterungen zur Notwendigkeit dieser Maßnahme nicht beurteilt werden**. Unklar ist weiters, wie die biometrischen Daten der Kunden ermittelt werden sollen und was unter „anderen gleichwertigen Kriterien“ (neben dem Beispiel „biometrische Daten“) zu verstehen ist. **Keinesfalls** kann diese Bestimmung die Rechtsgrundlage für **jegliche künftige Form einer Identitätsfeststellung** bilden (zB DNA-Analyse). **Weiters fehlt die Festlegung konkreter Datensicherheitsmaßnahmen gemäß § 14 DSG 2000**.

Im Übrigen wird angemerkt, dass Art. 13 und 14 der umzusetzenden Richtlinie 2015/849/EU keine Verpflichtung zur Identitätsüberprüfung in dieser Form enthalten.

In **Abs. 4** wird für Fälle, in denen der Kunde zur Identifikation nicht physisch anwesend ist, eine Identifikation durch ein videogestütztes elektronisches Verfahren (**Online-Identifikation**) ermöglicht. Die diesbezüglichen Sicherungsmaßnahmen hat die FMA mit Zustimmung des Bundesministers für Finanzen mit Verordnung festzulegen. **Aus datenschutzrechtlicher Sicht kann auch unter Berücksichtigung der Erläuterungen mangels näherer Ausführungen sowie mangels entsprechender unionsrechtlicher Vorgaben die Vereinbarkeit dieser geplanten Maßnahme mit dem Verhältnismäßigkeitsgrundsatz gemäß § 1**

Abs. 2 DSG 2000 nicht beurteilt werden. Datensicherheitsmaßnahmen gemäß § 14 DSG 2000 wären aber bereits auf gesetzlicher Ebene festzulegen.

Zu § 16:

Art und **Umfang der Datenverwendung** in **Abs. 5** sind weitgehend **unklar**, da der vorliegende Entwurf die Geldwäschemeldestelle pauschal zur Verarbeitung „aller erforderlichen Daten“ ermächtigt. Darüber hinaus ist unklar, was unter „sonstigen Einrichtungen mit Rechtspersönlichkeit“ zu verstehen ist.

Zu § 21:

In **Abs. 6** wird festgelegt, dass ein Verpflichteter die Erteilung einer Auskunft gem. § 26 DSG 2000 zu verweigern hat, wenn dies aufgrund des Verbots der Informationsweitegabe gem. § 20 dieses Entwurfes erforderlich ist. Es fällt auf, dass die entsprechende Bestimmung in Art. 41 Abs. 4 der umzusetzenden Richtlinie 2015/849/EU eine Einschränkung des Auskunftsrechtes nur dann für zulässig erachtet, „soweit diese teilweise oder vollständige Einschränkung in einer demokratischen Gesellschaft eine erforderliche und verhältnismäßige Maßnahme darstellt und den berechtigten Interessen der betroffenen Personen Rechnung trägt“. Im Lichte der zitierten Richtlinienvorgabe und im Lichte der Formulierung der Ausnahmetatbestände in § 26 DSG 2000 sollte anstelle der absolut formulierten Ausnahme auf eine „Kann-Bestimmung“ umgestellt werden.

Der Datenschutzrat weist in diesem Zusammenhang darauf hin, dass bei einer automatisierten Einzelentscheidung die Vorgaben des § 49 DSG 2000 einzuhalten sind.

Zu § 22:

In § 22 sollte näher dargelegt werden, um welche „sicheren Kommunikationskanäle“ es sich hierbei handeln kann.

Zu § 24:

Durch **Abs. 6** soll sichergestellt werden, dass vom gruppenweiten Informationsaustausch jedenfalls auch „alle kundenbezogenen Daten“ umfasst sind. Zumal nach Art. 45 Abs. 8 der Richtlinie 2015/849/EU die übermittelten Informationen in einem Zusammenhang mit dem Verdacht stehen müssen, dass Gelder aus kriminellen Tätigkeiten stammen oder mit Terrorismusfinanzierung in Verbindung stehen, ist

unklar, aus welchen Gründen hier die Übermittlung von **allen** kundenbezogenen Daten angeordnet wird.

Zu § 25:

Hinsichtlich der in **Abs. 5 und Abs. 6** pauschal und äußerst umfassend vorgesehenen Möglichkeit der FMA zur Datenübermittlung an Behörden in Mitgliedstaaten und Drittländern wird darauf hingewiesen, dass nach dem Verhältnismäßigkeitsgrundsatz nach § 1 Abs. 2 DSG 2000 Datenverwendungen zu konkretisieren sind und nur in dem Ausmaß vorgesehen werden dürfen, als dies im Hinblick auf die angeführten Zwecke tatsächlich notwendig ist. Zu berücksichtigen ist weiters, dass Datenübermittlungen ins Ausland den Vorgaben der §§ 12 f. DSG 2000 unterliegen.

