Schleswig-Holsteinischer Landtag

Stenographischer Dienst

N i e d e r s c h r i f t

Innen- und Rechtsausschuss

100. Sitzung

von Mittwoch, dem 21. April 2004, bis Donnerstag, den 22. April 2004,
in Bremen

Anwesende Abgeordnete

Monika Schwalm (CDU)	Vorsitzende
Gisela Böhrk (SPD)	
Ingrid Franzen (SPD)	
Klaus-Peter Puls (SPD)	
Thomas Rother (SPD)	
Thorsten Geißler (CDU)	
Peter Lehnert (CDU)	
Silke Hinrichsen (SSW)	

Die Liste der **weiteren Anwesenden** befindet sich in der Sitzungsakte.

Einziger Punkt der Tagesordnung:

Informationsreise des Innen- und Rechtsausschusses nach Bremen

Die Vorsitzende, Abg. Schwalm, eröffnet die auswärtige Sitzung des Ausschusses in Bremen am 21. April 2004 um 11:00 Uhr und stellt die Beschlussfähigkeit des Ausschusses fest. Die Tagesordnung wird in der vorstehenden Fassung gebilligt.

Einziger Punkt der Tagesordnung:

Informationsreise des Innen- und Rechtsausschusses nach Bremen

Der Ausschuss besucht am **Mittwoch, den 21. April 2004,** zunächst das Haus des Senators der Finanzen in Bremen. Frau Schwellach, Leiterin des Referates Neue Medien/E-Government beim Senator der Finanzen, und ihre Mitarbeiterin Frau Sommer informieren den Ausschuss über das Projekt E-Government in Bremen. Anhand einer PowerPoint-Vortrages erläutert Frau Schwellach die Grundlagen des Projektes, seine Finanzierung, seine Entwicklungsphase und die Einsatzmöglichkeiten in der bremischen Verwaltung. Frau Sommer stellt die rechtlichen Grundlagen für die Einführung des E-Government in Bremen dar und verweist in diesem Zusammenhang auf die Richtlinie für die Bereitstellung und Nutzung von Internet-/Intranetzugängen (Anlage 1 zu dieser Niederschrift) und die Richtlinie für die Nutzung der elektronischen Post (Anlage 2 zu dieser Niederschrift).

In der anschließenden Diskussion wird deutlich, dass das Angebot des elektronischen Zugangs und der elektronischen Dienstleistungen durch die Verwaltung in Bremen in erster Linie von gewerblichen Nutzern, Unternehmen, Rechtsanwaltskanzleien, Steuerberatern und ähnlichen genutzt wird, die Nachfrage der Bürgerinnen und Bürger in Bremen jedoch nach wie vor eher zurückhaltend ist.

Am Nachmittag besucht der Ausschuss die Hörfunkstudios von Radio Bremen und führt ein Gespräch mit dem Radio Bremen-Intendant, Dr. Heinz Glässgen, dem Nordwestradio-Programmleiter Jörg-Dieter Kogel und Herrn Michael Glöckner, Radio-Bremen-Sprecher und zuständig für die Presse- und Öffentlichkeitsarbeit des Senders, über die Zukunft von öffentlich-rechtlichen Rundfunksendern, die Erhöhung der Rundfunkgebühren und die für die Zukunft geplanten Projekte von Radio Bremen.

Am **Donnerstag, dem 22. April 2004**, lässt sich der Ausschuss durch den Direktor der Bremischen Bürgerschaft über den aktuellen Stand der Föderalismusreform und der Arbeit der Kommission von Bundestag und Bundesrat zur Modernisierung der bundesstaatlichen Ordnung informieren und diskutiert mit ihm über die Zukunft des Föderalismus in Deutschland.

Am Nachmittag stellt Dr. Stephan Klein, Geschäftsführer der bremen online services GmbH & Co. KG dem Ausschuss anhand praktischer Beispiele die Anwendung des E-Government in Bremen vor. Im Mittelpunkt steht dabei die von dem Unternehmen entwickelte Software Governikus, die Bremen für seine E-Government-Dienstleistungen einsetzt. Hieran schließt sich eine ausführliche Diskussion mit den Ausschussmitgliedern an.

Die Vorsitzende, Abg. Schwalm, schließt die Sitzung um 15:00 Uhr.

gez. Monika Schwalm	gez. Dörte Schönfelder
Vorsitzende	Geschäfts- und Protokollführerin

Anlage 1

H 1270
77

AMTSBLATT DER FREIEN HANSESTADT BREMEN

2004 | Ausgegeben am 10. Februar 2004 | Nr. 20

Inhalt

I.8 Richtlinie für die Bereitstellung und Nutzung von Internet/Intranet Zugängen

Vom 1. Februar 2004

Vorbemerkung

Die Internet-Technologien und das Internet sind eine wichtige Grundlage für die Erfüllung von Aufgaben der öffentlichen Verwaltung im Rahmen von E-Government. Die Einrichtung von Internet-Zugängen und die Bereitstellung von Internet- und Intranet-Angeboten der Bremischen Verwaltung ermöglicht den raschen Informationsaustausch zwischen den Behörden, den Bürgerinnen und Bürgern und erleichtert eine effiziente Erledigung der Verwaltungsaufgaben. Die Nutzung der Internet-Dienste soll unter anderem die Medienkompetenz der Mitarbeiterinnen und Mitarbeiter erhöhen (Prinzip: „Internet für Alle").

1. Gegenstand der Richtlinie

(1) Die Richtlinie regelt die Nutzung und Bereitstellung von Internet/Intranet-Zugängen und in diesem Zusammenhang das Abrufen und das Anbieten von Internetinhalten über das Bremische Verwaltungsnetz (BVN).

(2) Abrufen ist das Aufrufen und Einsehen von im Internet/Intranet vorhandenen Informationen.

Anbieten ist das Verbreiten von Inhalten über Internet/Intranet-Dienste.

