Vorblatt

Problem:

Die zunehmende Ausstattung von Arbeitsplätzen mit moderner Informationstechnologie führt zur Fragestellung, in welchem Umfang und in welcher Weise die Kontrolle der Bediensteten durch den Dienstgeber zulässig ist. Auch viele Bedienstete im Bundesdienst haben bereits Zugang zu Internetdienstleistungen, wie dem World Wide Web (WWW) oder E-Mail. Obwohl dadurch der Aktionsradius der Bediensteten wesentlich erweitert wird, bringen die neuen Kommunikationstechnologien nicht nur Vorteile mit sich. Zum einen wird auf Seiten der Bediensteten ein nicht zu unterschätzendes Missbrauchspotential geschaffen, zum anderen entstehen aufgrund der Datenvernetzung bisher nicht vorhandene Kontrollmöglichkeiten auf Seiten des Dienstgebers.

Ziel:

Durch den vorliegenden Entwurf soll ein dem Verhältnismäßigkeitsprinzip entsprechender Ausgleich dieser diametral entgegenstehenden und teilweise grundrechtlich geschützten Interessen auf Bediensteten- und Dienstgeberseite betreffend Nutzungs- und Kontrollmöglichkeiten geschaffen werden.

Inhalt:

Schaffung einer gesetzlichen Grundlage für die Zulässigerklärung der privaten IKT-Nutzung, insbesondere auch von Internet und E-Mail, durch die Bediensteten und für die Festlegung von Nutzungsgrundsätzen durch Verordnung der Bundesregierung; Festlegung von Kontrollgrundsätzen, mit denen eine überschießende und damit unverhältnismäßige Kontrolle durch den Dienstgeber hintangehalten werden soll.

Alternativen:

Keine.

Finanzielle Auswirkungen:

Keine. Es ist davon auszugehen, dass eventuell erforderliche Adaptierungen der Software aus den laufenden Budgets bedeckt werden können. Keine Zusatzkosten sollten auch durch die Zulässigerklärung der privaten IKT-Nutzung entstehen, da diese nicht jene Kosten übersteigen sollte, die durch eine bisherige – vom Dienstgeber tolerierte – private IKT-Nutzung entstanden sind.

Auswirkungen auf die Beschäftigung und den Wirtschaftsstandort Österreich:

Keine.

Auswirkungen auf die Verwaltungslasten für Unternehmen:

Es sind keine Informationsverpflichtungen für Unternehmen vorgesehen.

Auswirkungen in umweltpolitischer Hinsicht, insbesondere Klimaverträglichkeit:

Das Regelungsvorhaben ist nicht klimarelevant.

Auswirkungen in konsumentenschutzpolitischer sowie sozialer Hinsicht:

Keine.

Geschlechtsspezifische Auswirkungen:

Keine.

Besonderheiten des Normerzeugungsverfahrens:

Keine.

Verhältnis zu Rechtsvorschriften der Europäischen Union:

Die vorgesehenen Regelungen sind mit dem Gemeinschaftsrecht, insbesondere der Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, ABl. Nr. L 281 vom 23. November 1995 S. 31, vereinbar.

Erläuterungen

I. Allgemeiner Teil

Die zunehmende Ausstattung von Arbeitsplätzen mit moderner Informationstechnologie führt zur Fragestellung, in welchem Umfang und in welcher Weise die Kontrolle der Bediensteten durch den Dienstgeber zulässig ist. Auch viele Bedienstete im Bundesdienst haben bereits Zugang zu Internetdienstleistungen, wie dem World Wide Web (WWW) oder E-Mail. Obwohl dadurch der Aktionsradius der Bediensteten wesentlich erweitert wird, bringen die neuen Kommunikationstechnologien nicht nur Vorteile mit sich. Zum einen wird auf Seiten der Bediensteten ein nicht zu unterschätzendes Missbrauchspotential geschaffen, zum anderen entstehen aufgrund der Datenvernetzung bisher nicht vorhandene Kontrollmöglichkeiten auf Seiten des Dienstgebers.

Durch den vorliegenden Entwurf soll ein dem Verhältnismäßigkeitsprinzip entsprechender Ausgleich dieser diametral entgegenstehenden und teilweise grundrechtlich geschützten Interessen auf Bediensteten- und Dienstgeberseite betreffend Nutzungs- und Kontrollmöglichkeiten geschaffen werden.

