Auszug aus dem Protokoll des Stadtrates von Zürich

vom

11.04.2012

458.
Neuerlass Reglement über die Nutzung elektronischer Infrastruktur oder Dienste der Stadt Zürich (REID), Vernehmlassungsvorlage

IDG-Status: öffentlich

1. Zweck der Vorlage

Diese Vorlage regelt die Nutzung elektronischer Infrastrukturen oder Dienste der Stadt Zürich. Sie ersetzt das bisherige, weniger weit gehende «Reglement über die Nutzung und Überwachung von Internet und E-Mail» (StRB Nr. 765/2009; AS 236.300). Der Zweck der Reglementierung bleibe aber derselbe: Die Nutzenden der elektronischen Infrastrukturen oder Dienste der Stadt Zürich sollen künftig in einem Reglement (Beilage) umfassend über ihre Rechte und Pflichten, aber auch über allfällige Sanktionen bei Widerhandlungen informiert werden. Die Vorlage schafft darüber hinaus auch eine gesetzliche Grundlage für das Bearbeiten bestimmter Personendaten durch die Stadt Zürich.

2. Ausgangslage, Gründe für Neuregelung

Per 1. Juli 2009 hat der Stadtrat das «Reglement über die Nutzung und Überwachung von Internet und E-Mail» (StRB Nr. 765/2009; AS 236.300, nachfolgend «Internet- und E-Mail-Reglement») in Kraft gesetzt. Dieses Reglement beschränkte sich bewusst auf Internet- und E-Mail, obwohl man sich bereits zum damaligen Zeitpunkt bewusst war, dass auch die Telefonie entsprechend zu reglementieren sein wird, sobald sie über das Züri-Netz bzw. das Internet abgewickelt werden wird. Da damals die konkrete Telefonietechnologie für die Stadtverwaltung noch nicht bekannt war, sich aber eine Regelung von Internet und E-Mail aufdrängte, beschränkte man sich zunächst auf diese beiden Themen (Art. 1 Abs. 3 Internet- und E-Mail-Reglement).

Nachdem die Internettelefonie in der Stadtverwaltung weitgehend umgesetzt worden war, prüfte der Datenschutzbeauftragte das Bestehen eines allfälligen Handlungs- und Regelungsbedarfs im Bereich der Telefonie und stellte fest, dass es an klaren und verbindlichen Spielregeln und vor allem auch an Transparenz für die Nutzung weitgehend fehlt. Anfragen von Mitarbeitenden der Stadtverwaltung bei der Datenschutzstelle zur neuen Internettelefonie, insbesondere zur Aufzeichnung und Löschung von Telefongesprächen, bestätigten diese Feststellungen. Der Datenschutzbeauftragte initialisierte aus diesem Grund Anfang 2010 die Einsetzung einer Arbeitsgruppe, in welcher wie schon bei der Ausarbeitung des Internet- und E-Mail-Reglements wiederum das Departementssekretariat des Finanzdepartements, Human Resources Management (HRZ) und Organisation und Informatik der Stadt Zürich (OIZ) vertreten waren. Angesichts der technologischen Entwicklung kam die Arbeitsgruppe zum Schluss, dass eine (zusätzliche) Reglementierung der Telefonie im Rahmen des bestehenden Internet- und E-Mail-Reglements den sich stellenden Fragen bei der Nutzung der elektronischen Infrastrukturen oder Dienste nicht ausreichend Rechnung zu tragen vermag (vgl. zum Ganzen auch Tätigkeitsbericht 2010 der städtischen Datenschutzstelle, S. 6f.). Die Arbeitsgruppe entschied sich deshalb, eine allgemeine Reglementierung der Benutzung der elektronischen Infrastrukturen oder Dienste der Stadt Zürich auszuarbeiten.

Der vorliegende Entwurf basiert nicht nur auf einer Überarbeitung des Internet- und E-Mail-Reglements, sondern lehnt sich teilweise auch an die Änderungen des am 1. April 2012 in Kraft tretenden eidgenössischen Regierungs- und Verwaltungsorganisationsgesetzes vom 30. September 2010 (nachfolgend: E-RVOG) an, welcher den Datenschutz bei der Benut-

zung der elektronischen Infrastrukturen der Bundesverwaltung regelt. Das bisherige Internet- und E-Mail-Reglement soll entsprechend durch ein «Reglement der Benutzung der elektronischen Infrastrukturen oder Dienste der Stadt Zürich» (nachfolgend «REID» genannt) ersetzt werden. Art. 55 Abs. 2 AB PR umschreibt den besonderen Tatbestand der missbräuchlichen privaten Nutzung von technischen Einrichtungen und verweist auf das Internet- und E-Mail-Reglement. Materiell enthält das neue Reglement umfassendere Regelungen, so dass Art. 55 Abs. 2 aufgehoben werden kann.

Die Zuständigkeit für den Neuerlass des vorliegenden REID liegt gemäss Art. 49 und 113 Gemeindeordnung der Stadt Zürich vom 26. April 1970 und Art. 87 Abs. 1 des Personalrechts vom 6. Februar 2002 beim Stadtrat.

3. Unterschiede zum bisherigen Recht

Wie bereits erwähnt, findet eine Erweiterung des Internet- und E-Mail-Reglements auf alle elektronischen Infrastrukturen oder Dienste statt (vgl. zur beispielhaften Konkretisierung dieser Begriffe Art. 1 Abs. 2 REID).