(3) Die Richtlinie regelt

- die Aufgaben der Dienststellen im Zusammenhang mit der Bereitstellung von Internet- und Intranetzugängen und
- die Rechte und Pflichten der Nutzer und Nutzerinnen, auch im Hinblick auf den Schutz ihrer Privatsphäre.

2. Geltungsbereich

Diese Richtlinie gilt für alle Beschäftigten in Dienststellen, Eigenbetrieben und Einrichtungen des Landes sowie der Stadtgemeinde Bremen. Für privatrechtliche Gesellschaften mit einer Beteiligung der Freien Hansestadt Bremen, die per Vertrag[1] dem BVN beigetreten sind, gilt diese Richtlinie entsprechend.

Der Senator für Finanzen empfiehlt auch den privatrechtlichen Gesellschaften mit einer Beteiligung der FHB, die dem BVN nicht beigetreten sind, diese Richtlinie in ihrer Gesellschaft zur Anwendung zu bringen.

3. Zuständigkeiten

(1) Für das BVN und den zentral beim Provider eingerichteten Internetzugang der Freien Hansestadt Bremen ist der Senator für Finanzen zuständig. Der Betrieb wird durch einen Service-Provider gewährleistet. Der Service-Provider sichert das BVN und den Zugang (BVN - Internet) ab.

(2) Die Dienststellen sind für die Einrichtung des Internet/Intranet-Zugangs für alle PC-gestützten Arbeitsplätze zuständig. Sofern Arbeitsplätze für E-Government-Anwendungen vorgesehen sind, ist die vorherige Einrichtung eines Internet-Zugangs zwingend. Auch Mitarbeiterinnen und Mitarbeiter ohne PC-Arbeitsplatz soll ein Internet/Intranet-Zugang ermöglicht werden. Die Einrichtung erfolgt in Abstimmung mit der fachlich zuständigen Stelle in der Dienststelle und dem Provider des BVN.

(3) Die Dienststellen haben bei der Einrichtung der Internet/Intranet-Zugänge in ihrem Bereich folgendes sicherzustellen:

- Einrichtung der Internet/Intranet-Zugänge am Arbeitsplatz
- Gewährleistung von Datenschutz und Datensicherheit am Arbeitsplatz für den Zugriff auf das Internet/Intranet
- Installation von Programmen (gegebenenfalls aus dem Internet) durch administrierende Bereiche,
- Teilnahme der Mitarbeiter und Mitarbeiterinnen an Schulungen und Informationen über Sicherheitsrisiken und die geeigneten Maßnahmen zur Gewährleistung von Datenschutz und -sicherheit am Arbeitsplatz

1 Etwa durch den Muster-Beitrittsvertrag des Senators für Finanzen zur Nutzung von Infrastruktur und Dienstleistungen im Verwaltungsnetz der Freien Hansestadt Bremen (BVN)

- fachliche Betreuung der Mitarbeiter und Mitarbeiterinnen im Umgang mit den neuen Medien
- Einrichtung von Sicherheitssystemen, die zentral empfohlen werden
- Einrichtung von Virenscannern, insbesondere auch am Arbeitsplatz, die ständig aktualisiert werden und nicht durch Mitarbeiter oder Mitarbeiterinnen deaktiviert werden dürfen
- sofortige Ergreifung von Maßnahmen bei Erkennung von Sicherheitslücken
- ggf. Einrichtung und Betrieb eines Proxy- bzw. Terminal-Servers, ohne Protokollierung von Zugriffsaktivitäten auf das Internet/Intranet.

(4) Die Mitarbeiter und Mitarbeiterinnen haben im Rahmen ihrer Möglichkeiten sicherzustellen, dass eine Nutzung des Internets/Intranets vom Arbeitsplatz durch Unbefugte nicht möglich ist.

4. Unzulässige Nutzung, Verhaltensgrundsätze

(1) Unzulässig ist es, Inhalte über das Internet/ Intranet anzubieten oder abzurufen, die im Sinne des § 12 Abs. 1 MDStV

- gegen Bestimmungen des Strafgesetzbuches verstoßen
- den Krieg verherrlichen
- offensichtlich geeignet sind, Kinder oder Jugendliche sittlich schwer zu gefährden
- Menschen, die sterben oder schweren körperlichen oder seelischen Leiden ausgesetzt sind oder waren, in einer die Menschenwürde verletzenden Weise darstellen und ein tatsächliches Geschehen wiedergeben, ohne dass ein überwiegendes berechtigtes Interesse gerade an dieser Form der Berichterstattung vorliegt; eine Einwilligung ist unbeachtlich
- in sonstiger Weise die Menschenwürde verletzen.

(2) Unzulässig ist jede sonstige rechtswidrige Nutzung des Internet, insbesondere das Anbieten oder Abrufen von Inhalten unter Verstoß gegen das Urheberrecht.

(3) Unzulässig sind ferner folgende Nutzungen des Internets:

- Aufrufe kostenpflichtiger Seiten, die nicht durch die Dienststelle zugelassen sind
- Aktionen, die gegen die Dienstanweisung zum Verbot der sexuellen Diskriminierung und Gewalt am Arbeitsplatz vom 26. Mai 1993 (Brem. ABl. S.223) verstoßen
- das Down- oder Uploaden von Dateien, die durch ihr Volumen die Internet/Intranetnutzung anderer Mitarbeiter und Mitarbeiterinnen beeinträchtigen, wie z.B. Musik- oder Videodateien
- die Installation von Programmen aus dem Internet, die nicht durch schriftliche dienstliche Anweisung zugelassen ist
- Handlungen, die die Sicherheit von IT-Systemen innerhalb und außerhalb des BVN gefährden
- die Teilnahme an Internet-Chats
- das Pflegen von privaten oder kommerziellen Homepages
- Gebote bei elektronischen Versteigerungen
- elektronischer Handel (z.B. Aktien)
- die Nutzung von Anonymisierungsdiensten, um unzulässige Zugriffe im Sinne dieser Richtlinie auszuführen.