Die Bediensteten sind vor übermäßiger Kontrolle am Arbeitsplatz durch den Dienstgeber zu schützen. Eine Balance zwischen dem Schutz der Bediensteten und den berechtigten Interessen des Dienstgebers ist in diesem Sinne zu gewährleisten. Transparenz in Form von Grundsätzen für die private IKT-Nutzung ist daher besonders wichtig, damit die Bediensteten ihr Verhalten zulässig gestalten und somit eine Kontrolle vermeiden können. Sind Kontrollen aus den gesetzlich festgelegten Gründen dennoch erforderlich, so sind diese dem gegenständlichen Entwurf zufolge grundsätzlich einem Modell stufenweiser Kontrollverdichtung entsprechend vorzunehmen (zu diesem Modell *Kotschy/Reimer*, Die Überwachung der Internet-Kommunikation am Arbeitsplatz, ZAS 2004, 169).

Der Entwurf legt Kontrollgrundsätze für den Dienstgeber fest, die eine überschießende und damit unverhältnismäßige Kontrolle der IKT-Nutzung durch die Bediensteten hintanhalten sollen. Im Verfahren einer stufenweisen Kontrollverdichtung wird die Protokollierung von Daten aus technischen Gründen zwar maschinen- und damit auch personenbezogen vorgenommen. Die Kontrolle erfolgt allerdings vorerst nur durch die IT-Stelle. Erst und bloß im Fall des Weiterbestehens einer Gefahr für die IKT-Infrastruktur bzw. ihre korrekte Funktionsfähigkeit oder einer pflichtwidrigen Nutzung ist – in einem zweiten Schritt – die Offenlegung der personenbezogenen Daten gegenüber dem Leiter oder der Leiterin der jeweils zuständigen Dienststelle vorgesehen. Ausgenommen von diesem Verfahren einer stufenweisen Kontrollverdichtung sind nur die Fälle einer konkreten unmittelbaren Gefährdung für die IKT-Infrastruktur oder ihre korrekte Funktionsfähigkeit und ein bereits vorliegender begründeter Verdacht einer gröblichen Dienstpflichtverletzung gegen einen bestimmten Bediensteten oder eine bestimmte Bedienstete. Durch die im Entwurf ebenfalls vorgesehene Änderung des PVG werden die Mitwirkungsrechte der Personalvertretung bei der Durchführung von Kontrollmaßnahmen festgelegt.

Gleichzeitig wird eine gesetzliche Grundlage für die Zulässigerklärung der privaten Nutzung der IKT-Infrastruktur, insbesondere auch von Internet und E-Mail, durch die Bediensteten und für die Festlegung von Nutzungsgrundsätzen durch Verordnung der Bundesregierung geschaffen.

Kompetenzgrundlage:

Die Zuständigkeit des Bundes zur Erlassung des vorgeschlagenen Bundesgesetzes ergibt sich hinsichtlich der Art. 1 bis 4 (BDG 1979, VBG, RStDG, PVG) aus Art. 10 Abs. 1 Z 16 B-VG (Dienstrecht und Personalvertretungsrecht der Bundesbediensteten).

II. Besonderer Teil

Zu Art. 1, Art. 2, Art. 3 (§§ 79c bis 79i BDG 1979, § 29n VBG, § 206 erster Satz RStDG):

Zu § 79c Z 1 BDG 1979:

Der Begriff IKT ist die zusammenfassende Bezeichnung für Computer- und Kommunikationstechnik. Er erfasst alle Einrichtungen und Netze für die Übertragung sowie die für Empfang, Versand und Verarbeitung erforderlichen Endgeräte.

Zu § 79d BDG 1979:

Sowohl im öffentlichen Dienst als auch in der Privatwirtschaft ist es Realität, dass die IKT-Infrastruktur, die für dienstliche bzw. betriebliche Zwecke zur Verfügung steht, von den Bediensteten bzw. Arbeitnehmern auch privat genutzt wird. Diese Realität wird im Regelfall in einem gewissen Ausmaß und – sofern dies mit den in § 45 BDG 1979 und § 5b VBG normierten Dienstpflichten in Einklang gebracht

