REPUBLIK ÖSTERREICH
BUNDESMINISTERIUM FÜR JUSTIZ
BMJ-A231.00/0006-Pr 6/2009

Museumstraße 7
1070 Wien

Briefanschrift
1016 Wien, Postfach 63

e-mail
Kzl.A@bmj.gv.at

Telefon (01) 52152-0*
Telefax (01) 52152 2727

Sachbearbeiter(in): Mag. Gerhard Nogratnig
*Durchwahl: 2289

An das Bundeskanzleramt
Sektion III

iii@bka.gv.at

An das
Präsidium des Nationalrates

begutachtungsverfahren@parlament.gv.at

Betrifft: Entwurf eines Bundesgesetzes, mit dem das BDG 1979, das VBG und andere Bundesgesetze geändert werden (IKT-Nutzung) – Stellungnahme

Das Bundesministerium für Justiz beehrt sich, zu dem in Rede stehenden Begutachtungsentwurf folgende Stellungnahme abzugeben:

Eingangs ist anzumerken, dass im Entwurf (§ 79c Abs. 2) **lediglich Bestimmungen zu Kontrollmaßnahmen** vorgesehen sind, sich jedoch keine Grundlage für die Zulässigkeit der Aufzeichnung der personenbezogenen Daten und deren Sammlung an sich findet. Eine solche Datensammlung bildet jedoch die Voraussetzung für die Möglichkeit der Einsichtnahme, bevor in einem dritten Schritt deren weitere Verwendung zu regeln ist.

In § 79c Abs. 2 ist weiters von **personenbezogenen Daten der IKT-Nutzung** die Rede, wobei sich die Frage stellt, ob darunter alle personenbezogenen Daten fallen (auch dienstliche Emails) oder nur jene Daten, die der privaten Nutzung zuzuordnen sind. Überdies wird dabei **nicht zwischen persönlichen Daten des IKT-Nutzers und jenen von dritten Personen**, mit denen dieser in Kontakt steht, **unterschieden**. Mit den vorgesehenen Kontrollmaßnahmen sind jedenfalls auch Eingriffe in die Persönlichkeitsrechte Dritter möglich bzw. verbunden, weshalb den Bestimmungen des Datenschutzgesetzes auch außerhalb des Dienstverhältnisses besondere Bedeutung zukommt (§ 1 und §§ 17ff DSG).

Im konkreten Fall soll die Kontrolle einerseits Schäden an der IKT-Infrastruktur vorbeugen andererseits im Fall eines begründeten Verdachts einer „gröblichen“ Dienstpflichtverletzung zum Zweck der Verhinderung weiterer Dienstpflichtverletzungen, wenn zeitliche, inhaltliche oder quantitative Beschränkungen der bereitgestellten IKT-Nutzung dafür nicht ausreichen, oder zum Zweck der „Klarstellung“ des Sachverhalts eingesetzt werden dürfen (§ 79c Abs. 2 BDG 1979 in der Fassung des Entwurfs).

Zur Kontrolle bei begründetem Verdacht einer gröblichen Dienstpflichtverletzung (§ 79e BDG in der Fassung des Entwurfs) ist zu bemerken,

- dass damit – nicht nur Fall der Anordnung im Fall des Verdachts gegen einen konkreten Bediensteten gemäß Abs. 7 - der strafprozessuale Regelungsbereich der Auskunft über Daten einer Nachrichtenübermittlung sowie der Überwachung von Nachrichten (§§ 134, 135 StPO) unterlaufen wird, die grundsätzlich den Verdacht einer vorsätzlich begangenen Straftat voraussetzt, die mit Freiheitsstrafe von mehr als einem Jahr bedroht ist;
- dass zwar in § 79c Abs. 3 BDG 1979 in der Fassung des Entwurfs klargestellt wird, dass Inhalte übertragener Nachrichten nicht Gegenstand von Kontrollmaßnahmen zum Zweck der Verhinderung weiterer Dienstpflichtverletzungen oder zum Zweck der „Klarstellung“ des Sachverhalts sein dürfen, jedoch im Übrigen der Datenbegriff des Entwurfs ebenso wie der zentrale Begriff der „**gröblichen Dienstpflichtverletzung**“ keiner inhaltlich ausreichenden Determinierung zugeführt werden kann (nur als Beispiel: unter welchen Bedingungen wäre eine Verletzung der §§ 2 bis 4 der IKT-Verordnung als „gröblich“ zu bezeichnen?). Ebenso wirft der Begriff „**unbedingt notwendig**“ Unklarheiten und Widersprüche auf und schafft einen großen Interpretationsspielraum. Ein derart schwerwiegender Eingriff in die Persönlichkeitsrechte eines Beamten und/oder Dritter bedarf einer genauen Determinierung der Umstände, unter welchen die Interessen des Dienstgebers unter Berücksichtigung des Verhältnismäßigkeitsprinzips die schutzwürdigen Interessen der Betroffenen verdrängen. Insbesondere wird erst nach Einschau in den Inhalt der Nachrichten beurteilt werden können, ob die inhaltliche Kontrolle „unbedingt notwendig“ ist, weshalb diese Bestimmung einen unlösbaren inneren Widerspruch in sich birgt.