(4) Bei vorsätzlichem oder nachweislich wiederholtem Abrufen oder Anbieten von unzulässigen Inhalten im Sinne von Ziffer 4 (1) die eindeutig nicht in dienstlichem Zusammenhang stehen, hat die jeweilige Dienstelle die Strafverfolgungsbehörden einzuschalten.

(5) Bei vorsätzlichem oder nachweislich wiederholtem Abrufen oder Anbieten von unzulässigen Inhalten im Sinne von Ziffer 4 (1) bis Ziffer 4 (3), die eindeutig nicht in dienstlichem Zusammenhang stehen, kann die jeweilige Dienststelle disziplinarische oder arbeitsrechtliche Konsequenzen einleiten.

5. Nutzung des Internets am Arbeitsplatz

(1) Das Internet darf grundsätzlich nur für dienstliche Zwecke genutzt werden. Die private Nutzung ist eingeschränkt entsprechend Ziffer 6 zulässig. Sie fällt unter das Fernmeldegeheimnis. Die Versendung dienstlicher E-Mails an eigene private E-Mail-Postfächer ist untersagt.

(2) Abgerufene Inhalte dürfen nur gespeichert werden, wenn dies für dienstliche Belange erforderlich ist und nicht gegen Urheberrechte Dritter verstößt.

(3) Nicht mehr benötigte Inhalte sind zu löschen.

6. Private Nutzung des Internets am Arbeitsplatz

(1) Die private Nutzung des Internetzugangs ist immer den dienstlichen Belangen unterzuordnen.

Sie ist zulässig, sofern:

- täglich in der Summe 15 Minuten nicht überschritten werden

und

- eine ordnungsgemäße Erledigung der sonstigen Aufgaben der Bediensteten gewährleistet ist

und

- eine schriftliche Einverständniserklärung des Mitarbeiters oder der Mitarbeiterin bei der Dienststelle vorliegt, in welcher die Einsichtnahme in die durch die private Nutzung anfallenden Verbindungs- und Protokolldateien nach Ziffer 8 und Ziffer 9 dieser Richtlinie genehmigt wird (Anlage 1)

(2) Die private Nutzung kann im Einzelfall aus dienstlichen Gründen oder in anderen begründeten Fällen in Absprache mit dem örtlichen Personalrat untersagt werden.

(3) Die private Nutzung unterliegt weiteren Grundsätzen:

- Sie darf nur unter Einsatz eines Programms erfolgen, das es ermöglicht, zwischen privater und dienstlicher Nutzung zu differenzieren und zwi-

schen zwei Nutzungsmodi zu wechseln. Je nach Nutzungsmodus wird der Abruf von Inhalten über separate Proxy geleitet, die vom Provider des BVN betrieben werden. Bei der privaten Nutzung des Internets am Arbeitsplatz wird von der Nutzerin / dem Nutzer ein einheitlicher monatlicher Betrag gezahlt.

- Für die private Nutzung des Internets am Arbeitsplatz sind lediglich die Dienste http und https zugelassen.
- Die private Nutzung ist beschränkt auf das Abrufen von Inhalten. Das Anbieten von Inhalten ist nicht zulässig, weil das Land Bremen und nicht die jeweilige Privatperson Dritten als Quelle kenntlich gemacht würde.
- Privat abgerufene Inhalte dürfen nicht gespeichert werden.
- Die Nutzung kostenpflichtiger Dienste ist bei der privaten Nutzung untersagt.

(4) Die private Nutzung des Internets ohne dienstlichen Anlass wird nicht als arbeits- oder dienstrechtlicher Verstoß angesehen, sofern sie nicht gegen Ziffer 4 und die Einschränkungen der privaten Nutzung in Ziffer 6 (1) und 6 (3) verstößt.

(5) Für private e-Mails gilt die Richtlinie I.7 vom 7. März 2002 (Brem.ABl. S. 223).

7. Filterung und Sperrung unzulässiger oder rechtswidriger Inhalte

(1) Sowohl die dienstliche als auch die private Nutzung des Internets unterliegt Zugriffsregelungen eines zentral eingesetzten Content-Scanners im BVN. Der Senator für Finanzen behält sich vor, unzulässige und rechtswidrige Inhalte nach Ziffer 4 zentral BVN-weit zu sperren.

(2) Dienststellen können beim Senator für Finanzen beantragen, dass einzelne Arbeitsplätze (z.B. Strafverfolgung) aus der zentralen Filterung ausgenommen werden. Dies gilt nur für die dienstliche Nutzung. In diesen Fällen wird eine zentrale Vollprotokollierung mit Speicherung der ungekürzten IP-Endgeräte-Adressen vorgenommen. Die unter Ziffer 9 dieser Richtlinie beschriebenen Kontrollen werden angewandt.

8. Protokollierung

(1) Die Protokollierung aller Internetzugriffe erfolgt grundsätzlich auf den für die Internetnutzung zur Verfügung stehenden zentralen Systemen des Providers.

(2) Die dezentrale Protokollierung privater Zugriffe ist untersagt.

(3) Die dezentrale Protokollierung dienstlicher Zugriffe darf nur in Abstimmung mit dem Senator für Finanzen erfolgen (siehe dazu Ziffer 9 (5)).

(4) Für alle Zugriffe (auch private) auf das Internet werden zentral die vollständigen IP-Adressen der abrufenden Netze, (aber nicht die IP-Adressen der Arbeitsplatz-PCs), die aufgerufenen Internetseiten (URL), das Datum und die Uhrzeit sowie der Umfang der Datenmenge protokolliert.

(5) Die Protokolldaten der privaten und dienstlichen Zugriffe werden zentral auf getrennten Systemen gehalten. Die Nutzungsdaten über die privaten Zugriffe auf das Internet dürfen nur zu Abrechnungszwecken oder bei Einwilligung der Nutzerin oder des Nutzers gespeichert werden.