Zu § 26:

Es wird auf die Anmerkungen zu § 25 verwiesen. Im Übrigen wird festgehalten, dass das „Ermitteln von Daten“ bereits vom „Verarbeiten von Daten“ gem. § 4 Z 9 DSG 2000 umfasst ist.

Zu § 40:

Nach Ansicht des Datenschutzrates sollten alle Whistleblowing-Regelungen (d.s. anonyme Hinweisgebersysteme) in der österreichischen Rechtsordnung einheitlich ausgestaltet sein. Dies ist derzeit nicht der Fall. Daher wird grundsätzlich angemerkt, dass eine Regelung für Whistleblowing besondere datenschutzrechtliche Vorgaben enthalten muss, um dem Verhältnismäßigkeitsgrundsatz nach § 1 Abs. 2 DSG 2000 gerecht zu werden, so etwa hinsichtlich der Festlegung detaillierter Voraussetzungen für erlaubtes Whistleblowing, insbesondere dem Vorliegen einer begründeten Verdachtslage des Hinweisgebers, dem Schutz des Meldenden einerseits und der Verantwortung bei haltlosen Anschuldigungen andererseits sowie dem Schutz der Rechte der gemeldeten Person.

Es sollten zumindest die Eckpunkte für die datenschutzrechtlich geforderte Verhältnismäßigkeitsabwägung zwischen dem Interesse des Meldenden (z.B. Aufklärung von behaupteten Missständen im öffentlichen Interesse) und dem Interesse der gemeldeten Person gesetzlich vorgegeben werden.

In diesem Zusammenhang wird auf die Entscheidung der Datenschutzbehörde (DSB-D600.328-001/0001-DSB/2014 vom 13.5.2014) betreffend die Registrierung einer „Whistleblowing-Hotline“ unter entsprechenden Auflagen hingewiesen.)

Wesentlich ist aus Sicht des Datenschutzrates, dass die Kommunikation mit dem Hinweisgeber auch in anonymer Form stattfinden kann.

Eine Regelung für Hinweisgeber bzw. Whistleblower erfordert besondere datenschutzrechtliche Vorgaben, um dem **Verhältnismäßigkeitsgrundsatz nach § 1 Abs. 2 DSG 2000 gerecht zu werden**. Auch Art. 61 Abs. 2 lit. d der gegenständlichen Richtlinie legt fest, dass Mechanismen eingerichtet werden sollen, die den Schutz personenbezogener Daten gemäß den Grundsätzen der Richtlinie 95/46/EG sowohl für die Person, die die Verstöße meldet, als auch für die natürliche Person, die mutmaßlich für einen Verstoß verantwortlich ist, umfassen. **Hinsichtlich des Schutzes personenbezogener Daten ist der bloße Verweis nach § 40 Abs. 3 Z 4 auf die Grundsätze des DSG 2000 nicht ausreichend**, stattdessen sollten konkrete Regelungen vorgegeben werden, wie dieser Schutz verwirklicht werden soll. Hinsichtlich der in § 40 Abs. 2 vorgesehenen „Ermutigung“ durch die FMA, Verstöße oder den Verdacht eines Verstoßes anzuzeigen, ist unklar, wie diesfalls bei einer (allenfalls auch absichtlich) falschen Meldung eines Verstoßes vorgegangen werden soll.

Der Datenschutzrat nimmt die Ausführungen des informierten Vertreters des Bundesministeriums für Finanzen zur Kenntnis, dass den datenschutzrechtlichen Anregungen in der Stellungnahme des Bundeskanzleramtes-Verfassungsdienst zum vorliegenden Begutachtungsentwurf gefolgt wird.

Zu Artikel 6 (Änderung des Börsegesetzes 1989)

Zu § 25 Abs. 11:

Art und Umfang der Datenverwendung nach Abs. 11 zweiter Satz sind weitgehend unklar und wären zu präzisieren. Insbesondere sollte dargelegt werden, für welche Aufgaben welche konkreten Daten benötigt werden und welche Eigenschaften die genannte „Datei“ aufweist.

Zu berücksichtigen ist weiters, dass jede Übermittlung von Daten ins Ausland („Stellen anderer Staaten“) den Vorgaben der § 12 f. DSG 2000 unterliegt.

Zu Artikel 15 (Änderung des Glücksspielgesetzes)

Zu § 5:

Zu § 5 Abs. 4 lit. a Z 1 und lit. b Z 2 wird sinngemäß auf die Ausführungen oben unter Artikel 2 zu § 6 des Finanzmarkt-Geldwäschegesetzes verwiesen.

9. November 2016
Für den Datenschutzrat
Der Vorsitzende:
MAIER

Elektronisch gefertigt