Inhaltlich werden die bisherigen Regelungen in Bezug auf Nutzung und Überwachung grundsätzlich beibehalten und übernommen. Nicht mehr im Reglement geregelt werden einzig die Verpflichtung zur Aktivierung des Abwesenheitsassistenten bei länger dauernden Abwesenheiten (Art. 5 Abs. 1 Internet- und E-Mail-Reglement; vgl. zur Begründung unter Art. 9) sowie die abschliessende Aufzählung der einzelnen protokollierten Verkehrsdaten (Art. 7 Abs. 1 Internet- und E-Mail-Reglement). Auf letztere Bestimmung musste aufgrund des umfassenden Regelungsbereichs verzichtet werden, welcher eine abschliessende Aufzählung unmöglich macht. Der Grundsatz der Vermeidung des Personenbezugs bei der Datenbearbeitung wird bereits in § 11 des Gesetzes über die Information und den Datenschutz (IDG) statuiert, welcher ganz grundsätzlich festhält, dass öffentliche Organe Datenbearbeitungssysteme und -programme so zu gestalten haben, dass möglichst wenig Personendaten anfallen, die zur Aufgabenerfüllung nicht notwendig sind.

Neu geregelt werden im Reglement auch die Kosten, insbesondere die Kostenüberwälzung auf die Mitarbeitenden bei übermässiger oder missbräuchlicher Nutzung der elektronischen Infrastrukturen oder Dienste; bisher waren die Gebühren für private Telefongespräche des städtischen Personals im StRB Nr. 263 vom 26. Februar 2003 geregelt. Diese Regelung ist angesichts der technologischen Entwicklung überholt und bedurfte insofern einer Überarbeitung, welche nun im Rahmen des REID vorgenommen worden ist.

4. Erläuterungen zu den einzelnen Artikeln

Gegenstand des vorliegenden Reglements sind Datenbearbeitungen durch die Stadt Zürich als Eigentümerin und Verantwortliche der elektronischen Infrastrukturen und Dienste. Im Wesentlichen geht es dabei um Aufzeichnung und Auswertung von so genannten Verkehrsdaten, somit um Daten, die zwar einen Personenbezug aufweisen, nicht aber als besondere Personendaten i.S.v. § 3 IDG zu qualifizieren sind. Mit diesem Reglement werden der Stadt Zürich als Eigentümerin und Verantwortliche der elektronischen Infrastrukturen und Dienste keine neuen Kompetenzen hinsichtlich Datenbearbeitung erteilt, die sie nicht bereits aufgrund bestehender Rechtsgrundlagen hätte (Personalrecht, Gemeindeverordnung). Das Reglement schränkt im Gegenteil die zulässigen Datenbearbeitungen der Stadtverwaltung zugunsten derjenigen Personen, die die städtische Infrastruktur nutzen, ein. Aus diesen Gründen bedarf der Regelungsgegenstand des vorliegenden Reglements keiner formellgesetzlichen Grundlage; ein Erlass durch den Stadtrat genügt.

I. Allgemeine Bestimmungen

Art. 1 Geltungsbereich

Das vorliegende Reglement soll die Nutzung der elektronischen Infrastrukturen oder Dienste der Stadt Zürich regeln und gilt sowohl für stationäre als auch mobile Geräte. Unter das Reglement fallen alle Personen, welche die städtische Infrastruktur benutzen, unabhängig davon, ob sie zur Stadt in einem Dienstverhältnis (Angestellten- oder Behördenverhältnis) oder in einem Auftragsverhältnis stehen.

Es versteht sich von selbst, dass spezialgesetzliche oder höherrangige Bestimmungen der vorliegenden Regelung vorgehen. Auf eine entsprechende deklaratorische Bestimmung wie auf Bundesebene wird verzichtet (Art. 57i E-RVOG). Solche spezialgesetzlichen Bestimmungen, welche die Aufzeichnung und Auswertung von Personendaten nur unter strengen Voraussetzungen und in der Regel nur auf behördliche Anordnung hin zulassen, finden sich beispielsweise in folgenden Erlassen:

– Die Überwachung des Post- und Fernmeldeverkehrs im Zusammenhang mit einem Strafverfahren, einem Rechtshilfeverfahren oder zur Suche und Rettung einer vermissten Person nach BÜPF. Weiterhin möglich ist im Übrigen die Aufzeichnung von Gesprächen, sofern die Einwilligung der Gesprächsteilnehmerinnen und -teilnehmer vorliegt, z. B. im Zusammenhang mit der Qualitätsförderung in Kundenservice-Zentralen (Art. 55 Abs. 1 AB PR).

– Die Durchsuchung von Ton-, Bild- und anderen Aufzeichnungen, Datenträgern sowie Anlagen zur Verarbeitung und Speicherung von Informationen im Zusammenhang mit einem Strafverfahren gemäss Art. 246ff. StPO; für die Anordnung geheimer Überwachungen z. B. mit Video oder gestützt auf GPS-Peilsender sind die Art. 269ff. StPO massgebend.

– Besondere Regeln sieht ferner auch das Fernmeldegesetz vor, u. a. im Hinblick auf Standortdaten (vgl. Art. 43 bis 46 FMG).

Abs. 1: Der Geltungsbereich umfasst jede *Nutzung* der elektronischen Infrastrukturen oder Dienste der Stadt Zürich, die (mindestens teilweise) auch *dienstlich* sein muss (zu den Begriffen «elektronische Infrastrukturen» und «Dienste» siehe unten Abs. 2). Einzig die *rein private Nutzung* von Infrastrukturen oder Diensten, wie beispielsweise ein privates CMN-Abonnement, ist *nicht Gegenstand dieses Reglements*. Dies deshalb, weil sich in den Konstellationen der rein privaten Nutzung eine Regelung im Sinne des vorliegenden Reglements entweder erübrigt oder sich entsprechende Nutzungsbestimmungen nur im Rahmen des konkreten Vertragsabschlusses regeln lassen.

Der Geltungsbereich ist beschränkt auf elektronische Infrastrukturen oder Dienste, *bei deren Benutzung Personendaten anfallen* können. Nicht anwendbar ist das Reglement auf elektronische Infrastrukturen oder Dienste, bei denen keine Personendaten anfallen (wie beispielsweise Ticketautomaten oder elektronische Anzeigen im Tram).