(6) Die Protokolldaten aller Internetzugriffe werden spätestens nach 90 Tagen gelöscht.

9. Kontrolle der Internetzugriffe

(1) Die zentral erhobenen Protokolldaten dürfen ausschließlich vom Senator für Finanzen gemeinsam mit dem Gesamtpersonalrat ausgewertet werden, wenn

- bei privaten Zugriffen tatsächliche Anhaltspunkte den Verdacht auf eine unzulässige Nutzung im Sinne von Ziffer 4 (1)
- bei dienstlichen Zugriffen tatsächliche Anhaltspunkte den Verdacht auf eine unzulässige Nutzung im Sinne von Ziffer 4 (1) bis (3)

begründen.

(2) Die Auswertung beschränkt sich auf

- die Feststellung des Transfervolumens,
- die Feststellung der Anzahl der aufgerufenen Seiten,
- die Analyse der aufgerufenen Seiten. Die Analyse beschränkt sich bei privaten Zugriffen auf unzulässige Inhalte gemäß Ziffer 4 (1).

(3) Sofern sich bei einer Auswertung privater oder dienstlicher Zugriffe der Verdacht auf eine unzulässige Nutzung im Sinne von Ziffer 4 (1) bestätigt, informiert der Senator für Finanzen die zuständige Dienststelle, die danach die Strafverfolgungsbehörden einzuschalten hat.

(4) Sofern sich bei einer Auswertung dienstlicher Zugriffe der Verdacht auf eine unzulässige Nutzung im Sinne von Ziffer 4 (2) und (3), die eindeutig nicht in dienstlichem Zusammenhang steht, bestätigt, werden anstelle der Netzwerkadressen für einen Zeitraum von 30 Tagen die vollständigen IP-Adressen BVN-weit gespeichert. Die Dienststellen beauftragen für diese Auswertungen den Provider und tragen die Kosten (Anlage 2). Auswertungen dürfen nur auf den IP-Nummernkreis der beantragenden Dienststelle erfolgen. Die Dienststellen haben ihren Personalrat und den Landesbeauftragten für den Datenschutz davon unverzüglich zu informieren.

(4a)Sobald es ohne Gefährdung des Ermittlungszwecks möglich ist, ist in den Fällen der Absätze 3 und 4 den verdächtigten Beschäftigten Gelegenheit zu geben, sich zu äußern.

(5) Die Aktivierung der zentralen Protokollierung mit Netzbereich- und Endgeräte-Adresse erfolgt immer unter Beachtung des Vier-Augen-Prinzips. Die Auswertungen sind dabei auf die Netzbereiche der beantragenden Dienststelle zu begrenzen. Sofern die Endgeräte-Adresse zentral nicht zu protokollieren ist, darf nur mit Genehmigung des Senators für Finanzen die Aktivierung der dezentralen Protokollierung für den vorgenannten Zeitraum und Anlass in der Dienststelle unter Beachtung des Vier-Augen-Prinzips erfolgen (Siehe Anlage 2).

(6) Die unter Ziffer 9 (4) und Ziffer 9 (5) erstellten Protokolldaten unterliegen der Zweckbindung und sind vom Senator für Finanzen, der Dienstelle und dem örtlichen Personalrat umgehend auszuwerten. Das Ergebnis ist von der Dienstelle in einer Niederschrift festzuhalten und dem Senator für Finanzen schriftlich mitzuteilen (Anlage 2). Alle anderen Protokolldaten, die nicht unmittelbar zum Nachweis eines bestätigten Verdachts im Sinne von Ziffer 9 (4) oder (5) dienen, sind sofort zu vernichten.

10. Schlussbestimmung

Diese Richtlinie tritt mit Wirkung vom 1. Februar 2004 in Kraft.

Bremen, den 1. Februar 2004

Der Senator für Finanzen

Anlage 1

Einverständnis- und Verpflichtungserklärung für die private Nutzung des Internet

Ich möchte, wie in der Richtlinie für die Bereitstellung und Nutzung von Internet/Intranet-Zugängen vom 1. Februar 2004 (Brem.ABl. S. 77) festgelegt, den dienstlichen Internetzugang privat nutzen und erkläre mich durch nachfolgende Unterschrift bereit, ab dem

<Datum>

dafür monatlich € 2,– (zwei in Worten) zu zahlen. Die Zahlung wird mir von meiner Gehaltszahlung/Vergütung abgezogen. Ein Anspruch auf Rückzahlung im Falle der Nichtnutzung besteht nicht.

Die private Nutzung des Internet kann ich jederzeit formlos zum darauffolgenden Monatsende - nach Eingang des Schreibens - bei Performa Nord kündigen. Das entsprechende Nutzungsprogramm PDSwitch werde/lasse ich im Falle der Kündigung vom Arbeitsplatzrechner deinstallieren und den Deinstallationstermin mit der formlosen Kündigung bestätigen.

Ich verpflichte mich, die private Nutzung des Internet am Arbeitsplatz nach den Regularien und Verhaltensgrundsätzen der Internet-Richtlinie Richtlinie für die Bereitstellung und Nutzung von Internet/Intranet-Zugängen vom 1. Februar 2004 (Brem.ABl. S. 77) zu tätigen und darauf zu achten, dass ich bei der Nutzung der Internetadressen der Freie Hansestadt Bremen nach außen für die Freie Hansestadt Bremen in Erscheinung trete und dadurch eine besondere Sorgfaltspflicht an den Tag zu legen habe.

Ich wurde gesondert darüber belehrt, dass ein Verstoß dagegen arbeitsrechtliche oder disziplinarrechtliche Maßnahmen nach sich zieht.