werden kann – vom Dienstgeber toleriert. Mit der gegenständlichen Bestimmung soll klargestellt werden, dass die IKT-Infrastruktur grundsätzlich nur dienstlichen Zwecken dienen soll, in einem eingeschränkten Ausmaß und unter Einhaltung gewisser Nutzungsbedingungen aber auch privat genutzt werden darf. Diese Nutzungsbedingungen, die – unbeschadet weiterer ressort- bzw. arbeitsplatzspezifischer Nutzungsregelungen – durch Verordnung der Bundesregierung festzulegen sind, haben sich auf den zeitlichen Rahmen sowie Art und Umfang einer zulässigen privaten Nutzung zu beziehen. Sie haben damit auch näher festzulegen, was unter einer missbräuchlichen Nutzung zu verstehen ist, womit einerseits eine exzessive zeitliche und quantitative Nutzung gemeint ist, andererseits aber auch die Art der Nutzung wie beispielsweise eine missbräuchliche Berufung auf die dienstliche Stellung eines Beamten für private Zwecke. Wie Beispiele aus der Vergangenheit gezeigt haben, schadet dem Ansehen des öffentlichen Dienstes der Zugriff auf rechtswidrige oder aus sittlichen Gründen verpönte Internetseiten wie z.B. Seiten mit pornografischem Inhalt. Die Aufrechterhaltung eines geordneten Dienstbetriebes und die Sicherheit sowie die Leistungsfähigkeit der IKT-Infrastruktur sind schließlich ebenfalls einerseits durch eine exzessive Nutzung, andererseits aber durch das Herunterladen von bestimmten, besonders für deren Anfälligkeit für Schadprogramme bekannten, ausführenden Dateitypen beeinträchtigt bzw. gefährdet.

Die Beamten haben keinen Anspruch auf eine private Nutzung der für den Dienstbetrieb zur Verfügung stehenden IKT-Infrastruktur. Da sich eine private Nutzung immer nur auf die für den Dienstbetrieb bestehende IKT-Infrastruktur beziehen kann, steht es dem Dienstgeber frei zu entscheiden, ob bzw. welche IKT-Infrastruktur zur Verfügung steht. Es steht ihm damit prinzipiell auch frei zu entscheiden, welche Zugriffsmöglichkeiten er auf das Internet ermöglicht, da Ausgangspunkt immer die für den Dienstbetrieb erforderlichen Zugriffsmöglichkeiten sind. Er darf daher auch Filtersoftware zum Einsatz bringen. Werden jedoch nicht nur für den Dienstbetrieb erforderliche, sondern auch weitere Internetangebote allgemein zugänglich gemacht, so ist bei einer Beschränkung nach sachlichen, durch diese Bestimmung vorgezeichneten Motiven vorzugehen (vgl. in diesem Zusammenhang zum in Art. 10 EMRK verbürgten Grundrecht auf Informationsfreiheit EGMR 19. 12. 1994, ÖJZ 1995/23).

Zu § 79e BDG 1979:

Abs. 1 entspricht dem Wortlaut des bisherigen § 79c. Die Datenverwendung in anderen als den in Abs. 2 genannten Fällen bzw. unter Nichteinhaltung der Vorschriften der §§ 79f und 79g – sowohl durch den Dienstgeber als auch durch die IT-Stelle – zu Kontrollzwecken ist unzulässig (zB. der Einsatz von Software, die Arbeitsgewohnheiten der Bediensteten aufzeichnet [„Spionage-Software“]). Vom Begriff der Kontrolle nicht umfasst ist jedoch der Einsatz von Software-Programmen, die zur vollautomatischen Abwehr von Computerviren oder Ähnlichem bzw. als Spamfilter dienen. Schon nach geltendem Recht dürfen Kontrollmaßnahmen nur dann eingeführt werden, wenn diesbezüglich ein Einvernehmen mit dem Zentralausschuss im Sinne des § 10 PVG hergestellt wird (§ 14 Abs. 3 erster Satz PVG).

Die §§ 79e bis 79g BDG 1979 legen Kontrollgrundsätze fest, die eine überschießende und damit unverhältnismäßige Kontrolle durch den Dienstgeber hintanhalten sollen. Ihre Nichteinhaltung wäre nicht nur allgemein rechtswidrig, sondern würde gleichzeitig die Begehung einer Dienstpflichtverletzung durch die die Kontrollen durchführenden Bediensteten darstellen.

