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

Hamburg, 19.11.2009
Ort, Datum

Deutscher Gewerkschaftsbund
- Bezirk Nord –

Kiel, 26.11.2009
Ort, Datum

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

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

Anlage 1 zur Richtlinie Internet und E-Mail vom 01.01.2010
Stand: 01.01.2016

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,

Richtlinie zur Nutzung von Internet und E-Mail

Die Richtlinie regelt teilweise unmittelbar die Nutzung von Internet und E-Mail, bildet aber teilweise auch nur einen Rahmen für präzisierende und ergänzende Regelungen der Dienststellen für ihren (örtlichen) Zuständigkeitsbereich.
Die Vereinbarung enthält zur besseren Verständlichkeit auch das Angebot der Landesregierung, ihren Beschäftigten die private Nutzung des Internet zu gestatten, obwohl diese Erlaubnis selbst nicht mitbestimmungspflichtig ist.

1 Geltungsbereich

Mit dem Begriff „Beschäftigte" im Sinne des § 3 MBG sind die Richterinnen und Richter und die Staatsanwältinnen und Staatsanwälte, soweit sie in ihrer originären Zuständigkeit tätig sind, ausgenommen. Die Verbindung mit § 2 Abs. 1 MBG schließt ausdrücklich Personen ein, die für eine Dienststelle tätig sind und dort beschäftigt werden, ihr aber nicht angehören.
Explizit ausgenommen sind darüber hinaus die Gerichte und Staatsanwaltschaften; es wird angestrebt, für diesen Bereich gleichzeitig eine einheitliche Regelung zu schaffen.

Es wird klargestellt, dass Anlagen 1 und 2 Bestandteil dieser Vereinbarung sind. Einzelne Inhalte sind in Anlagen aufgenommen, damit sie in einem vereinfachten Verfahren geändert werden können.

2 Umfang

Es wird klargestellt, dass die Richtlinie vier Bereiche regelt:

- dienstliche Nutzung von Internet
- dienstliche Nutzung von E-Mail
- private Nutzung von Internet
- private Nutzung von E-Mail

Dienststellen müssen in ihrem lokalen Zuständigkeits- und Verantwortungsbereich diese Richtlinie präzisieren und ergänzen. Solche lokalen Dienstvereinbarungen

beziehungsweise mitbestimmungspflichtige Dienstanweisungen dürfen jedoch dieser Richtlinie nicht widersprechen (§ 59 Abs. 5 MBG). Insbesondere dürfen im Bereich Protokollierung und Kontrolle keine lokalen Vorgehensweisen festgelegt werden, die dazu führen können, dass der in der Dienstvereinbarung festgelegte Standard **unter**schritten wird und dadurch gegebenenfalls eine bis zum Endgerät durchgängige Kontrolle verhindert würde. So muss zum Beispiel bei dynamischer IP-Nummern-Vergabe eine Dienststelle sicherstellen, dass die in Anlage 1 beschriebenen Informationen in entsprechendem Umfang und für die entsprechende Dauer zur Verfügung gestellt werden können.

Regelungsbedarf besteht insbesondere bezüglich der nachfolgend genannten Punkte (viele davon sind oder werden Bestandteil eines Sicherheitskonzeptes sein):

- Muss die Nutzung von Internet und E-Mail über besondere technische Wege (zum Beispiel Terminal-Server) bereitgestellt werden, um Daten/Anwendungen mit besonderem Schutzbedarf Rechnung zu tragen?
- Müssen einzelne Arbeitsplätze von der Nutzung der Dienste ausgenommen werden, aus welchem Grund?
- Wird die Nutzung von Internet und E-Mail über das hinausgehend protokolliert, was die Richtlinie festlegt? Wie sind die Einzelheiten? Speicherumfang, Aufbewahrungsdauer, … Verlaufsprotokolle, Löschrechte, Löschmöglichkeiten für die Beschäftigten selbst? …
- Wie ist der Umgang mit E-Mail geregelt im Falle der ungeplanten oder geplanten Abwesenheit – Umleitung, Abwesenheitsassistent, … ?
- Wie ist der Umgang mit den lokalen Nutzungs-, Verkehrs- und Inhaltsdaten vorgesehen? Wer ist dafür zuständig? Wer darf kontrollieren? Welches Verfahren ist dazu festgelegt?
- Wie sind die Einzelheiten von lokalen Virenschutzprogrammen? Wie sind die PC-Arbeitsplätze vor der unbeabsichtigten Ausführung von Programmen geschützt?
- Wie muss an besonderen Arbeitsplätzen (mit zeitkritisch zu bearbeitenden Aufgaben) der Posteingang gesichtet werden?