Ich willige ein, dass meine Nutzerdaten personenbezogen nur unter den Voraussetzungen der Ziffern 8 und 9 der Internet-Richtlinie vom 1. Februar 2004 (Brem.ABl. S. 77) verarbeitet werden dürfen. Ich bin darüber unterrichtet worden, dass mir im Falle des jederzeitigen Widerrufs dieser Einwilligung die private Nutzung des Internets untersagt ist.

Bremen, den

<Unterschrift>

Anlage 2

Antrag und Auswertung für eine vollständige Protokollierung von dienstlichen Internet-Zugriffen aus dem BVN

Antragsdatum :
Dienststelle :

Begründung des Missbrauchsverdachtes/Art und Anlass

Zustimmung des örtlichen Personalrates

Erfolgt am:

Unterschrift

Zustimmung des Senators für Finanzen zum Protokollierungszeitraum
(maximal 4 Wochen)

Für den Class B/C-Netzbereich (IP-Adress-Raum):

Beginn: Ende:

Unterschrift

Auswertung der Protokolle

Ausgewertet am:

Namen der auswertenden Personen (Dienststelle, örtlicher PR, Senator für Finanzen):

Ist der Missbrauchsverdacht bestätigt? [ ] Ja [ ] Nein

Welcher?			Folgen, Maßnahmen?	
Strafrechtlich	:	[ ]	Strafanzeige	[ ]
Arbeitsrechtlich	:	[ ]	Verfahren	[ ]
Disziplinarrechtlich	:	[ ]	Verfahren	[ ]

Löschung der Protokolldateien am:

Löschung bestätigt durch:

Zurück an den Senator für Finanzen

Herausgegeben von der Senatskanzlei Bremen, Rathaus – Verlag: Carl Ed. Schünemann KG, Bremen, II. Schlachtpforte 7,
Druck: Girzig+Gottschalk, Hannoversche Straße 64, Bremen

I.7 Richtlinie für die Nutzung der Elektronischen Post (E-Mail) -TuI-E-Mail-Nutzung- vom 07.03.2002

Vorbemerkung

Mit der Einführung der elektronischen Post (E-Mail) werden neue Möglichkeiten der Kommunikation eröffnet. Vor diesem Hintergrund nutzt die bremische Verwaltung diese elektronische Kommunikation zum Austausch von Nachrichten und Anlagen in Form von Dateien sowohl im verwaltungsinternen als auch externen Verkehr.

Um einen reibungslosen, ordnungsgemäßen Betrieb und Ablauf der Kommunikationsdienste sicher zu stellen, sind nicht zuletzt wegen der datenschutzrechtlichen und sicherheitsrelevanten Aspekte entsprechende Regelungen erforderlich. Diese sind in dieser E-Mail-Richtlinie festgelegt.

Die Kommunikation mittels elektronischer Post ist ein Bereich, der sich technisch und organisatorisch ständig weiterentwickelt. Die Freie Hansestadt Bremen will die Nutzung elektronischer Post ausweiten und insbesondere elektronische Verschlüsselung und digitale Signaturen einsetzen. Entsprechende Regelungen und Standards sind z.Z. in der Entwicklung und können deshalb in dieser Richtlinie noch nicht vollständig berücksichtigt werden.

Erster Abschnitt: Allgemeines

1. Gegenstand der Richtlinie

Die Richtlinie regelt die Nutzung und Behandlung von elektronischer Post (E-Mail).

2. Geltungsbereich

Diese Richtlinie gilt für alle Dienststellen und Einrichtungen des Landes und der Stadtgemeinde Bremen.
Für Eigenbetriebe der Freien Hansestadt Bremen oder privatrechtliche Gesellschaften mit einer Mehrheitsbeteiligung der Freien Hansestadt Bremen , die per Vertrag[1] dem BVN beigetreten sind, gilt diese Richtlinie, sofern übertragbar.

3. Zuständigkeiten

(1) Um einen geordneten Dienstbetrieb zu gewährleisten, ist eine zentrale Steuerung der elektronischen Postdienste notwendig. Diese zentrale Steuerung wird vom jeweiligen Provider des Bremischen Verwaltungsnetzes (BVN) wahrgenommen, der vom Senator für Finanzen ausgewählt wird.

(2) Der Provider ist auch für die technische Abwicklung zuständig.

(3) Die Administration und das Einrichten von Postfächern erfolgt dezentral durch die jeweilgen Dienststellen.

(4) Die Dienststellen sind zuständig für ihren Bereich und haben folgende Regelungen zu treffenl:

- Einrichtung der E-Mail-Postfächer;
- Festlegung der E-Mail-Adressen gem. Namens-Konzept;
- Festlegung der Zugriffberechtigungen (z.B. bei organisationsbezogenen Postfächern), sofern es sich nicht um Postfächer und Verteiler der Personalvertretungsgremien handelt.

Zweiter Abschnitt: Voraussetzungen

1. Einrichtung

(1) Zur Teilnahme am elektronischen Postverkehr ist es erforderlich auf dem Mailserver elektronische Postfächer einzurichten und auf den PC E-Mail-clients zu installieren.

(2) Pro Dienststelle werden mindestens eingerichtet:

- zentrale Postfacher für die Dienststelle (zentrale elektronische Poststelle),
- dienstliche Postfächer für die Nutzer/ Nutzerinnen

sowie

- für die Frauenbeauftragte,
- den Personalrat,
- die Schwerbehindertenvertretung der Dienststelle

und bei Bedarf

- Postfächer für Organisationseinheiten und/oder Arbeitsgruppen.

