REPUBLIK ÖSTERREICH DATENSCHUTZRAT

BALLHAUSPLATZ 2, A-1014 WIEN
GZ ● BKA-817.386/0003-DSR/2011
TELEFON ● (+43 1) 53115/2527
FAX ● (+43 1) 53115/2702
E-MAIL ● DSRPOST@BKA.GV.AT
DVR: 0000019

An das
Bundesministerium für Verkehr,
Innovation und Technologie

Betrifft: **Bundesgesetz, mit dem das Telekommunikationsgesetz 2003, das KommAustria-Gesetz sowie das Verbraucherbehörden-Kooperationsgesetz geändert werden; Stellungnahme des Datenschutzrates**

Der **Datenschutzrat** hat in seiner 207. Sitzung am 2. Mai 2011 **mehrheitlich – mit einer Gegenstimme** – **beschlossen**, zu dem vorliegenden Gesetzesentwurf nachstehende Stellungnahme abzugeben:

2) Datenschutzrechtlich relevante Bestimmungen:

Vorbemerkung

Vorweg bemerkt der Datenschutzrat, dass er davon ausgeht, dass die gegenständliche EU-Richtlinie vollständig und richtig, insbesondere im Hinblick auf Art. 5 Abs. 3, umgesetzt wird.

Kritisch anzumerken ist allgemein, dass im besonderen Teil der Erläuterungen z.T. keinerlei Bezüge zwischen vorgeschlagenen neuen Textelementen und den zugrunde liegenden EU-Richtlinienbestimmungen hergestellt werden, worunter die Nachvollziehbarkeit der Plausibilität bzw. Erforderlichkeit der Einfügungen entsprechend leidet und in der Begutachtung ein unnötig erhöhter Zeitaufwand entsteht (vgl. bspw. § 96 Abs. 3 TKGneu).

Zu Art. 1 Z. 28 des Entwurfs (§ 16a Abs. 3, 4, 7 und 11)

In § 16a Abs. 3, 4, und 7 ist hinsichtlich verschiedener Aufgabenstellungen jeweils eine „wahlweise“ Zuständigkeit von „Datenschutzkommission“ und „Regulierungsbehörde“ vorgesehen. Dieser Regelungsansatz steht in einem

offenkundigen Spannungsverhältnis zu Art. 83 Abs. 2 B-VG. Nach stRsp des Verfassungsgerichtshofs verpflichtet letztere Norm den einfachen Gesetzgeber dazu, Behördenzuständigkeiten nach objektiven Kriterien, exakt, klar und eindeutig festzulegen (vgl. VfSlg. 3156/1953; 9937/1984; 11.288/1987 u.a.). Die Regelung der Behördenzuständigkeit muss präzise sein und strengen Prüfungskriterien standhalten (VfSlg. 12.788/1991; 13.029/1992). Die Zuständigkeit darf insbesondere nicht von Umständen abhängen, die vom Rechtsunterworfenen nicht vorhersehbar sind (VfSlg. 14.192/1995). **Dem vorliegenden Entwurf sind gerade ebensolche Kriterien, die eine klare Abgrenzung der Zuständigkeiten zwischen Datenschutzkommission und Regulierungsbehörde erlauben würden, nicht zu entnehmen.**

Zu Abs. 4 ist festzuhalten, dass die Datenschutzkommission „im Rahmen ihrer gesetzlichen Aufgaben“ keinerlei Zuständigkeit besitzt, Betreiber der öffentlichen Kommunikationsnetze zu verpflichten, sich einer Sicherheitsprüfung durch die Datenschutzkommission zu unterziehen, oder eine solche durchzuführen. **Darüber hinaus steht der Datenschutzkommission für diese vorgesehene Kontrolltätigkeit kein (insbesondere auch kein hiefür geschultes) Personal zur Verfügung.**

Zu Art. 1 Z. 33 des Entwurfs (§ 23 Abs. 4)

Nach dieser Bestimmung soll „die Übertragung der Rufnummer des Teilnehmers ohne seine „zumindest in elektronischer Form erteilte Zustimmung“ unzulässig sein. Das dezidierte Abstellen auf ein bestimmtes Medium, bzw. einen bestimmten technischen Kommunikationsweg erscheint im vorliegenden Fall nicht unbedingt sachadäquat. Aus datenschutzrechtlicher Sicht kommt es lediglich auf das Vorliegen der Kriterien des § 4 Z 14 DSG 2000 an (informierte, zwangsfreie Einwilligung). Schriftlichkeit oder gar eine bestimmte mediale Form (Papier, elektronischer Weg) wird von § 4 Z 14 DSG 2000 nicht verlangt. Im vorliegenden Kontext spricht sicher einiges dafür, aus Beweissicherungsgründen auf Schriftlichkeit abzustellen. Ob diese Schriftlichkeit durch eine Einwilligung in elektronischer Form oder durch Unterschrift auf einem Papierformular gewährleistet wird, ist dagegen sekundär. Die im Text vorgesehen Formulierung „zumindest in elektronischer Form“ erweckt freilich den Eindruck, bei Letzterer handle es sich um eine geringwertigere Form. Dies trifft allerdings nicht zu. Es kommt, wie gesagt vielmehr auf die sonstigen Aspekte (echte