- Wie ist insgesamt die private Nutzung des dienstlichen PC-Arbeitsplatzes geregelt?
- Ist das Speichern privater Dateien (ggf. auch Download aus dem Internet) zulässig, wie werden solche Dateien kenntlich gemacht, wie ist das Zugriffsrecht auf solche Dateien, vor allem im Vertretungsfall?
- Dürfen Seiten privat ausgedruckt werden, werden dafür Kosten in Rechnung gestellt?
- …
- …

3 Grundsätze der Nutzung von Internet und E-Mail

Diese Ziffer beinhaltet Regelungen, die sowohl die Nutzung des Internet als auch der E-Mail betreffen.
Zur Einordnung, welche Nutzung dieser Services jeweils **dienstlich bzw. privat** ist, ist Folgendes zu beachten:

- Zur Abgrenzung richtet man sich in erster Linie am **Zweck der Kommunikation** aus (unabhängig von der Zweckmäßigkeit); „dienstlich" ist jede die Arbeit fördernde Nutzung der Kommunikationsmittel (Neue Zeitschrift für Arbeitsrecht NZA 11/2002, RA Dr. Stefan Ernst, Freiburg/Br.).
- Dazu zählen auch fehlgeschlagene oder unzweckmäßige Versuche der Kommunikation.
- Als dienstlich gilt auch dienstlich motivierte private Kommunikation, deren Notwendigkeit in der Sphäre des Arbeitgebers resultiert und deren Gestattung sich aus der Fürsorgepflicht ergibt. Dazu zählt beispielsweise die Kommunikation über einen privaten Termin, der aus dienstlichen Gründen verschoben werden muss.
  Dazu zählt auch eine Mail an einen Einsender einer privaten E-Mail an die dienstliche E-Mail-Adresse mit der Bitte, künftig solche privaten E-Mails an die dienstliche Adresse zu unterlassen beziehungsweise alternativ dafür die private E-Mail-Adresse abcdefghi@jklmn.de zu benutzen.
  Es wird grundsätzlich empfohlen, bei allen dienstlichen E-Mails in der Absender-Signatur einen Hinweis aufzunehmen, dass es sich bei der absendenden E-Mail-Adresse um ein Postfach handelt, das nur für dienstliche E-Mails vorgesehen ist.

- Als dienstlich gilt der angemessene private Austausch am Arbeitsplatz, etwa das allgemeine Erkundigen nach dem Wohlbefinden, wie es auch bei Telefonaten üblich ist.
- Als dienstlich gilt **in sehr engen Grenzen** auch private Kommunikation, deren Erledigung in der Freizeit nicht möglich ist. Bei gleitender Arbeitszeit wird dies in der Praxis allerdings keine Bedeutung mehr haben.
- Kommunikation, die **weder objektiv noch subjektiv der Erfüllung der Arbeitspflicht** dient, ist **als privat zu werten**[1].
- E-Mail zwischen Gewerkschaft und Gewerkschaftsmitglied
  Eine klare Zuordnung privat / dienstlich ist in der Literatur nicht erkennbar. Daher wird die Zulässigkeit dieser Kommunikation in der Dienstvereinbarung (Ziffer 4.1) klargestellt, denn wegen der verfassungsrechtlich geschützten Koalitionsaufgaben und des unmittelbaren Zusammenhangs zur beruflichen Tätigkeit sind derartige Aktivitäten vom Arbeitgeber hinzunehmen. Die eigentliche Arbeitsleistung darf hierdurch allerdings nicht unzumutbar beeinträchtigt werden.

Zu den Regelungen im Einzelnen:

3.1 Es wird deutlich gemacht, dass Internetzugang und E-Mail grundsätzlich an jedem über das Landesnetz vernetzten PC-Arbeitsplatz zur Verfügung gestellt werden. Es soll verhindert werden, dass vom Angebot der privaten Nutzung nur diejenigen profitieren können, bei denen die dienstliche Notwendigkeit des Internetzugangs anerkannt worden ist und die deshalb damit ausgestattet worden sind („Dreiklassengesellschaft": MA ohne PC, MA mit PC, aber ohne Internet, MA mit PC und Internet und damit privater Internet-Nutzung). Vielmehr gilt als Grundsatz „Internet und E-Mail für alle".

Wenn die jeweils fachlich zuständige Stelle einzelne Arbeitsplätze in ihrem Verantwortungsbereich zur Nutzung der Dienste Internet / E-Mail nicht zulassen will, muss dies begründet und mit den jeweils zuständigen Vertretungsgremien abgestimmt werden. Ebenso ist die Ausgestaltung der örtlichen technischen Lösung (zum Beispiel Webbrowser an jedem Arbeitsplatz oder Webbrowser nur über Terminalserver) Aufgabe der jeweils fachlich zuständigen Stelle, die dabei

[1] Dabei wird man häufig aus dem Fehlen des objektiven Bezugs auf eine auch subjektive Privatnutzung schließen dürfen (ZfPR 5/2002, S. 152)

auch den Schutzbedarf ihrer sonstigen IT-Verfahren und Daten zu berücksichtigen hat.