2. E-Mail-Adressen

(1) Für die Dienststelle wird eine zentrale E-Mail-Adresse (zentrale elektronische Poststelle) eingerichtet. Diese lautet:
office@dienststellenname.bremen.de

(2) Für die Frauenbeauftragte der Dienststelle wird eine zentrale E-Mail-Adresse eingerichtet. Diese lautet:
frauenbeauftragte@dienststellenname.bremen.de

(3) Für den Personalrat der Dienststelle wird eine zentrale E-Mail-Adresse eingerichtet. Diese lautet:
personalrat@dienststellenname.bremen.de

(4) Für die Schwerbehindertenvertetung der Dienststelle wird eine zentrale E-Mail-Adresse eingerichtet. Diese lautet:
schwerbehindertenvertetung@dienststellename.bremen.de

(5) Alle Nutzer/Nutzerinnen, die über einen an das BVN angebundenen PC verfügen, erhalten mindestens eine E-Mail-Adresse. Diese Adressen müssen wie folgt aufgebaut sein:
Vorname.Nachname@dienststellenname.bremen.de

---

[1] *Beitrittsvertrag zur Nutzung von Infrastruktur und Dienstleistungen im Verwaltungsnetz der Freien Hansestadt Bremen (BVN)*

(6) Für Organisationseinheiten und/oder Arbeitsgruppen werden E-Mail-Adressen nach folgendem Schema eingerichtet:
Org-Einheit@dienststellenname.bremen.de
(z.B. Ref.-36@finanzen.bremen.de)
oder
Arbeitsgruppe@dienststellenname.bremen.de
(z.B. Telearbeit@finanzen.bremen.de).
(7) Die Festlegungen im Namenskonzept vom 1. Dezember 1997 werden bezüglich der Namenskonvention von E-Mail-Adressen werden insoweit geändert; die Umstellung der E-Mail-Adressen sollte kurzfristig vorgenommen werden.

Dritter Abschnitt: Rechtliche Aspekte

(1) Elektronische Nachrichten können rechtserhebliche Erklärungen enthalten und möglicherweise weitreichende Rechtsfolgen auslösen.

(2) Soweit rechtserhebliche Erklärungen keinen besonderen Formvorschriften unterliegen, dürfen sie ohne weiteres per elektronischer Post abgegeben werden. Elektronische Nachrichten von Mitarbeitern und Mitarbeiterinnen der Verwaltung, die eine unmittelbare Rechtswirkung auslösen können oder die von besonderer politischer Bedeutung sind, sollen aus Gründen der Beweisbarkeit mindestens mit einer fortgeschrittenen elektronischen Signatur im Sinne des Signaturgesetzes verbunden werden.

(3) Rechtserhebliche Erklärungen im Bereich des Zivilrechts

- für die durch Gesetz Textform vorgeschrieben ist, dürfen per elektronischer Post abgegeben werden, sofern dabei die Person des Erklärenden genannt und der Abschluss der Erklärung durch Namensnennung oder anders erkennbar gemacht werden. Elektronische Nachrichten von Mitarbeitern und Mitarbeiterinnen der Verwaltung, die eine unmittelbare Rechtswirkung auslösen können oder die von besonderer politischer Bedeutung sind, sollen aus Gründen der Beweisbarkeit mindestens mit einer fortgeschrittenen elektronischen Signatur im Sinne des Signaturgesetzes verbunden werden.
- für die durch Gesetz schriftliche Form vorgeschrieben ist, dürfen per elektronischer Post abgegeben werden, sofern dabei qualifizierte elektronische Signaturen im Sinne des Signaturgesetzes eingesetzt werden. Von diesem Grundsatz gibt es einige Ausnahmen (Beispiel: Bürgschaftserklärung eines Nichtkaufmanns), die im Einzelfall zu beachten sind.
- für die im Gesetz weitergehende Formanforderungen als Textform oder Schriftform vorgeschrieben sind (z.B. notarielle Beglaubigungen), dürfen nicht per elektronischer Post abgegeben werden.

(4) Rechtserhebliche Erklärungen im Bereich des Verwaltungsrechts, für die durch Gesetz die schriftliche oder eine andere besondere Form vorgeschrieben ist (Beispiel: Widerspruch), dürfen zur Zeit noch nicht per elektronischer Post abgegeben werden. Es sind aber Gesetzesänderungen in Vorbereitung, die die Rechtslage der im Bereich des Zivilrechts anpassen sollen.

(5) Gehen rechtserhebliche Erklärungen, die besonderen Formvorschriften unterliegen, per elektronischer Post ein, ist die zuständige Stelle verpflichtet, den Absender unverzüglich auf den Formmangel und die Folgen hinzuweisen.

(6) Angebote und Inhalte im E-Mail Verkehr sind gem. § 8 Absatz 1 Mediendienste-Staatsvertrag (MDStV)) unzulässig, wenn sie

- gegen Bestimmungen des Strafgesetzbuches verstoßen,
- den Krieg verherrlichen,
- offensichtlich geeignet sind, Kinder oder Jugendliche sittlich schwer zu gefährden,
- Menschen, die sterben oder schweren körperlichen oder seelischen Leiden ausgesetzt sind oder waren, in einer die Menschenwürde verletzenden Weise darstellen und ein tatsächliches Geschehen wiedergeben, ohne daß ein überwiegendes berechtigtes Interesse gerade an dieser Form der Berichterstattung vorliegt; eine Einwilligung ist unbeachtlich,
- in sonstiger Weise die Menschenwürde verletzen.

Vierter Abschnitt: Behandlung der elektronischen Post

1. Allgemeines

Die bestehenden Regelungen (z.B.I: Gemeinsame GeschäftsOrdnung -GGO-; dienststelleninterne Regelungen) sind grundsätzlich analog anzuwenden bis auf die im Folgenden geregelte Behandlung von elektronischem Posteingang und elektronischem Postausgang.
Die Manipulation von E-Mail (z.B. Verfälschung des Absenders oder des Inhalts) ist verboten.

2. Private Nutzung elektronischer Post

Die private Nutzung der elektronischen Post ist in allen dienstlichen Postfächern unzulässig. Zugelassen ist die Nutzung von Free-Mail-Servern im Internet oder Intranet mit dafür speziell eingerichteten privaten Postfächern, die wiederum nicht für dienstliche Zwecke genutzt werden dürfen. Der Zugriff auf Free-Mail-Server für die Nutzung privater E-Mail ist durch ein Zugangspasswort zu sichern, das nicht im dienstlichen Bereich hinterlegt und zugänglich gemacht werden darf.