Auf beide Fragen gehen im Übrigen auch die Erläuterungen nicht ein.

Verfassungsrechtlich können Ermittlungsbefugnisse vergleichbarer Art wohl nur dann gerechtfertigt werden, wenn man – wie die **arbeitsrechtlichen Senate des OGH** (8 ObA 288/01p; 9 ObA 109/06d) – davon ausgeht, dass bestimmte Daten einer IKT-Nutzung nicht dem Bereich des Fernmeldegeheimnisses unterliegen (Artikel 10a StGG). Gerade dann wäre es jedoch unentbehrlich, die angesprochenen Datenkategorien im Gesetz genau zu umschreiben.

Der OGH erklärt in diesen beiden Entscheidungen, welche nur die lückenlose Erfassung „äußerer“ und nicht inhaltlicher Grunddaten betreffen, dass solche Kontrollsysteme (dort betreffend die Telefonanlage bzw. Fingerscanning) die Menschenwürde berühren können, weshalb die Zustimmung des Betriebsrates iSd § 96a ArbVG einzuholen sei. Auch werde bei Verwendung der oben angeführten Systeme das schutzwürdige Interesse an der Geheimhaltung personenbezogener Daten gemäß § 1 Abs. 1 DSG nicht berücksichtigt. In seiner Begründung zur Entscheidung zu 8 ObA 288/01p erklärte der OGH, dass es den beiderseitigen Interessen entspräche, eine Betriebsvereinbarung abzuschließen, wo Schutzmaßnahmen vor übermäßiger Kontrolle in folgender Weise festgeschrieben werden sollten: Die Rufdatenerfassung **sollte nur im Verdachtsfall unter Einbeziehung des Betriebsrates geöffnet werden können**. Im Falle des Weiterbestehens von Verdachtsmomenten sollten diese nach Information des Betriebsrates **mit dem jeweiligen Dienstnehmer erörtert werden** und weitere Erhebungen sollten erst möglich sein, wenn der Dienstnehmer die Verdachtsmomente nicht entsprechend entkräften könne.

Werden die vom OGH festgelegten Grundsätze auf den vorliegenden Gesetzesentwurf übertragen, wäre die **Personalvertretung bereits vor und bei Einsichtnahme** in die aufgezeichneten „äußeren“ Daten einzubeziehen. Hier wäre zum Schutz auch eine **automatische Protokollierung** der Einschau wünschenswert, um – wie im Datenschutzrecht üblich - Missbrauch zu verhindern bzw. nachvollziehbar zu machen.

Bei **Einsicht in die inhaltlichen, personenbezogenen Daten** wäre wohl eine noch restriktivere, die schutzwürdigen Interessen der Betroffenen im Sinne der Bestimmungen des DSG und des Artikels 8 MRK sowie des Briefgeheimnisses berücksichtigende Regelung einzuführen.

Die **Strafsenate des OGH** sehen das freilich grundsätzlich anders und beziehen Vermittlungs- oder Verkehrsdaten regelmäßig in den Anwendungsbereich der

Bestimmungen über die Überwachung einer Telekommunikation ein (13 Os 161/95; zuletzt 11 Os 57/05z).

Das ist jedoch unabhängig von diesem Lehrenstreit deshalb von Bedeutung, weil Verwertungsverbote damit auf dem Umweg eines Disziplinarverfahrens unterlaufen werden können, wenn der Verdacht der Dienstpflichtverletzung zugleich den Verdacht einer Straftat begründet, die für sich genommen keine Anordnung und Bewilligung einer Maßnahme nach den §§ 134 und 135 StPO rechtfertigen würde. Dafür besteht aus Sicht des Bundesministeriums für Justiz ausgehend von einem „Stufenbau“ der Strafrechtsordnungen (und dem Grundsatz der Verhältnismäßigkeit) keine Rechtfertigung. Gleichzeitig besteht aber auch die Gefahr einer Verhinderung sinnvoller strafprozessualer Überwachungsmaßnahmen, weil die betroffenen Bediensteten umgehend von dem Ermittlungsauftrag in Kenntnis zu setzen sind (§ 79e Abs. 3 und 7 BDG 1979 in der Fassung des Entwurfs).

Schließlich wird dem Leiter der Dienststelle damit aber auch eine Ermittlungsfunktion übertragen, die grundsätzlich den Disziplinarkommissionen obliegt; im Fall eines begründeten Verdachts ist wohl ein Disziplinarverfahren einzuleiten und von der Kommission zu entscheiden, welche Ermittlungen zur Klärung des Verdachts durchzuführen sind.

