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 die 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.

Auswirkungen auf die Beschäftigung und den Wirtschaftsstandort Österreich:

Nicht nur denkbar, sondern auch erwünscht ist, dass der vorliegende Entwurf Beispielcharakter sowohl im öffentlichen als auch im privaten Bereich entwickelt und somit zumindest indirekt die Unternehmenskultur in Österreich positiv beeinflusst.

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 die 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 im PVG 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

1. hinsichtlich der Art. 1 bis 4 (BDG 1979, VBG, RStDG, PVG) aus Art. 10 Abs. 1 Z 16 B-VG,

2. hinsichtlich des Art. 5 (LDG 1984) aus Art. 14 Abs. 2 B-VG und

3. hinsichtlich des Art. 6 (LLDG 1985) aus Art. 14a Abs. 2 B-VG.

II. Besonderer Teil

Zu Art. 1, Art. 2, Art. 3, Art. 5, Art. 6 (§§ 79c bis 79f BDG 1979, § 29n VBG, § 206 erster Satz RStDG, § 113c LDG 1984, § 119f LLDG 1985):

Zu § 79c BDG 1979:

Die Datenverwendung in anderen als den in Abs. 2 genannten Fällen bzw. unter Nichteinhaltung der Vorschriften der §§ 79d und 79e – 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 §§ 79c Abs. 2 bis 4 und 79d bis 79e 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).

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 Inhalte übertragener Nachrichten nur dann kontrolliert werden, wenn dies zur Erreichung dieser Zwecke unbedingt notwendig ist. Selbst für diesen Fall wird im § 79d 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 § 79g Z 5 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.

Zu § 79d 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 § 79d 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 § 79d 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 belehren hat. Die nachweisliche Belehrung 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 Belehrung 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 § 79e 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 – § 79c Abs. 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 § 79e ist zusätzlich zur IT-Stelle auch das zuständige Organ der Personalvertretung vom Zeitpunkt der Belehrung gemäß Abs. 3 zu verständigen. 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 Belehrung im Sinne der Ankündigung eines Beobachtungszeitraumes vorangeht. Nach Ablauf des Beobachtungszeitraumes auftretende Verdachtsfälle lösen jeweils ein neues Verfahren aus. Neben dem betroffenen Beamten ist auch das zuständige Organ der Personalvertretung über die namentliche Auswertung der IKT-Nutzungen im Umfang des Verlangens nach Abs. 5 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 zusätzlich das zuständige Organ der Personalvertretung über den erfolgten Datenzugriff und sein Ergebnis zu informieren.

Zu § 79f 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 §§ 79c bis 79e. Mit Ersuchen ist eine datenschutzrechtliche Zustimmung im Sinne des § 4 Z 14 DSG 2000 gemeint.

Zu § 206 erster Satz RStDG:

Die Bestimmungen des BDG 1979 über die Kontrolle der IKT-Nutzung sollen nicht für Organe der Gerichtsbarkeit und damit auch nicht für Staatsanwälte gelten.

Zu Art. 4 (§§ 9 Abs. 2, 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 § 79c Abs. 2 Z 2 BDG 1979 als auch bei der Festsetzung eines längeren Beobachtungszeitraumes zur Durchführung einer Kontrollmaßnahme (§§ 79d Abs. 3 und 79e 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 (§ 79e Abs. 7 letzter Satz BDG 1979)in das Verfahren eingebunden.

Zu § 14 Abs. 3 letzter Satz PVG:

Diese Bestimmung enthält jene Verordnungsermächtigung, die die Grundlage für bundeseinheitliche Richtlinien betreffend die private Nutzung der IKT-Infrastruktur des Bundes durch die Bundesbediensteten bildet. Die bisherige Verordnungsermächtigung entfällt, da sie aufgrund der umfassenden gesetzlichen Regelungen über die Kontrolle der IKT-Nutzung in den dienstrechtlichen Bestimmungen dieser Novelle entbehrlich ist.