Hinweis: Private E-Mail unterliegen dem Fernmeldegeheimnis nach §85 Abs. 1 Telekommunikationsgesetz (TKG) und dürfen nicht ohne Einwilligung der Kommunikationspartner dritten zugänglich sein.

3. Elektronischer Posteingang

(1) In der Regel geht die elektronische Post direkt bei den zuständigen Nutzern/Nutzerinnen ein. Für die zentralen Postfächer der Personalvertretungen ist durch geeignete Maßnahmen sicherzustellen, dass nur die legimitierten Mitglieder der Personalvertretungen Zugriff auf die dort eingehende elektronische Post verschaffen können.
Für das zentrale Postfach der Dienststelle sind die Zuständigkeit und die damit verbundenen Aufgaben gesondert festzulegen.
Das gleiche gilt für die Postfächer der Organisationseinheiten und/oder Arbeitsgruppen.
Unabhängig davon, wo die elektronische Post eingeht, gelten für die weitere Behandlung die in der GGO festgelegten Regelungen.
Der E-Mail-Client soll nach Möglichkeit ständig im Hintergrund aktiv sein, damit der Eingang neuer Nachrichten sofort angezeigt wird. Ist dies nicht möglich, ist der Posteingang wenigstens einmal pro Arbeitstag auf Neueingänge zu überprüfen.

(2) Bei vorhersehbarer Abwesenheit (Urlaub, Dienstreisen) kann ein automatischer Antworttext an den E-Mail-Absender geschickt werden, in dem auf die Abwesenheit des Empfängers hingewiesen bzw. eine andere dienstliche E-Mail-Adresse genannt wird. Andernfalls hat der zu Vertretende zu veranlassen, dass neu eingehende elektronische Post automatisch an den Vertreter weitergeleitet wird.
Bei nicht vorhersehbarer Abwesenheit (z.B. Erkrankung) muss die bereits aufgelaufene Post bearbeitet werden. Dazu sind Regelungen zur Vertretung schriftlich gem. Geschäftsverteilungsplan (GVP) zu treffen und zu hinterlegen.

(3) Erkennbar falsch adressierte Post ist nach Möglichkeit an die richtige Stelle oder die zentrale Posteingangsstelle elektronisch weiterzuleiten. Mindestens bei Weiterleitung über Dienststellengrenzen hinweg erhält der Absender eine automatisch zu generierende Nichtzustellungsnachricht.

(4) Ist eine eingegangene Nachricht nicht lesbar, nimmt der Empfänger Kontakt mit dem Absender auf, um das Problem zu lösen.

(5) Über den Umgang mit eingegangenen E-Mail, deren Absender oder Inhalt zweifelhaft erscheinen, sind Regelungen in der Dienstelle zu treffen.
Über den Umgang mit aktiven Inhalten sowie dem Aktivieren von Programmen und sonstigen Eingaben sind die Nutzerinnen/Nutzer regelmäßig aufzuklären.

(6) Wegen der Virengefahr ist ein ständig aktuell gehaltener Virenscanner zu aktivieren. In der Praxis haben sich folgende Sicherheitsmassnahmen bewährt:

- permanente Virenprüfung am Arbeitsplatz

und

- Virenprüfung direkt am Mailserver vor Weiterleitung der Nachrichten auf den E-Mail-Client.

(7) Das Abonnieren von elektronischer Post über Mailing-Listen darf nur zu dienstlichen Zwecken erfolgen und muss in jedem Fall auf das notwendige Maß beschränkt werden.

(8) Der Empfang privater E-Mail ist technisch nicht zu unterbinden. Dem Absender ist deshalb unverzüglich mitzuteilen, dass es sich ausschliesslich um ein dienstlich zu nutzendes E-Mail-Postfach handelt und die Zusendung privater Post zukünftig unterbleiben soll.

4. Elektronischer Postausgang

(1) Für die tägliche Dienstpost soll soweit wie möglich der elektronische Postverkehr genutzt werden.

(2) Dokumente, die rechtserhebliche Erklärungen enthalten, die nach geltendem Recht nicht in elektronischer Form abgegeben werden dürfen (siehe dazu den 3. Abschnitt), dürfen nur zusätzlich zur Übersendung in schriftlicher Form per elektronischer Post versandt werden.

(3) Die Übermittlung sensibler Daten mittels E-Mail ist nur unter Einsatz geeigneter Verschlüsselungsverfahren zulässig.
Damit eine Vertretungsregelung (Einsichtnahme in verschlüsselte E-Mail) gewährleistet ist, soll zukünftig, wenn technisch verfügbar, zur Verschlüsselung ein Gruppenzertifikat der Dienststelle bzw. des Servers eingesetzt werden, dessen öffentlicher Schlüssel in geeigneter Form bekanntzugeben ist.
Die derzeit genutzte Verschlüsselung mit einem dem Benutzer persönlich zugeordeneten Verschlüsselungszertifikat (z.B. bei Verfahren wie PuMa und SEKT) soll zukünftig durch ein Gruppenzertfikat der Dienststelle bzw. des Servers abgelöst werden.

(4) Attachments (Anlagen in Dateiform) sind grundsätzlich zulässig.
Spezielle Dateiformate (z.B. aus Fachanwendungen) sollen nur dann versandt werden, wenn bekannt ist, dass der Empfänger diese Dateien auch bearbeiten kann. Wegen der begrenzten Speicherkapazität der Mailserver sollen E-Mail einschl. eines Dateianhanges grundsätzlich nicht größer als 2 MB sein. Abweichungen hiervon sind vorab mit den jeweiligen Administratoren der Mailserver abzustimmen.
Programmdateien dürfen wegen der damit verbundenen Virengefahr nur durch die Systemverwaltung oder spezielle Fachverfahren versandt werden.