Der Weg ins Internet geht für vernetzte PC-Arbeitsplätze der Landesverwaltung grundsätzlich über das Landesnetz und die zentrale Firewall bei Dataport (Standardanbindung). Alternative Verbindungswege ins Internet können aus Ermittlungsgründen oder Datenschutzgründen geboten sein, insbesondere bei Polizei, Verfassungsschutz, Steuerverwaltung. **PC-Arbeitsplätze mit von der Standardanbindung abweichender Internetanbindung unterliegen nicht den Regelungen dieser 59’er Vereinbarung.** Hierfür sind durch die zuständige und verantwortliche Stelle jeweils eigene Regelungen zu vereinbaren. Der Rahmen, den diese Regelung setzt, ist dabei soweit möglich zu beachten.

3.2 Diese Ziffer enthält den Grundsatz der Nutzung von Internet und E-Mail und entspricht den Grundgedanken der Gemeinsamen Geschäftsordnung der Ministerien (GGO). Die explizite Erwähnung soll der teilweise noch zu beobachtenden Tendenz zur unverhältnismäßigen Inanspruchnahme der Dienste entgegenwirken. Beschäftigte müssen in ihrer Vorgehensweise bei der Aufgabenerledigung die Nutzungsmöglichkeit von Internet und E-Mail einbeziehen, und zwar angemessen im Hinblick auf die jeweilige Aufgabenstellung. Damit wird klar, dass zum Beispiel stundenlanges dienstliches Surfen im Internet, wenn es aus der dienstlichen Aufgabenstellung nicht erforderlich oder nicht angemessen ist, unzulässig sein kann.

3.3 Es wird explizit klargestellt, dass der als Arbeitsmittel zur Verfügung gestellte E-Mail-Dienst nur zu dienstlichen Zwecken genutzt werden darf. Für privates Mailen wird später in Ziffer 3.5 auf die Nutzungsmöglichkeit eines Web-Mail-Kontos verwiesen.

3.4 Hier wird deutlich, dass die private Internetnutzung ein freiwilliges, nicht bindendes Angebot der Landesregierung an ihre Beschäftigten ist. Beschäftigte ihrerseits müssen dieses Angebot nicht nutzen. Die Landesregierung darf deshalb die Nutzung an einschränkende Bedingungen knüpfen.

Die Formulierung „soweit dienstliche Interessen nicht entgegenstehen" beinhaltet Einschränkungen auch in zeitlicher Hinsicht:
die Erfüllung der dienstlichen Aufgaben geht am Arbeitsplatz grundsätzlich den privaten Interessen vor. Ein großzügiges Nutzen der Arbeitszeit für private Internetaktivitäten (etwa komplettes Organisieren einer Urlaubsreise; …) lässt sich regelmäßig nicht mit dienstlichen Interessen in Einklang bringen. Hier müssen Beschäftigte sich auf Zeiten außerhalb der Arbeitszeit verweisen lassen.
Bei eiligen Arbeitsaufträgen kann zum Beispiel auch die Folge sein, dass Beschäftige in dieser konkreten Situation das Internet gar nicht privat nutzen dürfen, da dies zu einer vom Arbeitgeber nicht hinzunehmenden Verzögerung in der Aufgabenerledigung führen würde.
Eine zeitliche Einschränkung (etwa „in geringem zeitlichen Umfang", „in der Mittagspause" o.ä.) ist entbehrlich. Sie wird auch nicht aus steuerrechtlichen Gründen erforderlich, denn laut § 3 Nr. 45 EStG sind „die Vorteile des Arbeitnehmers aus der privaten Nutzung von betrieblichen Personalcomputern und Telekommunikationsgeräten" steuerfrei.
Die private Nutzung des Internetzugangs ist eingeschränkt auf das Nutzen von Web-Seiten, das heißt Anzeigen, ggf. Ausfüllen von Formularen. Damit ist nicht zulässig etwa privates Radiohören oder Fernsehen über den Internetzugang.

