Zwischen dem Finanzministerium des Landes Schleswig-Holstein

einerseits

und

- dem DBB Beamtenbund und Tarifunion
Landesbund Schleswig-Holstein –

- dem Deutschen Gewerkschaftsbund
Bezirk Nord -

andererseits

wird die folgende Vereinbarung nach § 59 Mitbestimmungsgesetz des Landes Schleswig-Holstein (MBG) geschlossen.

Richtlinie zur Nutzung von Internet und E-Mail

1 Geltungsbereich

Diese Richtlinie gilt für die Beschäftigten (Beamtinnen und Beamten sowie Arbeitnehmerinnen und Arbeitnehmer) der unmittelbaren Landesverwaltung im Sinne des § 3 in Verbindung mit § 2 Abs. 1 Mitbestimmungsgesetz des Landes Schleswig-Holstein (MBG), deren PC-Arbeitsplatz an das Landesnetz angeschlossen ist und denen über diesen Anschluss die Dienste Internet und E-Mail zur Verfügung gestellt werden.

Sie gilt nicht für die Gerichte und Staatsanwaltschaften.

Sie gilt nicht für die Beschäftigten der Landtagsverwaltung und des Landesrechnungshofes.

Soweit die Präsidentin oder der Präsident des Landtages beziehungsweise des Landesrechnungshofes das Einvernehmen nach § 59 Abs. 4 MBG Schl.-H. erklärt, gilt diese Vereinbarung auch für die Beschäftigten des jeweiligen Bereiches.

Anlagen 1 und 2 sind Bestandteil dieser Vereinbarung.

2 Umfang

Diese Richtlinie regelt die dienstliche und private Nutzung der dienstlich zur Verfügung gestellten Services Internetzugang und E-Mail[1].

Die Regelungen dieser Vereinbarung müssen durch die Dienststellen für ihren Zuständigkeitsbereich in entsprechenden Dienstanweisungen oder Dienstvereinbarungen präzisiert und ergänzt werden.

3 Grundsätze der Nutzung von Internet und E-Mail

3.1 Internetzugang und E-Mail sind Arbeitsmittel, die an allen PC-Arbeitsplätzen, die an das Landesnetz angeschlossen sind, zur Verfügung gestellt werden sollen.

3.2 Die Nutzung von Internetzugang und E-Mail durch die Beschäftigten muss eigenverantwortlich und der jeweiligen dienstlichen Aufgabenstellung angemessen erfolgen.

3.3 Die Nutzung von E-Mail ist ausschließlich für dienstliche Zwecke zulässig.

3.4 Für private Zwecke ist den Beschäftigten die unentgeltliche Nutzung des dienstlichen Internetzugangs ausschließlich zum Nutzen von Web-Seiten (Dienste http / https) gestattet, soweit dienstliche Interessen nicht entgegenstehen.

3.5 Der lesende und schreibende Zugriff auf ein privates, bei einem externen Dienstanbieter geführtes E-Mail-Postfach (Web-Mail) ist den Beschäftigten gestattet, soweit dienstliche Interessen nicht entgegenstehen.

3.6 Die Zulassung der Nutzung des Internetzugangs nach Nr. 3.4 und 3.5 kann – für einen bestimmten Verwaltungsbereich oder im Einzelfall – widerrufen werden.

3.7 Die Nutzung von Internetzugang und E-Mail im Rahmen der Vereinigungsfreiheit entsprechend Artikel 9 Grundgesetz ist zulässig.

[1] Einzelheiten des Diensteumfangs sind jeweils aktuell der Anlage 1 zu entnehmen.

3.8 Die Beschäftigten werden in der Nutzung der angebotenen Dienste bedarfsgerecht geschult und über mögliche Risiken informiert. Beschäftigte sollen zur selbständigen und effizienten Nutzung von E-Mail und Internet im Rahmen ihrer dienstlichen Aufgaben befähigt werden. Wichtige Schulungsinhalte sind in Anlage 2 dargestellt.

3.9 Die Dienststellen haben im Rahmen ihrer Zuständigkeit die Nutzung der angebotenen Dienste unter Beachtung der in Nr. 6 und Anlage 1 dieser Vereinbarung festgelegten Grundsätze zu überwachen.

3.10 Die Sicherheitsmaßnahmen der vom Finanzministerium über Dataport betriebenen zentralen Komponenten entbinden die Dienststellen nicht von der entsprechenden Verantwortung für ihren jeweiligen Zuständigkeitsbereich.