Freiwilligkeit, ausreichende Transparenz etc an). **Es sollte daher sichergestellt werden, dass auch die elektronische Zustimmung als ausreichend angesehen wird.**

Zu Art. 1 Z. 99 des Entwurfs (§ 92 Abs. 3 Z 11)

Diese Ziffer definiert die "Verletzung des Schutzes personenbezogener Daten" als „jede Verletzung der Sicherheit, die auf versehentliche oder unrechtmäßige Weise zur Vernichtung, zum Verlust, zur Veränderung und zur unbefugten Weitergabe von bzw. zum unbefugten Zugang zu personenbezogenen Daten führt, die übertragen, gespeichert oder auf andere Weise im Zusammenhang mit der Bereitstellung öffentlicher Kommunikationsdienste in der Gemeinschaft verarbeitet werden".

Diese Textierung entspricht wörtlich der deutschen Fassung des damit umgesetzten Art. 2 lit. i der Richtlinie (RL) 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, ABl. L 201 vom 31.7.2002, S. 37, i.d.F. der RL 2009/136/EG, ABl. Nr. L 337 vom 18.12.2009, S. 11.

Bei genauer Betrachtung fällt auf, dass sich hier allerdings ein sinnstörender Fehler eingeschlichen hat. Die Verwendung des Bindeworts „und" nach „Veränderung" erweckt nämlich den Eindruck, dass nur eine „versehentliche oder unrechtmäßige" Veränderung, die mit einer unbefugten Weitergabe einhergeht, unter den Begriff der „Datenschutzverletzung" fallen soll. Dies wäre aber weder sachlogisch begründbar noch im Einklang mit Art. 17 Abs. 1 der „allgemeinen" Datenschutzrichtlinie 95/46/EG, ABl. L 281, vom 23.11.1995, 31. Tatsächlich zeigt ein Blick in die englische Sprachfassung des Art. 2 lit. i der Richtlinie (RL) 2002/58/EG, dass hier ein Übersetzungs- bzw. Redaktionsversehen vorliegen dürfte. Nach der englischen Fassung bedeutet ein "personal data breach" nämlich "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community."

Im Ergebnis wäre somit, nach Überprüfung der einschlägigen Sprachfassungen, in § 92 Abs. 3 Z 11 TKGneu das Bindewort "und" durch das Wort "oder" zu ersetzen.

Zu Art. 1 Z. 101 des Entwurfs (§ 95a)

§ 95 a Abs.1 des Entwurfes legt eine Informationsverpflichtung durch den Betreiber der öffentlichen Kommunikationsdienste, im Falle einer Verletzung des Schutzes personenbezogener Daten von Personen fest.

Soweit anzunehmen ist, dass Personen in ihrer Privatsphäre selbst beeinträchtigt werden, hat der Betreiber auch die betroffenen Personen unverzüglich von dieser Verletzung zu benachrichtigen.

Mit der Datenschutzgesetz - Novelle 2010 wurde erstmals bereits in § 24 Abs. 2a DSG 2000, eine neue Informationspflicht bei Datenmissbrauch (Data Breach Notification Duty) eingeführt. Um einheitliche Informationsverpflichtungen zu gewährleisten, könnte vom zuständigen Ressort geprüft werden, ob im Zuge dieses Gesetzgebungsverfahrens und im Einklang mit den Entwicklungen auf europäischer Ebene, nicht auch eine Anpassung der Bestimmungen des § 24 Abs. 2 a DSG 2000, an die zukünftige Regelung im Telekommunikationsgesetz erfolgen sollte.

Zu Art. 1 Z. 103 des Entwurfs (§ 96 Abs. 3 Satz 2 und 3)

Zufolge des § 96 Abs. 3 Satz 1 TKGneu sind Betreiber öffentlicher Kommunikationsdienste verpflichtet, den Teilnehmer oder Benutzer darüber zu informieren, welche personenbezogenen Daten er ermitteln, verarbeiten und übermitteln wird, auf welcher Rechtsgrundlage und für welche Zwecke dies erfolgt und für wie lange die Daten gespeichert werden. Diese Regelung entspricht im Wesentlichen der geltenden Rechtslage.