3.5 Private E-Mail über (kostenlose) Web-Mail-Dienste ist explizit zulässig.
Die private Nutzung des E-Mail-Dienstes wird nicht zugelassen. Dies wäre nur unter der Voraussetzung sinnvoll möglich, dass dienstliche und private Postfächer technisch getrennt würden. Das hätte doppelten Aufwand bei der Technik und der Systemadministration zur Folge und wäre daher nicht zu rechtfertigen. Ohne eine solche Trennung müssten allerdings alle E-Mails wie private E-Mail behandelt werden. Der Arbeitgeber dürfte etwa keine Regelungen für die dienstliche Nutzung der E-Mail erlassen und hätte keinerlei Zugangsmöglichkeit. Ausführliche Aussagen dazu enthält unter anderem die Veröffentlichung des ULD von November 2002 (siehe

http://www.datenschutzzentrum.de/material/themen/divers/wwwprivat.htm) und weitere (Orientierungshilfe E-Mail, Ausarbeitung der KBSt, des BfD, …). Detailliertere Ausführungen zum Fernmeldegeheimnis siehe unten: „Fernmeldegeheimnis bei der Nutzung von Internet und E-Mail - Erläuterungen". Für diese externe Mail-Nutzung ist der Arbeitgeber nicht „Anbieter" im Sinne des Telekommunikationsgesetzes und muss daher dafür nicht das Fernmeldegeheimnis wahren.

3.6 Es wird deutlich gemacht, dass das Angebot der privaten Nutzung widerruflich ist. Hier ist bewusst keine Zuständigkeit für einen solchen Widerruf festgelegt, da diese je nach Einzelfall verschieden sein kann. Die oder der Vorgesetzte kann zum Beispiel ihrem Mitarbeiter in einer konkreten Arbeitssituation mit hohem Zeitdruck die momentane private Internetnutzung untersagen.
Im Rahmen einer Disziplinarentscheidung kann das Recht zur privaten Nutzung für einzelne Beschäftigte von der oder dem zuständigen Dienstvorgesetzten widerrufen werden.
Wird umfangreicher Missbrauch in einem Verwaltungsbereich beobachtet, kann die Leitung dieses Verwaltungsbereichs die private Nutzung verbieten.

3.7 Die Nutzung von Internet und E-Mail im Rahmen der Vereinigungsfreiheit entsprechend Artikel 9 Grundgesetz wird hier für zulässig erklärt.
Die Nutzung von Internet und E-Mail in diesem Bereich wird weit überwiegend am Dienst- oder Arbeitsverhältnis orientiert sein und ist damit als dienstlich zu werten.
Damit dürfen Beschäftigte sich über Gewerkschaftsinformationen im Internet informieren, Gewerkschaften dürfen E-Mails an dienstliche E-Mail-Adressen senden usw. Eine unzumutbare Beeinträchtigung der eigentlichen Arbeitsleistung darf hierdurch allerdings nicht entstehen. Grenzen können auch durch allgemeine technische Erfordernisse gesetzt sein. Zum Beispiel dürfte eine gewerkschaftliche E-Mail an den Verteiler „Alle Beschäftigten der Landesverwaltung" wegen der zu erwartenden Mail-Belastung unzulässig sein. Entsprechend sind die Beschäftigten gehalten, in der dienstlichen

Kommunikation keine solchen Mails zu versenden (sondern dafür lieber das Intranet zu nutzen).

3.8 Die Einschränkung auf die „bedarfsgerechte" Schulung soll klarstellen, dass etwa bei Beschäftigten, die über die Dienste bereits gut informiert und in deren Nutzung geübt sind, eine Schulung in der Nutzung des Internet entbehrlich sein kann. Das gilt ebenso für die Risiken der Internetnutzung.

3.9 Die Zuständigkeit für die Kontrolle der Nutzung der Dienste ist entsprechend der Organisation der Landesregierung und damit entsprechend den jeweiligen Verantwortungsbereichen geteilt. Da Einzelheiten im Rahmen der Organisationshoheit von den Ressorts geregelt werden und sich verändern, können in der Richtlinie keine Einzelheiten festgelegt werden.
Das Finanzministerium als Betreiberin des Internetzugangs und E-Mail-Dienstes über die Firewall von Dataport und im Rahmen seiner Ressortübergreifenden IT- und Organisationszuständigkeit ist für eine pauschale Kontrolle der Nutzung der Dienste zuständig, die nicht nach den jeweiligen Ressorts differenziert. Als Finanzressort ist es außerdem zuständig zum Beispiel für die Kontrolle der Nutzung der Dienste im Bereich der Steuerverwaltung.

3.10 Die Verantwortung bezüglich der Sicherheit ist ebenfalls geteilt. Die Verantwortung des Finanzministeriums als Betreiberin des Internetzugangs und E-Mail-Dienstes über die Firewall von Dataport entbindet zum Beispiel lokal zuständige und verantwortliche Dienststellen nicht von der Notwendigkeit, stets aktuelle Virenschutzprogramme zu installieren, zu verhindern, dass auf den PC (schädliche) Programme unberechtigt zur Ausführung kommen können usw.

3.11 Diese Ziffer hat lediglich deklaratorischen Charakter, die erwähnten Vorschriften sind spezialrechtlich und außerdem höherwertiges Recht und gehen dieser Vereinbarung ohne weiters vor.