3.11 Die Regelungen der Abgabenordnung (insbesondere § 87 a Elektronische Kommunikation) und der Landesverordnung über die Verarbeitung personenbezogener Daten in Schulen (Datenschutzverordnung Schule) bleiben unberührt.

4 E-Mail

4.1 Für den Dokumentenverkehr ist, soweit keine rechtlichen, wirtschaftlichen oder technischen Gründe entgegenstehen, die elektronische Post vorrangig gegenüber der Briefpost und dem Fax einzusetzen. Ein paralleler Versand mit Briefpost soll unterbleiben.

4.2 Der E-Mail-Eingang soll mindestens einmal arbeitstäglich auf eingegangene E-Mail gesichtet werden.

4.3 E-Mail wird wie eingehende Post gewertet und weiterbearbeitet. Ziffer 5.2.1 der Gemeinsamen Geschäftsordnung für die Ministerien des Landes Schleswig-Holstein (GGO) ist nicht anzuwenden.

4.4 Wenn bei einer eingehenden E-Mail die absendende Stelle, der Inhalt oder die Anlage zweifelhaft erscheint, ist unverzüglich die zuständige Stelle[2] zu informieren. Diese entscheidet über die weitere Behandlung.

4.5 Eine elektronische Post mit vertraulichem Inhalt oder mit personenbezogenen Daten darf extern (außerhalb des Landesnetzes) nur versandt werden, wenn die Nachricht mit einem freigegebenen Programm verschlüsselt ist und die Empfängerin oder der Empfänger zur Entschlüsselung der elektronischen Post in der Lage ist. Sicher gekoppelte andere Verwaltungsnetze gelten in diesem Sinne als intern.

5 Internet

5.1 Unzulässig ist jede absichtliche oder wissentliche Nutzung des Internetzugangs, die gegen geltende Rechtsvorschriften verstößt oder geeignet ist, den Interessen der Landesregierung oder deren Ansehen in der Öffentlichkeit zu schaden oder die Sicherheit des Landesnetzes zu beeinträchtigen.

5.2 Unzulässig ist die Internetnutzung für Glücksspiele, Wetten und ähnliche Internetaktivitäten, die ein Suchtpotential und damit gesundheitliches Gefährdungspotential für Nutzer besitzen (Glücksspiele, Online-Poker, Sport-/Wetten, Lotto u.ä.).

5.3 Die Nutzung von Anonymisierungsdiensten ist verboten.

5.4 Mit der Erlaubnis zur privaten Nutzung des Internetzugangs ist kein Anspruch auf Verfügbarkeit des Dienstes und Betreuung begründet.

6 Protokollierung und Kontrolle

6.1 Eine Protokollierung der Nutzung der Dienste (Nutzungs-, Verkehrs- und Inhaltsdaten) erfolgt, soweit unbedingt erforderlich

- aus Gründen der Daten- und Systemsicherheit,
- aus Gründen der Systemtechnik (z.B. zur Fehlerverfolgung) und

[2] Wer diese Aufgabe vor Ort wahrnimmt, ist in den Dienststellen festzulegen, zum Beispiel im jeweiligen Sicherheitskonzept.

- aus Gründen der Arbeitsorganisation (z.B. zur Feststellung von Art und Umfang der Nutzung und zur Missbrauchskontrolle)

Einzelheiten der Protokollierung (Art, Umfang, Anonymisierung, Aufbewahrung) sind insbesondere in Anlage 1 in der jeweils aktuellen Fassung festgelegt.

6.2 Personal, das Zugang zu Protokollinformationen hat, ist besonders auf die Sensibilität dieser Daten hinzuweisen und auf Einhaltung von Datenschutz zu verpflichten. Bei der Auswahl des Personals ist dies entsprechend als Eignungsvoraussetzung zu berücksichtigen. Dafür ist auch Sorge zu tragen (zum Beispiel durch vertragliche Vereinbarung), wenn und soweit es sich nicht um eigenes Personal handelt.

6.3 Eine Auswertung von Protokolldaten muss die Grundsätze einer datenschutzgemäßen Kontrolle berücksichtigen, insbesondere den Grundsatz der Verhältnismäßigkeit. Eine individuelle Verhaltens- und Leistungskontrolle durch eine Auswertung der Protokolldaten ist grundsätzlich unzulässig. Auswertungen von Protokolldaten erfolgen grundsätzlich zunächst anonymisiert.