Abs. 2: Der Begriff der elektronischen Infrastrukturen oder Dienste wird weit gefasst, wie die beispielhaften Aufzählungen in Abs. 2 zeigen. Dadurch soll der technische Fortschritt nicht zu einer ständigen Anpassung der gesetzlichen Grundlagen zwingen. Grundsätzlich sollen alle elektronischen Arbeits-, Hilfs- und Kontrollmittel erfasst werden, welche die Stadt Zürich ihren Angestellten, allenfalls aber auch Dritten, zur Verfügung stellen. Es kann sich dabei sowohl um stationäre als auch um mobile Geräte handeln.

Abs. 3: Die Bestimmung entspricht abgesehen von sprachlichen Anpassungen der Bestimmung von Art. 1 Abs. 2 Internet- und E-Mail-Reglement. Für Dritte, d. h. für Personen, die nicht dem städtischen Personalrecht unterstehen, soll das Reglement gelten, falls ihnen Inf-

rastrukturen oder Dienste der Stadt Zürich zu dienstlichen Zwecken zur Verfügung gestellt werden. In diesen Fällen ist ihnen das Reglement zu überbinden.

Art. 2 Zuständigkeitsvorschriften

Die Bestimmung ist Art. 24 AB PR nachempfunden. Der Dienstchefin oder dem Dienstchef werden im vorliegenden Reglement zahlreiche Aufgaben und Kompetenzen zugeordnet (Art. 6 Abs. 2, Art. 7 Abs. 2, Art. 8 Abs. 2 und Abs. 4, Art. 11 Abs. 2, Art. 12 bis 15). Diese Zuordnungen werden in Art. 2 auf weitere Stellen/Funktionen in der Stadtverwaltung ausgedehnt. Selbstverständlich können die zugewiesenen Aufgaben im Rahmen der städtischen Kompetenzordnung auch delegiert werden.

II. Allgemeine Nutzungsvorschriften

Die Nutzungsvorschriften werden neu in «Allgemeine» (II.) und «Spezifische» (III.) Nutzungsvorschriften gegliedert. Materiell werden neu auch die Kosten unter den (allgemeinen) Nutzungsvorschriften geregelt.

Art. 3 Private Nutzung

Der Grundsatz, dass die zur Verfügung gestellten elektronischen Infrastrukturen oder Dienste für den geschäftlichen Gebrauch und die Erfüllung dienstlicher Aufgaben bestimmt sind, ist eigentlich eine Selbstverständlichkeit und ergibt sich bereits aus Art. 1 (bisher Art. 3 Abs. 1 [1. Satz] Internet- und E-Mail-Reglement).

Art. 4 Meldepflicht

Diese Meldepflicht entspricht materiell Art. 3 Abs. 2 Internet- und E-Mail-Reglement (Marginale «Allgemeine Grundsätze»). Verzichtet wird jedoch auf eine Regelung, die vorschreibt, wem diese Meldung zu machen ist (bisher: Linienvorgesetzter oder Betreiberin Internet- und E-Mail-Dienst). Dieser Verzicht lässt sich dadurch rechtfertigen, dass die zuständige Stelle je nach Dienstabteilung variiert, diese aber den Mitarbeitenden in aller Regel bekannt ist (im Zweifel der unmittelbar Vorgesetzte).

Art. 5 Missbrauch

Entspricht weitgehend Art. 6 Internet- und E-Mail-Reglement.

Abs. 1: Abs. 1 zählt exemplarisch, d. h. nicht abschliessend, missbräuchliche Verwendungszwecke auf. Die exemplarische Aufzählung soll beibehalten bleiben, insbesondere auch deshalb, weil teilweise Nutzungen untersagt werden, welche bei einer rein privaten Nutzung an sich zulässig wären.

In lit. d wird dem Umstand Rechnung getragen, dass das Zugreifen auf Daten mit inkriminiertem Inhalt bei einzelnen Mitarbeitenden gerade auch der Erfüllung dienstlicher Aufgaben dienen kann, beispielsweise bei der Polizeiarbeit (für die Prüfung und den Entscheid diesbezüglicher Ausnahmeregelungen ist gemäss StRB Nr. 332/2002 die OIZ zuständig).

Abs. 2: Es versteht sich von selbst, dass es grundsätzlich im Interesse der Betreiberin der elektronischen Infrastrukturen oder eines Dienstes liegt, den Zugriff auf Webseiten mit pornografischen, sexistischen sowie weiteren widerrechtlichen Inhalten zu blockieren. Allerdings wird es nie möglich sein, sämtliche inkriminierten Seiten im Web zu blockieren. Aus diesem Grund nimmt Abs. 1 lit. d die einzelnen Benutzerinnen oder Benutzer persönlich in die Pflicht, den Zugriff auf inkriminierte Daten zu unterlassen; denn die Möglichkeit des Zugriffs rechtfertigt den Zugriff in diesen Fällen auch dann nicht, wenn die Betreiberin die Blockierung der inkriminierten Daten unterlassen hat. Die Blockierung von Webseiten mit inkriminiertem Inhalt an sich ist nicht Gegenstand dieses Reglements.

5. Kosten

Im vorliegenden Reglement werden neu auch die Kosten geregelt, indem verschiedene kostenintensive Nutzungen verboten werden bzw. einer Bewilligung durch die Dienstchefin oder den Dienstchef bedürfen (Art. 6) und die Überbindung der Kosten auf die Nutzenden geregelt wird (Art. 7). Die bisherige Regelung in StRB Nr. 263 vom 26. Februar 2003 trägt den neuen Entwicklungen im Kommunikationsbereich nicht mehr ausreichend Rechnung und soll mit dem vorliegenden Reglement aufgehoben werden (vgl. Art. 18).

Art. 6 Nutzungsbeschränkungen

Hohe Kosten zulasten der Stadt werden insbesondere durch den vermehrten Einsatz von mobilen Geräten (insbesondere Geschäftshandys) und die Nutzung neuartiger Dienste verursacht.