4 E-Mail

4.1 Hier wird der bisher teilweise schon bestehende grundsätzliche Vorrang der E-Mail gegenüber der Briefpost fortgeschrieben (z.B. Dienstanweisung für die Benutzung des elektronischen Postsystems MHS/X.400 im Innenministerium von 1995; wird durch diese Vereinbarung gegenstandslos).
Ein paralleler Versand in Papierform kann rechtlich geboten sein, aber auch sinnvoll zum Beispiel als Arbeitserleichterung für schwer behinderte Kolleginnen und Kollegen, etwa sehbehinderte Menschen, die besser mit Papier arbeiten können.

4.2 Hier wird nur ein Grundsatz normiert. Auch für die Sichtung des Posteingangs gilt das Prinzip der Aufgabenangemessenheit. Wer sehr zeitkritische Aufgaben zu erledigen hat, muss seine Post jeweils sofort sichten. Dies ist organisatorisch vor Ort festzulegen.

4.3 Aus dem Grundsatz, E-Mail wie eingehende Post zu behandeln, ergibt sich selbstverständlich, dass der Inhalt einer E-Mail bzw. ihrer Anhänge zur Akte zu nehmen ist. Ob und welche Inhalte der E-Mail jeweils (als Ausdruck) zu den Akten zu nehmen sind, ist in eigener Verantwortung zu entscheiden. Dies entspricht den Grundsätzen der Gemeinsamen Geschäftsordnung (GGO), siehe Ziffer 5.1.1.
Sobald in einem Verwaltungsbereich die elektronische Akte eingeführt worden ist (begleitet durch entsprechende organisatorische Regelungen), kann die E-Mail bzw. der Anhang unmittelbar zu eAkte genommen werden.
Die GGO regelt auch bereits die Informationspflichten zwischen Führungskräften und Mitarbeiterinnen und Mitarbeitern (insbesondere Ziffer 5.1.2 sowie Ziffer 5.2.2). Dies ist auch bei E-Mail-Kommunikation entsprechend anzuwenden.
Aus der Analogie zur Post ergibt sich ebenso selbstverständlich die folgende Verpflichtung: soweit der Inhalt einer eingehenden E-Mail zu seiner Wirksamkeit der Schriftform bedarf, ist die absendende Stelle unverzüglich darüber zu informieren und um Zusendung eines entsprechenden Schreibens zu bitten. Die Information kann telefonisch oder per E-Mail, natürlich auch schriftlich erfolgen.

Soweit im Schriftverkehr mit anderen Behörden oder mit Dritten Dokumente betroffen sind, bei denen durch Rechtsvorschrift eine Schriftform angeordnet ist, kommt eine Versendung durch E-Mail nur in Betracht, wenn die Voraussetzungen entsprechend den verwaltungsverfahrensrechtlichen Vorschriften (qualifizierte Signatur) erfüllt sind2.

Aus der Analogie zur Post ergeben sich weitere selbstverständliche Verhaltensnormen. Nachfolgend sind Beispiele dargestellt: E-Mail-Irrläufer werden baldmöglichst richtig zugestellt oder – falls das nicht möglich ist – der Absender über seinen Irrtum informiert. Insbesondere wird versehentlich erhaltene vertrauliche Post (Personalangelegenheiten, Kommunikation mit Funktionsträgern wie Personalvertretungen, Betriebsärztinnen, .-..) vertraulich behandelt.

4.4 Wer die „zuständige Stelle" ist, kann hier nicht allgemeingültig festgelegt werden, sondern muss lokal organisatorisch festgelegt werden, zum Beispiel im Sicherheitskonzept. Im Regelfall wird es die jeweilige IT-Leitstelle sein.

4.5 Hier ist implizit geregelt, dass innerhalb des Landesnetzes solche Post auch ohne Verschlüsselung versandt werden darf. Aus gegebener Veranlassung und soweit bei den Beteiligten die notwendigen Voraussetzungen vorhanden sind, kann aber auch verschlüsselt versandt werden.

Wenn ein Adressat dem Versand einer E-Mail mit ihn betreffenden schützenswerten Daten an ihn selbst auch ohne Verschlüsselung zugestimmt hat, ist dies zulässig.

Eine gesonderte Regelung für den Versand von dienstlichen Dateien auf den eigenen PC ist entbehrlich. Es gilt die 59'er Vereinbarung zur dienstlichen Nutzung privater PCs außerhalb der Diensträume von 1995 (Gl.-Nr.: 2015.2 Fundstelle: Amtsbl. Schl.-H. 1995 S. 513). Der Versand von dienstlichen Dateien auf den privaten PC nach Hause kann etwa im Rahmen von alternierender Telearbeit zulässig sein.