In Umsetzung des Art. 5 Abs. 3 der RL 2002/58/EG i.d.F. der RL 2009/136/EG wird nun der zweite Satz neu gefasst**. Demnach „ist eine Ermittlung dieser Daten ist nur zulässig, wenn der Teilnehmer oder Nutzer seine Einwilligung dazu erteilt hat“.** Dies, so der geringfügig modifizierte Folgesatz, „steht einer technischen Speicherung oder dem Zugang nicht entgegen, wenn der alleinige Zweck die Durchführung der Übertragung einer Nachricht über ein Kommunikationsnetz ist oder, wenn dies unbedingt erforderlich ist, damit der Anbieter eines Dienstes der Informationsgesellschaft, der vom Teilnehmer oder Benutzer ausdrücklich gewünscht wurde, diesen Dienst zur Verfügung stellen kann“. Um das Verhältnis der beiden zuletzt zitierten Sätze zueinander zu verdeutlichen bzw. den Sinngehalt des Letzteren leichter fassbar zu machen, sollte Satz 3 des § 96 Abs. 3 leg. cit. etwas

zielgerichteter formuliert bzw. eingeleitet werden, uzw. etwa wie folgt: **„Keiner solche Einwilligung bedarf es für eine technische Speicherung oder den Zugang zu solchen Daten, wenn deren alleiniger Zweck die Durchführung […] ist […].**

Die zunehmende Verwendung so genannter **„Cookies“** und vergleichbarer technischer Gestaltungen werfen Bedenken im Hinblick auf den Schutz des Grundrechts auf Datenschutz und der Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme auf. Dies gilt insbesondere im Hinblick auf die Gefahr einer Profilbildung durch die Verknüpfung einer Vielzahl von – z. B. unter Einsatz von „Cookies“ gewonnener - Informationen und Daten, ohne das der Nutzer hiervon Kenntnis oder Einfluss hierauf hat.

Zur Problematik von „Cookies“ verweist in diesem Zusammenhang der Datenschutzrat auf Erwägungsgrund 66 der Richtlinie 2009/136/EG, zur Änderung der Richtlinie 2002/22/EG über den Universaldienst und Nutzerrechte bei elektronischen Kommunikationsnetzen und –diensten, der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation und der Verordnung (EG) Nr. 2006/2004 über die Zusammenarbeit im Verbraucherschutz, sowie auf die laufende Diskussion auf europäischer Ebene, wo Guidelines für die Umsetzung des Artikel 5 Abs. 3 der gegenständlichen Richtlinie erarbeitet werden.

Zu Art. 1 Z. 110 des Entwurfs (§ 106 Abs. 2 und 3)

Zur in § 106 TKG schon bisher geregelten „Fangschaltung“ ist anzumerken, dass dem Gesetz keinerlei Befristungen – etwa im Sinne einer Höchstdauer - für solche Maßnahmen zu entnehmen sind. Da in bestimmten sensiblen Zusammenhängen (Bsp.: Hotline für psychische Krisenfälle uä.) ein grundsätzliches Interesse von Anrufern bestehen kann, insbesondere durch die angerufene Stelle nicht identifiziert zu werden, böte es sich im Zuge der Novellierung an, auch diese Frage zu regeln.

Sonstiges

In den Erläuterungen zu § 16a ist sinnstörender Weise die Rede davon, dass „[…] diese Probleme auch Gefahren der Sicherheit oder Vertraulichkeit der Daten selbst

verursachen [können], die die Datenschutzkommission gemäß § 95a zu vollziehen hat“.

Abschließend hält der Datenschutzrat aus grundsätzlichen Überlegungen Folgendes fest:

Um die Tätigkeit der Datenschutzkommission als Kontrollbehörde in diesem Zusammenhang sicherzustellen, wäre für deren Kontrolltätigkeit zuerst die gesetzliche Zuständigkeit klarzustellen.

Sollten der Datenschutzkommission Kontrollaufgaben nach dem TKG im Sinne dieses Entwurfes übertragen werden, muss allerdings sichergestellt sein, dass zur Erfüllung dieser Aufgaben auch die dafür erforderlichen Ressourcen zur Verfügung gestellt werden.

Darüber hinaus ersucht der Datenschutzrat, vor Erlassung der im Gesetzesentwurf vorgesehenen Verordnungsermächtigungen und im Falle eines datenschutzrechtlichen Bezugs, dem Datenschutzrat die Möglichkeit zur Abgabe einer Stellungnahme zu geben.

Anlage:
Votum Separatum Dr. Zeger

4. Mai 2011
Für den Datenschutzrat
Der Vorsitzende:
MAIER

Elektronisch gefertigt