Abs. 1: Um insbesondere durch mobile Geräte verursachte Kostenexplosionen zu verhindern, werden verschiedene Nutzungen verboten, welche Zusatzkosten für die Stadt verursachen. Die Aufzählung ist nicht abschliessend. Grundsätzlich fallen darunter alle Nutzungen, welche in der Regel nicht dienstlicher Natur sind und/oder bei welchen Kosten anfallen, welche über den für «normale» Inlandgespräche üblichen Kosten liegen. Beispiele sind die Nutzung im und ins Ausland, Kontaktaufnahmen – telefonisch oder per SMS – mit gebühren- oder kostenpflichtigen Nummern (beispielsweise 090x), der Kauf und die Bezahlung von Waren und Dienstleistungen aller Art usw. Solche Nutzungen werden bereits an sich verboten; sie sind somit grundsätzlich und unabhängig vom Zweck der Nutzung (Zahlung von Billetten oder Abonnements, Teilnahme an Wettbewerben) verboten.

Die Nutzungsbeschränkungen sind nicht auf mobile Geräte beschränkt, sondern gelten auch für stationäre Geräte. Bei Verstoss gegen die Nutzungsbeschränkungen können dem Nutzenden die dadurch entstandenen Kosten überbunden werden (Art. 7).

Abs. 2: Sieht die Möglichkeit von Ausnahmen von Abs. 1 vor. Die Dienstchefin bzw. der Dienstchef (vgl. dazu Art. 2) kann gemäss Abs. 1 verbotene Nutzungen bewilligen, falls solche für die Erfüllung dienstlicher Aufgaben notwendig sind (beispielsweise die Nutzung mobiler Geräte im und/oder ins Ausland).

Art. 7 Kostenüberbindung

Im vorliegenden Reglement wird auf die Statuierung einer *Deklarationspflicht für Privatgespräche*, wie sie der Stadtrat mit StRB Nr. 263 vom 26. Februar 2003 eingeführt hat, verzichtet (StRB Nr. 263 wird entsprechend aufgehoben, vgl. Art. 18). Der Grund liegt darin, dass sich diese Deklarationspflicht in der Praxis nicht oder nur teilweise durchgesetzt hat. Zudem ist eine solche Deklarationspflicht technisch nur bei Festanschlüssen möglich und gerade nicht beim – kostenintensiven – Einsatz von mobilen Geräten. Anstelle einer Deklarationspflicht wird neu der Grundsatz statuiert, dass den Nutzenden die Kosten einer unerlaubten oder übermässigen Nutzung in Rechnung gestellt werden können (Abs. 1) und die Dienstchefin bzw. der Dienstchef für die Kontrolle der Abrechnungen verantwortlich ist (Abs. 2).

Abs. 1: Die Möglichkeit, Kosten den Nutzenden in Rechnung zu stellen, kann sich einerseits bei *übermässiger Nutzung* ergeben. Hierbei wird die übermässige private Nutzung im Vordergrund stehen. Art. 3 erklärt die private Nutzung als grundsätzlich zulässig, setzt dieser aber gleichzeitig auch Schranken. Kosten, die das Mass üblicher privater Nutzung überschreiten, sollen weiterverrechnet werden können. Andererseits sollen auch Kosten aus *unerlaubter Nutzung* in Rechnung gestellt werden können. Unerlaubt sind Nutzungen, die gegen die Nutzungsbeschränkungen (Art. 6) verstossen oder missbräuchlich sind (Art. 5).

Abs. 2: Für die Kontrolle der Abrechnung ist die Dienstchefin oder der Dienstchef verantwortlich. Die Aufgabe kann selbstverständlich innerhalb der Dienstabteilung delegiert werden. Unter die für die Kontrolle erforderlichen Informationen fallen die Verbindungsdaten und Ver-

bindungskosten. Aufgrund des allgemeinen Verhältnismässigkeitsgrundsatzes dürfen nur diejenigen Informationen bekannt gegeben werden, die für die vorzunehmenden Kontrollen geeignet und erforderlich sind.

III. Spezifische Nutzungsvorschriften

Art. 8 Zugriff auf personalisierte Ablagen

Abgesehen von der bisherigen Beschränkung auf E-Mail-Accounts und kleineren sprachlichen Änderungen entspricht diese Bestimmung Art. 4 Internet- und E-Mail-Reglement (Marginale «Zugriff auf persönliche E-Mail-Account»). Die Bestimmung wird neu ausgedehnt auf personalisierte Ablagen, d. h. auf alle Ablagen, auf welchen (mündliche oder schriftliche) Nachrichten für den Inhaber der Ablage hinterlassen werden können und welche nur dieser abrufen kann. Darunter fallen beispielsweise der persönliche E-Mail-Account sowie E-Mail-Ablagen und -Archive, aber auch das (üblicherweise private) Laufwerk «H» oder ein persönlicher Voice Recorder. Die Bestimmung ist nicht anwendbar auf allgemeine Info-Adressen oder Telefonbeantworter von Haupt- oder allgemeinen Anschlüssen.

Abs. 1: *Drittperson* im Sinne dieser Bestimmung ist jede Person, welche nicht mit derjenigen identisch ist, auf deren Namen eine bestimmte Ablage lautet. Drittperson ist insbesondere auch die Dienstchefin bzw. der Dienstchef. Aus der Bestimmung (insbesondere auch Abs. 2 und 3) ergibt sich, dass die Einwilligung für einen Zugriff ausdrücklich zu erfolgen hat. Eine Einwilligung setzt voraus, dass die betroffene Person umfassend informiert worden ist und weiss, wozu sie einwilligt. Eine Zustimmung ist zudem nur gültig, wenn sie freiwillig erfolgt ist, d. h., dass eine Einwilligung auch jederzeit widerrufen werden kann.