6.4 Ergeben sich dabei eindeutige Hinweise auf unzulässige Zugriffe oder auf eine deutliche Überschreitung der erlaubten privaten Nutzung (Stufe 1), ist der betroffene Kreis der Beschäftigten zunächst pauschal auf die Unzulässigkeit dieses Verhaltens hinzuweisen (Stufe 2). Gleichzeitig wird darüber unterrichtet, dass bei Fortdauer der Verstöße zukünftig eine gezielte Kontrolle (Stufe 3) nach einem gesondert festzulegenden Verfahren stattfinden kann. An der Festlegung des Verfahrens und Auswertung von Protokolldaten sind die zuständige Gleichstellungsbeauftragte, Personalvertretung, Schwerbehindertenvertretung und ggf. die oder der behördliche Datenschutzbeauftragte beteiligen. Das Verfahren ist den Beschäftigten bekannt zu machen.

Für die gezielte Kontrolle (personenbezogene Protokollierung) entsprechend Stufe 3 müssen der genaue Zweck, der Umfang der Daten, der Zeitraum der Protokollierung und deren Auswertung vorab in einem Konzept festgelegt werden; der Umfang der von der Protokollierung erfassten Personen muss dabei auf den Kreis der Verdächtigen begrenzt werden. Es darf nicht das

gesamte Personal überwacht werden. Die personenbezogenen Daten sind nach der Auswertung zu löschen. Die Ergebnisse sind den Betroffenen bekannt zu geben. Entsprechend der Ergebnisse ist das weitere Vorgehen abzuwägen:
- Einstellen der Kontrollen/keine weitere Überwachung,
- erneutes Ermahnen des betroffenen Personenkreises und Fortführen der gezielten Kontrolle oder
- Verschärfen der Kontrolle, in dem die Protokollierung auf dem Arbeitsplatzrechner stattfindet (Stufe 4).

Für die Protokollierung auf dem Arbeitsplatz gelten dieselben Anforderungen wie in Stufe 3 mit Ausnahme der Ankündigung. Die Mitarbeiterinnen und Mitarbeiter müssen über diese Maßnahme aufgeklärt werden. In diesem Stadium ist auch zu erwägen, ob bereits eine Strafanzeige zu stellen und eine Strafverfolgungsbehörde hinzuziehen ist, um bei der Beweissicherung keine Fehler zu machen.

6.5 Bei fortgesetzten Verstößen sind dienst- oder arbeitsrechtliche Maßnahmen gegen die betreffenden Beschäftigten nicht ausgeschlossen.

6.6 Unzulässig sind Auswertungen insbesondere von Protokolldaten (Nutzungs-, Verkehrs- und Inhaltsdaten), um Informationen über die Nutzung des Dienstes Internet und die E-Mail-Kommunikation in Zusammenhang mit besonders zu schützenden Funktionen (zum Beispiel Personalvertretungen, Gleichstellungsbeauftragte, Schwerbehindertenvertretungen, behördliche Datenschutzbeauftragte und ähnliche) sowie über die Kommunikation im Sinne von Ziffer 3.7 zu gewinnen. Bei Verdacht von Straftaten ist die Auswertung von Protokolldaten den zuständigen Strafverfolgungsbehörden zu überlassen.

7 In-Kraft-Treten

Diese Richtlinie tritt am 01.01.2010 in Kraft.

Schlussbestimmungen

Die zu dieser Vereinbarung gehörenden Anlagen 1 und 2 können in der Weise aktualisiert werden, dass das Finanzministerium einen entsprechenden

Änderungsvorschlag vorlegt, der beschlossen ist, sobald von allen Beteiligten (im Regelfall schriftlich) zugestimmt wurde.

Diese Vereinbarung kann mit einer Frist von einem Jahr erstmalig zum 31. Dezember 2012 von beiden Seiten gekündigt werden.

Wenn diese Vereinbarung gekündigt wird, gilt sie in allen Punkten so lange weiter, bis eine neue Vereinbarung abgeschlossen wurde, die die hier geregelten Sachverhalte neu regelt. Dies gilt auch für den Fall, dass die gesetzlichen Regelungen zur Mitbestimmung oder zum Beschäftigtendatenschutz geändert werden.

Diese Vereinbarung einschließlich Anlagen und deren Aktualisierungen werden im Intranet der Landesregierung und im Amtsblatt veröffentlicht.