Soweit in § 79e des Entwurfes davon ausgegangen wird, dass der Leiter einer Dienststelle die IT-Stelle beauftragen kann, auf einen Verdachtsfall Bezug habende Daten der IKT-Nutzung zu „ermitteln“, ergibt sich die Frage, ob die daran geknüpften Pflichten (Abs 2 und Abs 3) auch ausgelöst werden, wenn die Zugriffsmöglichkeit des Dienstgebers (der IT-Stelle) auf eine Datensammlung bereits – ohne Übergabe eines bestimmten Codes oder mittels Einschaltung einer dritten Person – besteht, weil sich die Daten in seiner Gewahrsame befinden und keine Protokollierung der Nutzung dieser Zugriffsmöglichkeit stattfindet.

Weiters ergeben sich **Zweifel, ob** vom Begriff der IKT-Nutzung **auch elektronische Akten erfasst** sind. Die Begriffsbestimmungen in § 79g geben dahingehend Aufschluss, dass als IKT-Infrastruktur alle Geräte, die vom Dienstgeber zur Verfügung gestellt werden oder im Einvernehmen mit dem Dienstgeber für dienstliche Zwecke benützt werden und der Informationsverarbeitung für Zwecke des Dienstgebers dienen, sowie die darauf befindlichen Programme und Daten mit der Ausnahme von Fernsprechanlagen zu verstehen sind. Elektronische Akten sind jedoch weder vom Dienstgeber speziell dem Dienstnehmer zur Verfügung gestellt

noch im Einvernehmen mit dem Dienstgeber für dienstliche Zwecke zu benützen, sondern im Rahmen der Gesetze, der Approbationsbefugnisse, Zuständigkeiten und des Weisungszuges. Daher dürften elektronische Akten wohl nicht unter diese Definition fallen. Dies sollte aber klargestellt werden. Bei der Einbeziehung elektronischer Akten würde sich wiederum das Problem stellen, ob die Grundsätze der Datenverwendung auch auf jene Personen anzuwenden ist, denen Einsichtsbefugnisse kraft ihrer Amtsstellung im Verfahren zukommen.

Zur Systematik des Entwurfs ist zu bemerken, dass die Bestimmungen zT nicht recht klar geordnet sind. So soll gemäß § 79e Abs. 1 ein schriftlicher Ermittlungsauftrag zu ergehen haben, auf Grund dessen einerseits die IT- Stelle über die IKT-Nutzungen im Umfang des Ermittlungsauftrags in anonymisierter Weise (Abs. 2) zu berichten, andererseits dem Leiter der Dienststelle über die IKT-Nutzungen im Umfang des Verlangens nach Abs. 5 namentlich und in schriftlicher Form zu berichten (Abs. 6) haben. Erst aus dem Zusammenhalt der Bestimmungen des Abs. 5 mit jener des Abs. 3 Z 2 ergibt sich, dass diese namentliche Berichterstattung nur in dem Fall zulässig ist, dass der im Ermittlungsauftrag gemäß Abs. 1 genannte Verdachtsfall fortbesteht oder ein gleichgelagerter Verdachtsfall auftritt.

Gleiches gilt auch für die zulässige Dauer der Überwachung, weil sich diese bloß aus der verpflichtenden Mitteilung gemäß § 79e Abs. 3 BDG 1979 in der Fassung des Entwurfs ergibt. Nach der Formulierung des Abs. 4 dieser Bestimmung („Ein längerer als der in Abs. 3 Z 2 vorgesehene Beobachtungszeitraum darf nur in begründeten Ausnahmefällen festgesetzt werden.“) ist wiederum zweifelhaft, ob eine Verlängerung zulässig ist.

Die Formulierung des Abs. 7 lässt wiederum nicht eindeutig bestimmen, ob der Beamte nach Übermittlung eines Berichts der IT- Stelle umgehend zu informieren ist oder bereits vom Ermittlungsauftrag, die Formulierung des letzten Satzes lässt beide Auslegungsvarianten offen („Der Beamte und das zuständige Organ der Personalvertretung sind vom Leiter der Dienststelle umgehend über den Ermittlungsauftrag und über den Bericht der IT-Stelle zu informieren.“).

Zuletzt wäre zu klären, in welchem Verhältnis die neuen Mitwirkungsrechte der Personalvertretung gemäß § 9 Abs. 2 lit. n und o PVG zum bestehenden Mitwirkungsrecht nach lit. f stehen (bzw. weiter greifend, in welchem Verhältnis die da bzw. dort angesprochenen Maßnahmen zueinander stehen).

*****

Zusammenfassend wird angeregt, das **Grundkonzept** insbesondere im Zusammenhang mit den Bestimmungen des Datenschutzes und der Judikatur zu den Persönlichkeitsrechten zu **überdenken** und zu verfeinern, eine Befugnis zur „Klarstellung von Dienstpflichtverletzungen“ (§ 79c Abs. 2 Z 2 BDG 1979 idF des Entwurfs) (i.S. eines bloßen Erkundungsbeweises) sollte damit nicht verbunden sein.

05. Februar 2009
Für die Bundesministerin:
Dr. Anton Paukner

Elektronisch gefertigt