Abs. 2: Die Dienstchefin bzw. der Dienstchef kann sich von den Betreibern der elektronischen Infrastrukturen oder Dienste in Ausnahmefällen (z. B. Unfall, fristloser Entlassung usw.) selbst einen Zugriff einräumen lassen oder den Zugriff einer Drittperson gewähren. Voraussetzung ist, dass der Zugriff aus dienstlichen Gründen notwendig *und* die Einholung einer Einwilligung des Inhabers der personalisierten Ablage nicht zumutbar (z. B. im Fall einer fristlosen Kündigung oder bei unvorhergesehener längerer Abwesenheit infolge eines Unfalls) oder unmöglich (beispielsweise im Todesfall) ist. Diese zwei Voraussetzungen müssen *kumulativ* gegeben sein.

Der Zugriff ist zudem beschränkt auf die Zeit zwischen unvorhergesehenem Ereignis und Zeitpunkt der Kenntnisnahme einer längerdauernden Abwesenheit von der Arbeitsstelle bzw. des Austritts aus dem Anstellungsverhältnis. Aufgrund des Verhältnismässigkeitsgrundsatzes drängen sich Massnahmen auf, um diese Zeitspanne möglichst kurz zu halten. D. h., die Dienstchefin bzw. der Dienstchef hat bei Kenntnisnahme einer längerdauernden Abwesenheit oder der Beendigung des Arbeitsverhältnisses umgehend weitere Massnahmen zu treffen und zu veranlassen, wie beispielsweise die Einrichtung eines *Abwesenheitsassistenten* (mit Angabe der Stellvertreterregelung) oder das Sperren eines *E-Mail-Accounts* (vgl. dazu auch Abs. 4).

Der Grund für dieses Vorgehen liegt u. a. auch darin, dass immer auch die Persönlichkeitsrechte des Absenders zu berücksichtigen sind, welcher seine Nachricht an einen bestimmten Empfänger richtet. Ein Absender hat Anspruch auf die Information, dass der gewünschte Empfänger ein ihm zugestelltes E-Mail nicht mehr zur Kenntnis nehmen kann. Durch die Angabe eines Stellvertreters erhält der Absender einer Nachricht somit die Möglichkeit, seine Nachricht dem Stellvertreter zu schicken.

Mit der Mitteilungspflicht an den Betroffenen, die sowohl der anordnenden Dienstchefin/dem anordnenden Dienstchef als auch der ausführenden Stelle (Betreiber der jeweiligen elektronischen Infrastrukturen oder Dienste) auferlegt wird, soll missbräuchlichen Zugriffen entgegengewirkt und sichergestellt werden, dass die Betroffenen (nach ihrer Rückkehr an den Arbeitsplatz) sobald als möglich über allfällige Zugriffe unterrichtet werden.

Abs. 3 regelt klar, dass Nachrichten, welche als privat erkennbar sind, nicht eingesehen und bearbeitet werden dürfen. Die Bestimmung verpflichtet einerseits die Benutzenden, private Nachrichten möglichst als solche zu kennzeichnen oder diese zu löschen. Private E-Mails sind beispielsweise durch den Vermerk «privat» in der Betreffzeile und/oder Verschiebung in einen als «privat» bezeichneten Ordner zu kennzeichnen und/oder aus dem Account zu löschen. Ohne die Erkennbarkeit als «privat» nehmen die Benutzenden in Kauf, dass die E-Mails im persönlichen Account vom Arbeitgeber im Falle eines (berechtigten) Zugriffs (Abs. 2) eingesehen werden.

Abs. 4: Die Benutzenden haben beim Austritt ihre privaten Nachrichten zu löschen. Der Zugriff auf personalisierte Ablagen, insbesondere den persönlichen E-Mail-Account, endet mit dem Austritt aus der Stadtverwaltung. Keine Rolle spielt es, ob der Austritt freiwillig, geplant oder unvorhergesehen erfolgt.

Personalisierte Ablagen, insbesondere der persönliche E-Mail-Account, müssen sobald als möglich gesperrt bzw. definitiv gelöscht werden. Die entsprechende Deaktivierung personalisierter Ablagen hat die Dienstchefin bzw. der Dienstchef sicherzustellen.

Art. 9 E-Mail

Art. 9 Abs. 1 entspricht Art. 5 Abs. 2 Internet- und E-Mail-Reglement (Marginale «Abwesenheiten, Um- und Weiterleitungen»), welcher die automatische Um- oder Weiterleitung von E-Mails an E-Mail-Adressen ausserhalb des Stadtnetzes untersagt.

Art. 5 Abs. 1 des bisherigen Reglements wurden ersatzlos gestrichen. Dass bei länger dauernden Abwesenheiten der Abwesenheitsassistent aktiviert werden muss, dürfte den Mitarbeitenden in aller Regel bekannt sein, ist aber auch je nach Dienstabteilung anders geregelt. Auf eine allgemeine Regelung wie bisher soll daher verzichtet werden.

Art. 9 Abs. 2 entspricht Art. 3 Abs. 3 Internet- und E-Mail-Reglement (Marginale «Allgemeine Grundsätze»).

IV. Aufzeichnung und Auswertung von Verkehrsdaten

Bei Verkehrsdaten (auch «Randdaten» genannt), handelt es sich um systembedingte Bearbeitungen von Personendaten, welche bei der Nutzung von Infrastrukturen oder Diensten anfallen. § 11 IDG verlangt ausdrücklich, dass Datenbearbeitungssysteme und -programm so zu gestalten sind, dass möglichst wenig Personendaten anfallen, die zur Aufgabenerfüllung nicht notwendig sind (Abs. 1). Datenbearbeitungssysteme sind demnach so einzurichten, dass Personendaten erst gar nicht erhoben werden (sofern sie nicht zur Aufgabenerfüllung notwendig sind).