Kiel, 26.11.2009
Ort, Datum

Staatssekretär des Finanzministeriums
Schleswig-Holstein

gez. Dr. Olaf Bastian
Dr. Olaf Bastian

Hamburg, 19.11.2009
Ort, Datum

Deutscher Gewerkschaftsbund
- Bezirk Nord –

gez. Carlos Sievers
Carlos Sievers

Kiel, 26.11.2009
Ort, Datum

Deutscher Beamtenbund und Tarifunion
- Landesbund Schleswig-Holstein e.V. –

gez. Anke Schwitzer
Anke Schwitzer

1. Der Internet-Dienst umfasst
   1.1. http (hypertext transport protocol) – Surfen
   1.2. https (hypertext transport protocol secure) – verschlüsseltes Surfen
   1.3. smtp (simple mail transport protocol) – Internet-Mail
   1.4. ftp (file transport protocol) – Download (ggf. Upload) von Dateien
   1.5. nntp (network news transfer protocol) – Newsgroups
   1.6. Anschluss an andere Verwaltungsnetze

   Der Zugang wird grundsätzlich rund um die Uhr angeboten (erreichte Verfügbarkeit größer als 98,5% im Jahresmittel). Grundsätzlich wird der Firewall vom Netz getrennt, wenn unbekannte Angriffe aus dem Internet auftreten oder die Vermutung besteht, dass Systeme unberechtigt genutzt werden.

   Einzelheiten zum Internet-Dienst sind der Anlage „Service Level Agreement Internet-Zugang über den Dataport Firewall SH“ - Version: 1.2 vom 02.12.2015 - zu entnehmen.
2. Der E-Mail-Dienst umfasst

   Mailen im Bereich des Landesnetzes und in sicher gekoppelten anderen Verwaltungsnetzen (z.B. DOI, CNPON, ParlaNet, …) sowie im Internet.

   Einzelheiten zum E-Mail-Dienst sind der Anlage “Service Level Agreement Internet E-Mail SH – Version 1.2 vom 02.12.2015“ zu entnehmen.

   Die Details zur technischen Dienstleistung „E-Mail Transport“ und „E-Mail Filterung“ sind dort dem Kapitel 3 zu entnehmen.
3. Inhaltsdaten der E-Mail werden an der Firewall nicht protokolliert.

   Von den Verkehrsdaten der E-Mail werden an der Firewall bzw. im Spamfilter protokolliert:
   a) Datum / Uhrzeit,
   b) Adressen von Absender und Empfänger,
   c) Übertragene Datenmenge,
   d) IP-Adresse des unmittelbaren Eingangs- und Ausgangs-Servers,
   e) SMTP-Statuscode (z.B. gesendet oder abgewiesen) und die ID der Mail auf dem nächsten Server, an den die Mail für den weiteren Transport übergeben wurde,

f) Betreff der E-Mails (nur anlassbezogen zur Gefahrenabwehr insbesondere bei Spamfluten),
g) Prüfungen der Spambewertung (welche Regeln haben angeschlagen) sowie Diagnoseinformationen zur Spam/Virenprüfung.

Die E-Mail-Protokolldaten werden 10 Tage aufbewahrt und dann gelöscht.
Art und Umfang der Aufbewahrung und Verwendung von E-Mail-Inhaltsdaten durch die Dienststellen sind von diesen für ihren jeweiligen Zuständigkeitsbereich festzulegen und den Beschäftigten bekannt zu machen.

4. Von den Nutzungsdaten des Internets werden protokolliert:
   a) IP-Adresse des aufrufenden Arbeitsplatzes
   b) URL (www-Adresse) und IP des Zielsystems
   c) HTTP-Methode und Statuscode
   d) Datum / Uhrzeit
   e) Menge der übertragenen Daten

   Nach einem Tag werden die Protokolle anonymisiert, das heißt, die letzten Stellen der IP-Adressen (ab dem letzten Punkt) werden gelöscht. Die Protokolle werden nach zehn Tagen gelöscht.
5. Diese Festlegungen gelten für die zentralen Komponenten und entsprechend für die lokalen Komponenten, soweit dort keine weitergehenden Regelungen getroffen, vereinbart und bekannt gemacht worden sind.

Anlage 2 zur Richtlinie Internet und E-Mail

Schulungsbausteine zur Nutzung von Internet und E-Mail

Grundlagen, für Nutzerinnen und Nutzer

- Bedienung von aktuellem Internet-Browser und E-Mail-Client
- Viren und SPAM
- Internet-Dienste und ihre Einsatzmöglichkeiten
    - WWW-Suchmaschinen
    - Newsgroups
    - E-Mail
    - File-Transfer
- Modellhafte Internet-Angebote ausgewählter Verwaltungen
- Datenschutz und Datensicherheit (Einführung)

Vertieftes Wissen, insbesondere für Fachpersonal

- Kompakt-Einstieg in die Datenkommunikation
- Datenschutz bei der Internetnutzung
- Technik und Recht bei Firewalls
- Datenschutz bei der Internetnutzung durch Schulen