Personenbezogene Daten, die allgemein zugänglichen Quellen entnommen

[2] Gesetz zur Förderung der rechtsverbindlichen elektronischen Kommunikation im Verwaltungsverfahren vom 15.06.2004, in Kraft getreten am 25.06.2004

werden können, sowie Daten, die die Betroffenen selbst zur Veröffentlichung bestimmt haben, dürfen auch ohne Verschlüsselung elektronisch versandt werden, soweit schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden. Dies entspricht allgemeinen Datenschutzgrundsätzen.

5 Internet

5.1 Diese Regelung gilt für jede Internetnutzung (dienstlich oder privat) und dient unter anderem dazu, das Image der Landesregierung zu schützen, da der Aufruf von Internetseiten durch Beschäftigte der Landesregierung im Internet vielfältig bekannt werden kann. Seiten dürfen insbesondere nicht abgerufen werden, wenn sie

- gegen Strafrecht, Persönlichkeitsrecht, Urheberrecht oder Datenschutzrecht verstoßen beziehungsweise
- beleidigenden, verleumderischen, verfassungsfeindlichen, fremdenfeindlichen, sexistischen oder pornografischen Inhalt darstellen.

5.2 keine Erläuterungen dazu

5.3 Für die Internetnutzung im privaten Bereich empfehlen Datenschützer die Nutzung von so genannten Anonymisierungsdiensten. Diese verbergen die tatsächlich aufgerufenen Seiten. Die Nutzung solcher Dienste am Arbeitsplatz würde es dem Arbeitgeber erschweren oder sogar unmöglich machen zu erkennen, ob Beschäftigte das Internet in unzulässiger, sogar strafbarer Weise genutzt haben. Technisch kann die Nutzung solcher Dienste nicht verhindert werden, sie wird daher hier generell verboten.

5.4 Das Angebot der privaten Nutzung darf für den Arbeitgeber mit keinerlei Kosten oder personellem Aufwand verbunden sein. Daher ist mit dem Angebot der privaten Nutzung kein Anspruch auf Verfügbarkeit des Dienstes und Betreuung verbunden.

6 Protokollierung und Kontrolle

6.1 Es ist im Voraus klarzustellen, zu welchem Zeck Protokolldaten genutzt werden dürfen (Grundsatz der Zweckbindung bei der Erhebung von personenbezogenen Daten).
Die Einzelheiten der Protokollierung sind trotz ihrer elementaren Wichtigkeit für die Vereinbarung in Anlage 1 dargestellt. Die Anlagen haben keine andere Rechtsqualität als die Vereinbarung selbst (deren Bestandteil sie außerdem sind), sie sind nicht etwa eine „Vereinbarung zweiter Klasse". Durch das für die Anlagen vereinbarte erleichterte Änderungsverfahren soll lediglich dem Umstand Rechnung getragen werden, dass bestimmte Sachverhalte sich dynamisch verändern können müssen. Das gilt zum Beispiel auch für die Protokollierung. So kann aus Sicherheitsgründen kurzfristig ein anderes Protokollierungserfordernis entstehen.

6.2 Die konkrete Ausgestaltung dieser Regelung obliegt den jeweiligen Dienststellen. Eine analoge Anwendung etwa des Sicherheitsüberprüfungsgesetzes scheint allgemein nicht angemessen, da hier die Schwellen („streng geheim", „geheim" oder „VS-vertraulich", Gefahren für Leib und Leben) nicht vergleichbar sind, sondern kommt gegebenenfalls für Bereiche, deren Kommunikation besonders sensible Daten beinhalten kann (zum Beispiel Steuerdaten), in Betracht.

6.3 Hier werden Grundsätze für die Auswertungen der Protokolldaten festgelegt. Die Zuständigkeit dafür muss und kann hier nicht explizit festgelegt werden, da sie sich aus der Organisation der Landesregierung sowie der jeweiligen örtlichen Organisation ergibt.
So hätte etwa das Finanzministerium die Zuständigkeit für übergreifende Auswertungen der Protokolldaten sowie auch die Zuständigkeit für Auswertungen der Protokolldaten für den Bereich des Ministeriums oder der Steuerverwaltung.
Die Notwendigkeit, die Nutzung der Dienste angemessen zu kontrollieren, besteht unabhängig davon, ob private Nutzung zugelassen wird oder nicht. Auch wenn die Nutzung nur dienstlich zugelassen wird, muss der Arbeitgeber

sich darum kümmern, dass diese Regelung eingehalten wird und andernfalls geeignete Maßnahmen (organisatorisch, arbeitsrechtlich, disziplinarisch, …) ergreifen. Solche Maßnahmen sind mitbestimmungspflichtig.