Die technische Prävention sowie die Sensibilisierung und Mitwirkung der Mitarbeitenden hat Vorrang gegengenüber der personenbezogenen Auswertung von Verkehrsdaten. Eine personenbezogene Auswertung kommt daher nur in Betracht, wenn ein Missbrauch durch (andere) präventive Schutzmassnahmen nicht verhindert werden kann und ist nur in den abschliessend geregelten Fällen zulässig.

Art. 10 Grundsatz

Die Bestimmung lehnt sich an Art. 57l und Art. 57m E-RVOG an, regelt allerdings nur die *Aufzeichnung von Verkehrsdaten* zu den aufgeführten Zwecken.

Eine Aufzeichnung und Auswertung von Verkehrsdaten zwecks Überprüfung von Arbeitszeiten von Mitarbeitenden ist nicht zulässig. Für diesen Zweck sollen ausschliesslich die diesbezüglichen Zeiterfassungssysteme zur Verfügung stehen.

Die Aufzählung in Abs. 1 lit. a bis f ist abschliessend.

Bei elektronischen Infrastrukturen oder Diensten dürfen Verkehrsdaten zu folgenden Zwecken aufgezeichnet werden: zur Sicherstellung der Systemsicherheit (vgl. zu personenbezogenen Auswertungen bei Störungen Art. 11), zu Wartungs- und Kontrollzwecken, zur Erfassung der Kosten (vgl. dazu Art. 7), zum Nachvollzug des Zugriffs auf Datensammlungen der Stadt Zürich (vgl. zu personenbezogenen Auswertungen bei Zugriffen auf Datensammlungen Art. 12) sowie zur Gewährleistung der Sicherheit von Gebäuden und Räumen bei Zutrittskontrollsystemen (beispielsweise durch den Einsatz von elektronischen Schlüsseln). Wird für die Zutrittskontrolle Videoüberwachung eingesetzt, sind zudem die Bestimmungen über die Videoüberwachung in der neuen Datenschutzverordnung (AS 236.100) zu beachten (Art. 9 bis 11 DSV).

Eine Aufzeichnung und Auswertung von Verkehrsdaten zwecks Überprüfung der Arbeitszeiten von Mitarbeitenden ist nicht zulässig. Für diesen Zweck sollen ausschliesslich die diesbezüglichen Zeiterfassungssysteme zur Verfügung stehen.

Abs. 2 entspricht dem bisherigen Art. 7 Abs. 2 Internet- und E-Mail-Reglement. Auf eine Aufzählung der protokollierten Daten gemäss bisherigem Art. 7 Abs. 1 soll aufgrund des über Internet und E-Mail hinausgehenden Geltungsbereichs künftig verzichtet werden. Die Verpflichtung gemäss § 11 IDG, wonach das öffentliche Organ Datenbearbeitungssysteme und -programme so zu gestalten hat, «dass möglichst wenig Personendaten anfallen, die zur Aufgabenerfüllung nicht notwendig sind», bezieht sich insbesondere auf die Protokollierung bzw. Erfassung von Verkehrsdaten.

Art. 3: Die Verkehrsdaten dürfen grundsätzlich nur ohne Personenbezug ausgewertet werden. Vorbehalten sind die personenbezogenen Auswertungen nach Art. 7 (zur Kostenüberbindung), Art. 11 (bei Störungen), Art. 12 (bei Zugriffen auf Datensammlungen), Art. 13 (bei Verdacht auf Missbrauch) und Art. 14 (bei strafbaren Handlungen).

Art. 11 Personenbezogene Auswertungen bei Störungen

Die Bestimmung entspricht Art. 10 Abs. 1 und 2 des Internet- und E-Mail-Reglements (Ausnahmetatbestände). Auch der bisherige Abs. 3 von Art. 10 des Internet- und E-Mail-Reglements wird materiell beibehalten, neu allerdings in zwei Bestimmungen (Art. 13 Abs. 6 und Art. 14) geregelt.

Abs. 1: Die protokollierten Verkehrsdaten dürfen bei Störungen ohne vorgängige Orientierung der Betroffenen personenbezogen ausgewertet werden. Eine solche Auswertung darf durch die jeweiligen Betreiber elektronischer Infrastrukturen oder Dienste aber nur durchgeführt werden, sofern die Gewährleistung der Systemsicherheit, der Funktionsfähigkeit oder der Verfügbarkeit von E-Mail und Internet unumgänglich ist, d.h., keinen Aufschub erlaubt. Vorausgesetzt sind somit eine *erhebliche Störung* sowie die *zeitliche Dringlichkeit*, welche eine vorgängige Orientierung nicht zulassen. Die personenbezogene Auswertung muss zudem für die Störungsbehebung *notwendig* sein.

Abs. 2: Die Orientierung der betroffenen Person(en) ist im Hinblick auf das künftige Verhalten bzw. die Vermeidung schwerer Störungen notwendig. Eine Orientierung der Dienstchefin oder des Dienstchefs, welche die namentliche Nennung allfälliger Störungsverursachenden beinhaltet, hat nur zu erfolgen, wenn ein Anhaltspunkt für eine erhebliche missbräuchliche Nutzung i.S.v. Art. 5 vorliegt.

Art. 12 Personenbezogene Auswertungen bei Zugriffen auf Datensammlungen

Gemäss § 7 Abs. 2 IDG müssen Informationsbearbeitungen einer Person zugerechnet werden können und Veränderungen von Informationen erkennbar und nachvollziehbar sein (lit. d und e). Diese Grundsätze gelten insbesondere für Zugriffe auf Datensammlungen der Stadt Zürich (beispielsweise Alpha, Polis).