Im Hinblick auf das Vorliegen eines begründeten Verdachtes der Begehung von Dienstpflichtverletzungen soll ein überschießender Zugriff auf Daten der Bediensteten dadurch verhindert werden, dass nicht jegliches pflichtwidrige Verhalten eine Kontrolle der IKT-Nutzung von Bundesbediensteten legitimieren kann, sondern nur ein solches, das eine gröbliche Verletzung von Dienstpflichten bedeutet (Abs. 2 Z 2). Mit dem Begriff der gröblichen Dienstpflichtverletzung wird – da diese Bestimmung für Beamte und Vertragsbedienstete gleichermaßen gelten soll – an den Kündigungsgrund des § 32 Abs. 2 Z 1 VBG angeknüpft.

Gemäß Abs. 3 dürfen Inhalte übertragener Nachrichten (Inhaltsdaten) nicht Gegenstand von Kontrollmaßnahmen sein, die im Hinblick auf das Bestehen eines begründeten Verdachtes einer gröblichen Dienstpflichtverletzung erfolgen. Auch zur Abwehr von Schäden an der IKT-Infrastruktur und zur Gewährleistung ihrer korrekten Funktionsfähigkeit dürfen Inhaltsdaten nur dann kontrolliert werden, wenn dies zur Erreichung dieser Zwecke unbedingt notwendig ist. Die zuständige IT-Stelle hat daher aufgrund ihres technischen Sachverstandes im Einzelfall jeweils zu prüfen, ob es – in einer Betrachtung ex ante – nicht möglich ist, diese Zwecke anders als durch den Zugriff auf Inhaltsdaten zu erreichen. Selbst für diesen Fall wird im § 79f Abs. 1 und 4 jedoch festgelegt, dass diese Daten von der IT-Stelle nicht an den Leiter oder die Leiterin der zuständigen Dienststelle weitergegeben werden dürfen. Die Definition des Begriffes „Nachricht“ in § 79c Z 6 orientiert sich dabei am § 92 Abs. 3 Z 7 TKG 2003 und damit ebenso wie diese Bestimmung (vgl. RV 128 BlgNR 22. GP, 17 f.) an der entsprechenden Begriffsbestimmung des Art. 2 lit. d der Richtlinie 2002/58/EG über die Verarbeitung personenbezogener

Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. Nr. L 201 vom 12. Juli 2002 S. 37.

Bei der Durchführung von Kontrollmaßnahmen ist darauf Bedacht zu nehmen, dass davon nicht mehr Bedienstete erfasst werden, als es zur Verfolgung einer der Zwecke des Abs. 2 erforderlich ist. Abs. 4 definiert den Kreis der von Kontrollmaßnahmen potentiell betroffenen Bediensteten unter zwei Gesichtspunkten: Zum einen soll dieser Kreis nicht zu klein sein, um die Anonymität der Bediensteten nicht zu gefährden. Zum anderen soll er aber auch nicht so umfangreich sein, dass eine zu große Zahl an Bediensteten, die mit jenen IKT-Nutzungen, auf Grund derer ein Kontrollverfahren eingeleitet wird, nichts zu tun haben, Adressat einer Kontrollmaßnahme wird. Der Entwurf legt daher als Minimum des zu kontrollierenden Personenkreises fünf Bedienstete fest. Nur wenn eine Organisationseinheit diese Anzahl an Bediensteten unterschreitet, dürfen die Bediensteten der nächstgrößeren Organisationseinheit in die Kontrollmaßnahme miteinbezogen werden. Ausnahmsweise darf jedoch auch ein kleinerer Bedienstetenkreis kontrolliert werden, nämlich dann, wenn eine bestimmte Anwendung oder ein bestimmtes Programm, das von einer Kontrollmaßnahme erfasst werden soll, selbst bei Ausdehnung der Kontrollmaßnahme auf die übergeordneten Organisationseinheiten weniger als fünf Bediensteten zur Verfügung steht.

Abs. 5 nimmt schließlich darauf Bedacht, dass es gesetzliche Regelungen gibt, die die Überprüfung des Datenzugriffs von Beamten normieren (vgl. z.B. § 14 Abs. 2 Z 7 DSG 2000). Mit dieser Bestimmung wird klargestellt, dass derartige Regelungen vom gegenständlichen Gesetzesentwurf unberührt bleiben und somit die Protokollierung der Zugriffe von Bediensteten etwa auf Kundendaten oder die generalpräventive auswertende Kontrolle der Protokolle zum Zweck der Feststellung und künftigen Unterbindung unzulässiger Zugriffe zur Verwirklichung der Datensicherheit im Rahmen dieser Bestimmungen möglich bzw. geboten ist. § 79e Abs. 5 erstreckt sich auch auf die §§ 79f und 79g.