6.4 Ein derartiges Verfahren muss örtlich festgelegt und bekannt gemacht werden. Werden im Rahmen der gezielten personenbezogenen Kontrolle keine weiteren Hinweise auf Verstöße festgestellt, ist das Verfahren zu beenden. In etwaigen späteren Verfahren sind alle Handlungsstufen erneut zu durchlaufen (Belehrung, Ankündigung der personenbezogenen Kontrolle, Einleitung der gezielten Kontrolle,...).

6.5 Welche dienst- oder arbeitsrechtlichen Maßnahmen im Einzelfall ergriffen werden müssen, kann in der Richtlinie nicht generell festgelegt werden. Die Umstände und Besonderheiten des Einzelfalles sind zu betrachten und es müssen jeweils angemessene Maßnahmen ergriffen werden.
So kann eine absichtliche, wiederholte unerlaubte Internetnutzung, die gleichzeitig einen Straftatbestand erfüllt, auch ohne vorausgegangene Abmahnung ein Kündigungsgrund sein. Dagegen wird die einfache unerlaubte private Nutzung der dienstlichen E-Mail in der Regel keine Kündigung rechtfertigen.
Zur weiteren Orientierung sind nachfolgend einige Leitsätze von (Landes-) Arbeitsgerichtsurteilen aufgeführt.
Bundesarbeitsgericht Urteil vom 7. Juli 2005 Az: 2 AZR 581/04
Auch wenn der Arbeitgeber die Privatnutzung nicht ausdrücklich verboten hat, verletzt der Arbeitnehmer mit einer intensiven zeitlichen Nutzung des Internets während der Arbeitszeit zu privaten Zwecken seine arbeitsvertraglichen Pflichten. Das gilt insbesondere dann, wenn der Arbeitnehmer auf Internetseiten mit pornographischem Inhalt zugreift. Diese Pflichtverletzung kann ein wichtiger Grund zur fristlosen Kündigung des Arbeitsverhältnisses sein. Ob die Kündigung in einem solchen Fall im Ergebnis wirksam ist, ist auf Grund einer Gesamtabwägung der Umstände des Einzelfalls festzustellen.
Landesarbeitsgericht Frankfurt 5. Kammer, Urteil vom 13. Dezember 2001,

Az: 5 Sa 987/2001 – Leitsatz
Ein Verstoß gegen das vom Arbeitgeber ausgesprochene Verbot privaten E-Mailverkehrs, das dem Virenschutz dienen soll, rechtfertigt grundsätzlich erst nach vorangegangener erfolgloser Abmahnung den Ausspruch einer Verhaltensbedingten außerordentlichen oder ordentlichen Kündigung.
Landesarbeitsgericht Niedersachsen 3. Kammer, Beschluss vom 26. April 2002, Az: 3 Sa 726/01 B – Orientierungssatz
Eine fristlose Kündigung aufgrund privaten Surfens im Internet ist auch ohne vorherige Abmahnung wirksam, wenn ein Arbeitnehmer nachweisbar während seiner Arbeitszeit Dateien mit pornografischen Inhalten aus dem Netz auf die Festplatte des betrieblichen PC herunterlädt. Dies gilt insbesondere dann, wenn eine vom Arbeitnehmer unterzeichnete Dienstanweisung verdeutlicht, dass der Arbeitgeber eine derartige private Nutzung nicht duldet.
Arbeitsgericht Frankfurt 2. Kammer, Urteil vom 2. Januar 2002, Az: 2 Ca 5340/01 – Orientierungssatz
Das Herunterladen und geordnete Speichern umfangreicher pornographischer Dateien ohne Genehmigung im Rahmen der Nutzung einer betrieblichen Datenverarbeitungsanlage und des Internetzuganges rechtfertigt eine ordentliche verhaltensbedingte Kündigung. Bei einem derartigen Vorgehen ist der Ausspruch einer Abmahnung entbehrlich.

6.6 Bezüglich der Auswertung von Protokolldaten (Nutzungs-, Verkehrs- und Inhaltsdaten) werden diejenigen Daten, die Beschäftigte in einer besonders zu schützenden Funktionen betreffen, besonders geschützt. Dies gilt nicht nur bezüglich den jeweiligen Funktionsträgerinnen oder Funktionsträgern selbst, sondern auch bezüglich denjenigen, die mit ihnen per E-Mail kommunizieren. Wie diesem Schutzinterese konkret Rechnung getragen wird, hat die jeweils zuständige Stelle zu entscheiden.

7 In-Kraft-Treten

keine Erläuterungen dazu

Schlussbestimmungen

Die Geltungsdauer der Vereinbarung ist unbefristet.
Die Vereinbarung und ihre Anlagen 1 und 2 werden im Intranet der Landesregierung (SHIP) und im Amtsblatt veröffentlicht werden. Zusätzlich zur Vereinbarung und ihren Anlagen werden dieses Erläuterungsdokument sowie die Firewall-Spezifikationen im Intranet veröffentlicht werden. Diese Dokumente werden laufend fortgeschrieben bzw. ergänzt, z.B. um häufige Fragestellungen und Anworten dazu usw.