Da Zugriffe auf Datensammlungen der Stadt Zürich häufig einem grossen Benutzerkreis eingeräumt werden müssen, ist sicherzustellen, dass keine missbräuchlichen Zugriffe und Nutzungen (insbesondere zu nicht dienstlichen Zwecken) erfolgen. Um zu überprüfen, dass Mitarbeitende nur auf die für die Erfüllung ihrer dienstlichen Aufgaben erforderlichen Informationen in Datenbanken zugreifen, kann zu Kontrollzwecken eine personenbezogene Auswertung der Zugriffe notwendig sein. Dadurch lässt sich überprüfen, ob nur rechtmässige Zugriffe auf Datensammlungen der Stadt Zürich erfolgen. Art. 12 sieht daher vor, dass die Zulässigkeit der Zugriffe auf Datensammlungen der Stadt Zürich auf Anordnung der Dienstchefin oder des Dienstchefs ausgewertet werden können. Die Auswertung kann sich dabei auf bestimmte Informationen oder ein bestimmtes Dossier beziehen (beispielsweise welche Mitarbeitenden haben in einer bestimmten Zeitspanne auf Informationen über Herrn X oder ein bestimmtes Dossier zugegriffen). Die Auswertung kann sich aber auch auf bestimmte Mitarbeitende beziehen (auf welche Informationen haben die Mitarbeitenden A bis C zugegriffen). Es versteht sich, dass dabei die Grundsätze des Personalrechts zu beachten sind, insbesondere das Gleichbehandlungsgebot der Mitarbeitenden sowie das Willkürverbot.

Art. 13 Personenbezogene Auswertungen bei Verdacht auf Missbrauch

Die Abs. 1 bis 5 entsprechen Art. 9 Internet- und E-Mail-Reglement (Personenbezogene Auswertungen), Abs. 6 entspricht Art. 10 Abs. 3 zweiter Spiegelstrich Internet- und E-Mail-Reglement (Ausnahmetatbestände).

Abs. 1 bis 5 setzen eine vorgängige Information der Betroffenen voraus, Abs. 6 lässt im Sinne einer Ausnahme eine personenbezogene Auswertung ohne vorgängige Information zu.

Abs. 1: Wesentliche Voraussetzung für die Anordnung einer personenbezogenen Auswertung muss das Vorliegen eines Verdachts auf missbräuchliche Benützung sein. Ein Verdacht liegt vor, wenn Anhaltspunkte für eine übermässige private (i.S.v. Art. 3 Abs. 1) oder missbräuchliche Nutzung gegeben sind, beispielsweise wenn eine Verwaltungsstelle wiederholt Probleme mit der Infrastruktur hat. Eine Auswertung darf zudem nur einem begrenzten Personenkreis gegenüber angeordnet werden. Angesichts des Grundsatzes der Verhältnismässigkeit hat sich die Anordnung somit – sowohl in personeller als auch in zeitlicher Hinsicht – auf das zur Missbrauchsbekämpfung Notwendige zu beschränken.

Gemäss Abs. 2 ist eine personenbezogene Auswertung erst nach vorgängiger schriftlicher Information der Benutzenden zulässig, d. h., es dürfen nur Verkehrsdaten ausgewertet werden, welche nach dem Zeitpunkt dieser Information angefallen sind (zu den Ausnahmen vgl. Abs. 6 und 7 sowie Art. 11, 12 und 14). Eine rückwirkende Überprüfung ist nicht zulässig.

Abs. 3: Grundlage für eine personenbezogene Auswertung ist eine klare Auftragserteilung der Dienstchefin oder des -chefs an die Betreiber der jeweiligen elektronischen Infrastrukturen oder Dienste. Die Dienstchefin oder der Dienstchef hat auch den Datenumfang festzulegen, insbesondere kann sie bzw. er die OIZ bzw. einen anderen Betreiber beauftragen, nur die Daten weiterzuleiten, welche Hinweise auf eine missbräuchliche Nutzung geben.

Mit Abs. 4 wird sichergestellt, dass die bereits vorgängig informierten betroffenen Personen abschliessend auch über das Resultat und die getroffenen Massnahmen informiert werden. Im Gegensatz zum bisherigen Reglement sind die Departementsvorstehenden nachträglich nicht mehr zu orientieren.

Abs. 5: Diese Bestimmung hat, gestützt auf das personal- und datenschutzrechtliche Einsichts- und Auskunftsrecht in bzw. über eigene Daten, rein deklaratorischen Charakter. Da der Benutzerkreis über das städtische Personal hinaus auch weitere Personen umfasst, sollen die Nutzenden dennoch ausdrücklich auf dieses Recht hingewiesen werden. Gleichzeitig werden damit auch die Vorgesetzten daran erinnert, dass Auswertungsdaten von den Mitarbeitenden eingesehen werden können und somit für eine gewisse Zeit zur Verfügung zu halten sind.

Abs. 6: In Einzelfällen, in denen ein erheblicher Verdacht auf Missbrauch i.S.v. Art. 5 besteht, sind personenbezogene Auswertungen auch ohne vorgängige Mitteilung zulässig. Die in Art. 5 erwähnten Missbrauchstatbestände sind nicht abschliessend, so dass sich unter den Voraussetzungen von Abs. 6 auch weitere Missbrauchstatbestände auswerten lassen. Vorausgesetzt ist, dass ein *erheblicher Verdacht* besteht, d. h., konkrete Anhaltspunkte für das Vorliegen eines Missbrauchs gegeben sind, und es sich um einen konkret abzuklärenden Einzelfall handelt. Beispielsweise soll die Identität eines Mitarbeitenden bei so genannten Zufallsfunden festgestellt werden können, wie etwa beim Vorfinden von pornografischen Bildern beim Drucker oder anlässlich einer versehentlichen Zustellung von E-Mails mit solchen Bildern oder anderen Inhalten gemäss Art. 5 Abs. 1. Die Auswertung ist in diesen Fällen auf die *Feststellung der Identität* der fehlbaren Person beschränkt; weitere Auswertungen dürfen nicht gemacht werden bzw. sind nur nach Abs. 1 bis 5 möglich. In den Fällen von Abs. 6 hat die Dienstchefin oder der Dienstchef den Auftrag zur Feststellung der Identität schriftlich an den jeweiligen Betreiber der elektronischen Infrastrukturen oder Dienste zu erteilen.