Zu § 79f BDG 1979:

Durch die IKT-Nutzung kann es nicht nur zu einer Gefahr eines Schadens für die IKT-Infrastruktur kommen (zB Datenverluste, kompletter Ausfall durch Überlastung u.a.), sondern auch zu einem Fehlverhalten der IKT-Infrastruktur. Bei einer Infektion durch Schadsoftware kann es durchaus sein, dass die IKT noch reibungslos funktioniert, jedoch Informationen an Dritte übermittelt (zB durch Trojaner, die Passwort-Eingaben aufzeichnen und versenden) oder E-Mails mit problematischem Inhalt aus dem Netzwerk nach außen verschickt werden. Ebenso kann die Bedienung der IKT-Geräte durch eine große CPU-Belastung wesentlich verlangsamt werden. IKT-Nutzungen im Sinne des § 79f Abs. 1 BDG 1979 müssen nicht notwendigerweise gleichzeitig auch Dienstpflichtverletzungen darstellen. Zu Beginn der stufenweisen Kontrollverdichtung soll bei einer Gefahr eines Schadens für die IKT-Infrastruktur oder einer Gefahr für die Gewährleistung ihrer korrekten Funktionsfähigkeit eine anonymisierte Auswertung über Art und Dauer der IKT-Nutzungen erfolgen. Damit wird garantiert, dass diesfalls keine personenbezogenen Daten aus dem Einflussbereich des zuständigen Systemadministrators übermittelt werden. Das Verfahren nach § 79f BDG 1979 wird somit von der IT-Stelle initiiert, woraufhin der Leiter oder die Leiterin der für die betroffene Organisationseinheit zuständigen Dienststelle die Bediensteten dieser Organisationseinheit über die Information der IT-Stelle in Kenntnis zu setzen, auf die Beseitigung der Gefahr hinzuwirken und die Bediensteten über die Möglichkeit einer namentlichen Ausforschung bei Fortbestehen der Gefahr innerhalb eines vierwöchigen Beobachtungszeitraumes nachweislich zu informieren hat. Der Beobachtungszeitraum darf in begründeten Ausnahmefällen die Dauer von vier Wochen überschreiten (Abs. 3). Ein begründeter Ausnahmefall wird dann vorliegen, wenn technische Probleme nur zu gewissen – beispielsweise monatlichen – Stichtagen auftreten oder in einer Organisationseinheit, in der sich Bedienstete längere Zeit auf Urlaub oder im Krankenstand befinden. Die Dauer für eine Verlängerung muss sich daher immer aus einem sachlichen Grund heraus rechtfertigen lassen, der eine auf maximal vier Wochen beschränkte Kontrolle als nicht zielführend erscheinen lässt. Die nachweisliche Information der Bediensteten ist ein wesentliches Element der stufenweisen Kontrollverdichtung, um die Verhältnismäßigkeit von Maßnahmen, die der Abwehr von Schäden an der IKT-Infrastruktur und der Gewährleistung ihrer korrekten Funktionsfähigkeit dienen, zu sichern. Die personenbezogene Übermittlung bei Fortbestand der Gefahr darf daher erst dann erfolgen, wenn der Dienststellenleiter oder die Dienststellenleiterin den zuständigen Systemadministrator von der erfolgten Information gemäß Abs. 2 unterrichtet hat und nach diesem Zeitpunkt die Gefahr weiterbesteht. Liegt hingegen eine konkrete unmittelbare Gefährdung für die IKT-Infrastruktur oder ihre korrekte Funktionsfähigkeit vor (Abs. 5), ist ein sofortiger Zugriff auf personenbezogene Daten gerechtfertigt, soweit dies zur Behebung dieser Gefährdung unbedingt notwendig ist. Über einen derartigen Zugriff ist ein Protokoll zu führen, das auf ein entsprechendes Verlangen dem oder der Bediensteten zur Verfügung zu stellen ist.

Zu § 79g BDG 1979:

Liegt ein begründeter Verdacht einer gröblichen Dienstpflichtverletzung vor, so können zwecks Verhinderung allfälliger weiterer Dienstpflichtverletzungen und/oder zur Klarstellung des Sachverhaltes in einem ersten Schritt wiederum anonymisierte Auswertungen über Auftrag des Dienststellenleiters oder der Dienststellenleiterin erfolgen. Sollen ausschließlich weitere Dienstpflichtverletzungen verhindert werden, ist dabei jedoch – § 79e Abs. 2 Z 2 lit. a entsprechend – vorher zu überprüfen, ob es möglich ist, diese durch zeitliche, inhaltliche oder quantitative Beschränkungen der IKT-Nutzung hintanzuhalten.