(5) E-Mail sind mit einem aussagefähigen Betreff zu versehen, um dem Empfänger den Überblick über die eingegangenen Nachrichten zu erleichtern.

(6) Einstellungen zur Priorität sind im internen E-Mail-Verkehr auf das notwendige Maß zu beschränken.
Die Verwendbarkeit von Attributen, wie Prioritäten „niedrig", „normal" oder „hoch" und Vermerke der Vertraulichkeit, wie „normal", „persönlich" oder „vertraulich" sind von den eingesetzten E-Mail-Client-Produkten abhängig. Es kann somit nicht

sichergestellt werden, dass abgesendete Attribute auch auf der Empfängerseite interpretiert werden können.

(7) Elektronische Post dient der schnellen Übermittlung von Informationen und unterliegt deshalb keiner besonderen Gestaltungsvorgabe. Sollte eine besondere Gestaltung erforderlich sein (z.B. Kopfbogen), ist der Nachricht ein entsprechender Dateianhang beizufügen.
Die E-Mail muss den Absender und die absendende Dienststelle eindeutig erkennen lassen.

(8) Sendeoptionen (z.B. Empfangsbestätigungen) basieren derzeit nicht auf Internetstandards. Darüber hinaus erzeugen sie unnötige Netzlast und könnten zur Mitarbeiterkontrolle verwendet werden.
Im Bedarfsfall kann im versandten Nachrichtentext eine Empfangsbestätigung durch den Empfänger erbeten oder die Sendeoption eingestellt werden.

(9) Die automatische Weiterleitung von E-Mail ist nur an Postfächer innerhalb des BVN zugelassen. Dabei sind verschlüsselt eingegangene E-Mail auch verschlüsselt weiter zuleiten.
Greifen Mitarbeiter und Mitarbeiterinnen von ausserhalb des BVN auf Postfächer im BVN zu, sind diese Zugriffe durch entsprechende Authentisierung, Identifikation und Verschlüsslung des Verbindungskanals abzusichern.
Sofern der berechtigte Zugriff nur auf zentrale Komponenten im BVN erfolgen darf, können E-Mail-Postfächer auf zentralen E-Mail Servern im BVN dupliziert und durch Umlenkung vom persönlichen auf das zusätzlich zentral eingerichtete Postfach dem Zugriff von aussen zugänglich gemacht werden.

5. Ablage

E-Mails, die für die Bearbeitung von Vorgängen von Bedeutung sind, sind diesen in ausgedruckter Form beizufügen.
Die Grundsätze einer ordnungsgemäßen Aktenführung gelten sinngemäß auch für ein- und ausgehende elektronische Post.
Nicht mehr benötigte E-Mail sind zu löschen.
Für die Archivierung von elektronischen Vorgängen sind zukünftig Archivierungssysteme einzusetzen.

Fünfter Abschnitt: Verzeichnis der E-Mail-Adressen; Verteilerlisten

Alle personen- und organisationsbezogenen E-Mail-Adressen befinden sich im globalen E-Mail-Verzeichnis. In das globale Adressbuch sind lediglich Familienname, Vorname, Dienststelle, Funktionsbereich, Organisationskennzeichen, die dienstliche Telefonnummer und dienstliche Faxnummer sowie die dienstliche E-Mail-Adresse aufzunehmen. Die Pflege dieses Adressbuches erfolgt sowohl zentral als auch dezentral durch die jeweiligen Administratoren.
Das Anlegen von persönlichen Adressbüchern und Verteilerlisten, über die sich eine größere Zahl von Empfängern zeitgleich erreichen lässt, ist zulässig.
Allgemein ist beim Gebrauch von Verteilerlisten aber zu beachten, dass hierdurch nicht unerhebliche Aktivitäten ausgelöst werden.
Zur Vermeidung von missbräuchlicher Nutzung von Verteilerlisten sollte der Gebrauch auf deren Mitglieder beschränkt werden (Versand nur an und durch die im Verteiler genannten Mitglieder).

Sechster Abschnitt: Protokollierung

Das E-Mail-System führt Protokolldateien (Sende- und Empfangsdaten; keine Inhaltsdaten) über ein- und ausgehende E-Mail.
Die Protokolldateien für Internet-Mail werden nur in Fehlerfällen zur Klärung der Ursache nach Rücksprache mit der betroffenen Dienststelle ausgewertet. Einzelheiten sind ggf. in einer besonderen Regelung zu treffen.
Eine Auswertung der Protokolldateien auf der Basis von Messungen des Lastverkehrs ist nur anonymisiert durch den Provider zugelassen.
Bezüglich der Löschung der Protokolldateien finden die Bestimmungen der einschlägigen Datenschutzgesetze Anwendung.

Siebter Abschnitt: Administrative Aufgaben

(1) Es ist nicht zu lässig, im Rahmen der Administration (d. h. Einsichtnahme / Veränderung / Löschung) auf Postfächer der Mitarbeiter/-innen ohne deren Genehmigung zu zugreifen.

(2) Eine Leistungs- und Verhaltenskontrolle (z. B. Erstellen von Kommunikationsprofilen) ist nicht zulässig.

(3) Das Löschen von Postfächern erfolgt erst, nachdem die Mitarbeiter/-innen Gelegenheit zum Auslesen und Sichern des Inhalts ihrer Postfächer hatten. Sie teilen dies dem Admnistrator/Administratorin mit.

(4) Sofern durch die Wahrnehmung von Administrationsaufgaben (Herunterfahren des Systems, Software Updates) die Arbeit der Mitarbeiter/-innen beeinträchtigt wird, sind diese vorher zu informieren. Es ist ihnen Gelegenheit zu geben, Ihre Arbeitsergebnisse zu sichern.

Achter Abschnitt: Schlussbestimmung

Diese Richtlinie tritt am Tage ihrer Verkündung in Kraft.

Bremen, den 07.03.2002 Der Senator für Finanzen