Art. 14 Personenbezogene Auswertungen bei strafbaren Handlungen

Entspricht Art. 10 Abs. 3 erster Spiegelstrich des Internet- und E-Mail-Reglements (Ausnahmetatbestände).

Auch falls strafbare Handlungen wahrgenommen werden oder erhebliche Verdachtsgründe für eine solche vorliegen, dürfen personenbezogene Auswertungen ohne vorgängige Orientierung erfolgen. Das Verfahren richtet sich in diesen Fällen nach dem Personalrecht, insbesondere nach AB PR 152.

V. Schlussbestimmungen

Art. 15 Informationspflicht

Art. 15 Abs. 1 und 2 entsprechen Art. 2 Internet- und E-Mail-Reglement, mit der Ausnahme, dass in Art. 15 Abs. 1 nun konkreter «die Dienstchefin oder der Dienstchef» verpflichtet wird anstelle der «Departemente und Dienstabteilungen». Diese Präzisierung wurde u. a. auch deshalb vorgenommen, damit die durch das Reglement ermächtigten und verpflichteten Stellen auch sprachlich jeweils gleich bezeichnet werden. Dadurch sollen die jeweiligen Zuständigkeiten und Kompetenzen klar geregelt werden. Vgl. dazu auch Art. 2.

Abs. 2 entspricht Art. 2 Abs. 2 des bisherigen Reglements. Die Mehrheit der Arbeitsgruppe ist für ersatzlose Streichung dieser Bestimmung, möchte sie aber dennoch in die Vernehmlassung geben.

Art. 16 Sanktionen

Entspricht Art. 11 Internet- und E-Mail-Reglement.

Art. 17 Ergänzende Nutzungsbestimmungen

Das vorliegende Reglement ist für die ganze Stadtverwaltung verbindlich. Angesichts der grossen Diversität der städtischen Verwaltungstätigkeiten müssen *ergänzende Nutzungsbestimmungen* möglich sein. Ergänzende Bestimmungen können im Bereich der allgemeinen (Titel II., Art. 3 bis 7) und spezifischen (IV., Art. 8 bis 9) Nutzungsvorschriften erlassen werden.

Wesentlich ist, dass nur ergänzende, d. h. zusätzliche Bestimmungen zu den allgemeinen und spezifischen Nutzungsvorschriften erlassen werden können, welche über den Mindeststandard dieses Reglements hinausgehen, *ohne von diesem zu Ungunsten der Benutzerinnen und Benutzer abzuweichen*.

Ausnahmen im Sinne von abweichenden Bestimmungen sind nur dort zulässig, wo sie im Reglement ausdrücklich vorgesehen sind. Dies ist bei folgenden Bestimmungen der Fall:

Art. 5 Abs. 1 lit. d (Missbrauch);

Art. 6 Abs. 2 (Nutzungsbeschränkungen). Für Ausnahmeregelungen ist hier zudem die Dienstchefin oder der Dienstchef zuständig;

Art. 9 Abs. 1 (Um- und Weiterleitung E-Mail).

Abs. 1: Denkbar ist, dass künftig neue Nutzungsmöglichkeiten zur Verfügung stehen, welche einer einheitlichen städtischen Nutzungsregelung bedürfen. Sofern das vorliegende Reglement keine ausreichende Regelung enthält, wird dem Finanzvorstand die Kompetenz eingeräumt, ergänzende Nutzungsvorschriften von gesamtstädtischer Tragweite zu erlassen. Dadurch soll auf neue Nutzungsmöglichkeiten möglichst rasch reagiert werden können.

Abs. 2 ermöglicht den Erlass ergänzender Nutzungsvorschriften durch die Departementsvorstehenden im jeweiligen Zuständigkeitsbereich. Die Bestimmung entspricht abgesehen von sprachlichen Änderungen und Präzisierungen Art. 12 Internet- und E-Mail-Reglement.

Art. 18 Aufhebung bisherigen Rechts

Aufzuheben sind neben dem Internet- und E-Mail-Reglement (StRB Nr. 765 vom 17. Juni 2009, AS 236.300) auch Teile des StRB Nr. 263 vom 26. Februar 2003 betreffend Weiterverrechnung der Gebühren für private Telefongespräche des städtischen Personals. Die Kostenregelung ist nun Teil des vorliegenden Reglements (vgl. dazu Art. 6 und Art. 7).

6. Vernehmlassung

Das Reglement wurde von der erwähnten Arbeitsgruppe erarbeitet. Die Vorlage ist vor ihrer definitiven Verabschiedung den Departementen (für sich und zuhanden der Dienstabteilungen), der Konferenz der Schulpräsidentinnen und Schulpräsidenten sowie i.S.v. Art. 74 Abs. 4 PR i.V.m. Art. 144 Abs. 1 lit. a AB PR den Personalverbänden zur Vernehmlassung zu unterbreiten.

Auf Antrag des Vorstehers des Finanzdepartements beschliesst der Stadtrat:

1. Das «Reglement über die Nutzung elektronischer Infrastruktur oder Dienste der Stadt Zürich» wird den Departementen (für sich und zuhanden ihrer Dienstabteilungen), der Konferenz der Schulpräsidentinnen und Schulpräsidenten sowie den Personalverbänden als Entwurf zur Vernehmlassung (Entwurf vom 11. April 2012) unterbreitet.
2. Mitteilung je unter Beilage an den Vorsteher des Finanzdepartements, die übrigen Mitglieder des Stadtrates, die Stadtschreiberin, den Rechtskonsulenten, den Datenschutzbeauftragten, Human Resources Management und Organisation und Informatik.

Für getreuen Auszug
die Stadtschreiberin