Der Verdacht muss von der Dienststelle ausgehen, die IT-Stelle kann das Verfahren nicht initiieren. Der anonymisierte Bericht der IT-Stelle im Umfang des Ermittlungsauftrages (Abs. 2) kann auch eine Leermeldung sein. Die Information der Bediensteten nach Abs. 3 erster Satzteil hat aber in jedem Fall (auch im Fall einer Leermeldung) zu erfolgen. In den Anwendungsfällen des § 79g ist die IT-Stelle vom Zeitpunkt der Information gemäß Abs. 3 Z 2 zu verständigen. Für die Festsetzung eines längeren als vierwöchigen Beobachtungszeitraumes gilt das zu § 79f Abs. 3 Ausgeführte (Abs. 4). Besteht innerhalb einer Beobachtungsfrist ein Verdachtsfall im Sinne des Abs. 3 Z 2 (weiter), so sind dem Leiter oder der Leiterin der Dienststelle auf dessen oder deren Verlangen (Abs. 5) die Daten über die IKT-Nutzungen personenbezogen zur Kenntnis zu bringen. Der oder die ausgeforschte Bedienstete muss nicht der- oder diejenige sein, der oder die den ursprünglichen Verdachtsfall gesetzt hat. Das ist deshalb gerechtfertigt, weil dieser Maßnahme eine allgemeine Information im Sinne der Ankündigung eines Beobachtungszeitraumes vorangeht. Nach Ablauf des Beobachtungszeitraumes auftretende Verdachtsfälle lösen jeweils ein neues Verfahren aus. Der betroffene Beamte oder die betroffene Beamtin ist über die namentliche Auswertung der IKT-Nutzungen im Umfang des Verlangens nach Abs. 5 umgehend zu informieren (Abs. 6). Liegt hingegen ein begründeter Verdacht gegen eine bestimmte Person wegen eines konkreten Vorfalls vor, muss das Verfahren einer stufenweisen Kontrollverdichtung nicht eingehalten werden, sondern ist, da hier jedenfalls die Klärung des Sachverhaltes erforderlich ist, unter Einhaltung der Verfahrensschritte des Abs. 7 der sofortige Zugriff auf die Daten der betreffenden Person zulässig. Auch in diesem Fall ist der betroffene Beamte oder die betroffene Beamtin über den erfolgten Datenzugriff und sein Ergebnis zu informieren.

Zu § 79h BDG 1979:

In jenen Fällen, in denen ein Benutzer oder eine Benutzerin um Serviceleistungen im Zusammenhang mit der IKT-Nutzung ersucht, handelt es sich nicht um Kontrollmaßnahmen gemäß den §§ 79e bis 79g. Unter Serviceleistungen sind insbesondere die Hilfestellung durch die IT-Stelle bei der Wiederherstellung von Dokumenten oder die Überprüfung von technischen Abläufen, die zur Verhinderung des Empfanges eines E-Mails (etwa wegen Spam-Verdachtes oder Virenbefalles) geführt haben, zu verstehen. Mit Ersuchen ist eine datenschutzrechtliche Zustimmung im Sinne des § 4 Z 14 DSG 2000 gemeint.

Zu § 79i BDG 1979:

Da im Bereich des Parlaments in der EDV-Verwaltung keine Trennung zwischen Bundesbediensteten und Abgeordneten und deren Mitarbeitern und Mitarbeiterinnen gemäß Klubfinanzierungsgesetz 1985 und Parlamentsmitarbeitergesetz vorhanden ist, könnte eine Kontrollmaßnahme gegenüber Beamten und Beamtinnen sowie Vertragsbediensteten der Parlamentsdirektion zu einer ungewollten Kontrolle der den Abgeordneten und deren Mitarbeitern und Mitarbeiterinnen zur Verfügung stehenden IKT-Infrastruktur führen. Um dieses Problem hintanzuhalten, sind die Bediensteten der Parlamentsdirektion von den Bestimmungen betreffend die Kontrolle der IKT-Nutzung ausgenommen. Gelten sollen für sie jedoch die Begriffsbestimmungen des § 79c, die in § 79d festgelegten Nutzungsgrundsätze sowie der dem früheren § 79c entsprechende § 79e Abs. 1, sodass insofern die bisherige Rechtslage für die Parlamentsbediensteten weiter gilt. Ebenso soll § 79h für Parlamentsbedienstete anwendbar sein; damit wird klargestellt, dass Serviceleistungen im Zusammenhang mit der IKT-Nutzung auch für Parlamentsbedienstete nicht unter den Begriff „Kontrollmaßnahme“ fallen.

Zu § 140 Abs. 3 und Anlage 1 Z 1.3.8 BDG 1979:

Organisatorische Änderungen im Verfassungsgerichtshof machen eine Anpassung der taxativ aufgelisteten Richtverwendungen sowie der Verwendungsbezeichnungen erforderlich.

Zu § 206 erster Satz RStDG:

Die Bestimmungen des BDG 1979 sind trotz der Zusammenfassung des Dienstrechtes von Richtern und Staatsanwälten im Richter- und Staatsanwaltschaftsdienstgesetz teilweise noch auf Staatsanwälte anwendbar. Die Neufassung des ersten Satzes bezweckt, dass Staatsanwälte vom Anwendungsbereich der Bestimmungen des 5a. Unterabschnittes des 6. Abschnittes des BDG 1979 über die IKT-Nutzung und Kontrollmaßnahmen nicht erfasst sind.

Zu Art. 4 (§§ 9 Abs. 2, 9 Abs. 3 und 14 Abs. 3 letzter Satz PVG):

Zu § 9 Abs. 2 PVG:

Als Pendant zu den dienstrechtlichen Vorschriften betreffend die Kontrolle der IKT-Nutzung der Bundesbediensteten enthalten die neuen Bestimmungen in lit. n und o Regelungen über die Mitwirkung der Organe der Personalvertretung bei derartigen Kontrollmaßnahmen. Sowohl bei der Durchführung einer Kontrollmaßnahme bei einem begründeten Verdacht einer gröblichen Dienstpflichtverletzung gemäß § 79e Abs. 2 Z 2 BDG 1979 als auch bei der Festsetzung eines längeren Beobachtungszeitraumes zur Durchführung einer Kontrollmaßnahme (§§ 79f Abs. 3 und 79g Abs. 4 BDG 1979) ist das Einvernehmen mit dem jeweils zuständigen Organ der Personalvertretung herzustellen. Im Fall einer Kontrollmaßnahme auf Grund des Verdachtes einer gröblichen Dienstpflichtverletzung ist die Personalvertretung somit sowohl hinsichtlich der beabsichtigten Durchführung einer Kontrollmaßnahme als auch im Hinblick auf ihr Ergebnis (§ 79g Abs. 7 letzter Satz BDG 1979) in das Verfahren eingebunden. Da gemäß § 79e Abs. 5 BDG 1979 in anderen Bundesgesetzen enthaltene Regelungen über die Zulässigkeit der Überprüfung der ordnungsgemäßen Verwendung von Daten von den Kontrollvorschriften des BDG 1979 unberührt bleiben, bezieht sich auch das Mitwirkungsrecht der Personalvertretung nicht auf diese Vorschriften.

Zu § 9 Abs. 3 PVG:

In den Anwendungsfällen des § 79g BDG 1979 ist zusätzlich zur IT-Stelle das zuständige Organ der Personalvertretung vom Zeitpunkt der Information gemäß § 79g Abs. 3 Z 2 BDG 1979 zu verständigen. Neben dem betroffenen Beamten oder der betroffenen Beamtin (§ 79g Abs. 6 BDG 1979) ist auch das zuständige Organ der Personalvertretung über die namentliche Auswertung der IKT-Nutzungen im Umfang des Verlangens nach § 79g Abs. 5 BDG 1979 zu informieren. Auch bei einer auf eine bestimmte Person abzielenden Kontrollmaßnahme gemäß § 79g Abs. 7 BDG 1979 ist das zuständige Organ der Personalvertretung über den erfolgten Datenzugriff und sein Ergebnis zu informieren.

Zu § 14 Abs. 3 letzter Satz PVG:

Die bisherige Verordnungsermächtigung entfällt, da sie aufgrund der umfassenden gesetzlichen Regelungen über die Kontrolle der IKT-Nutzung in den dienstrechtlichen Bestimmungen entbehrlich ist.