Anlage 1 zur Richtlinie Internet und E-Mail - Erläuterung

Erläuterungen zu Anlage 1 sind entbehrlich.

Anlage 2 zur Richtlinie Internet und E-Mail - Erläuterung

Schulungsbausteine zur Nutzung von Internet und E-Mail

Angelehnt an Angebote von Dataport und der Datenschutzakademie werden hier mögliche Schulungsinhalte dargestellt. Diese beziehen sich nur auf die Dienste Internet und E-Mail. Weitere Funktionalitäten des E-Mail-Clients, zum Beispiel Kalenderfunktion, Aufgabenüberwachung oder künftig wahrscheinlich Verschlüsselung und PKI, sind hier nicht genannt, da die Nutzung dieser Funktionalitäten nicht Gegenstand dieser Vereinbarung ist.
Ergänzend wird auf die „Vereinbarung nach § 59 Mitbestimmungsgesetz Schleswig-Holstein Fortbildungskonzept für eine moderne Landesverwaltung (Fortbildungskonzept)“ verwiesen.

Fernmeldegeheimnis bei der Nutzung von Internet und E-Mail - Erläuterungen

1. **Ausschließlich dienstliche Nutzung**

   Gestattet der Arbeitgeber die Nutzung von Internet-Diensten ausschließlich zu dienstlichen Zwecken, ist er nicht Anbieter im Sinne des Telekommunikations- bzw. Teledienstesrechts. Die Erhebung und Verarbeitung von Daten über das Nutzungsverhalten der Beschäftigten richtet sich in diesen Fällen nach den einschlägigen Vorschriften des Beamtenrechts bzw. für Tarifbedienstete nach denen des Landesdatenschutzgesetzes (Orientierungshilfe zur datenschutzgerechten Nutzung von E-Mail und anderen Internetdiensten am Arbeitsplatz des Arbeitskreises "Medien" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom März 2002 – kurz: Orientierungshilfe).

2. Sobald ein Arbeitgeber seinen Beschäftigten die **private** Nutzung des Internetzugangs erlaubt, ist er Anbieter von Telediensten im Sinne des Telemediengesetzes – TMG (§ 11 Abs. 1 Nr. 1 TMG). Das TMG lässt die Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten aufgrund einer „anderen Rechtsvorschrift" (§ 12 Abs.1 und 2 in Zusammenhang mit Abs. 3) oder aufgrund einer Einzeleinwilligung zu. Die Zulässigkeit einer solchen Rechtsvorschrift ist dadurch begründet, dass die private Nutzung des Internetzugangs vom Arbeitnehmer in Anspruch genommen werden kann, aber nicht muss (eine Monopolstellung beim Angebot des jeweiligen Teledienstes würde eine solche Rechtsvorschrift verhindern).
   Durch eine solche Dienstvereinbarung oder alternativ durch Einwilligung im Einzelfall können die Beschäftigten auch im Hinblick auf die private Nutzung des Internet einer bestimmten stärkeren Kontrolle unterworfen werden. Dabei dürfen allerdings die Mindeststandards nicht unterschritten werden, die dem allgemeinen Datenschutzrecht und dem Persönlichkeitsrecht entstammen. Insbesondere sind die Grundsätze der Datensparsamkeit und Transparenz zu achten, und die Kontrolle hat datenschutzgerecht zu erfolgen.

   Beim Angebot der privaten Nutzung der dienstlichen E-Mail wäre der Arbeitgeber Anbieter von Telekommunikationsdiensten und müsste gegenüber den an der Telekommunikation Beteiligten das Fernmeldegeheimnis wahren. Eine Einschränkung dieses Schutzes ist seit der Neufassung des Telekommunikationsgesetzes im Juni 2004 nur aufgrund eines Gesetzes möglich, dabei müssen Telekommunikationsvorgänge ausdrücklich erwähnt werden („Zitiergebot").
   Da ein solches Gesetz nicht vorliegt und die Folgen der Erlaubnis der privaten E-Mail-Nutzung den Arbeitgeber in seinen ureigenen Interessen unverhältnismäßig einschränken würden (jede Mail wäre wie private Mail zu behandeln), bleibt nur das Beschränken der Nutzung des E-Mail-Dienstes auf die ausschließlich dienstliche Nutzung.

FAQ’s - Richtlinie zur Nutzung von Internet und E-Mail

Stand Dezember 2013

Verantwortlich: StK Z23/OE2

1. **Sind neben der Richtlinie noch andere Regelungen zu beachten?**
2. **Warum sind die in Anlage 1 der Richtlinie genannten Funktionalitäten zum Teil nicht nutzbar?**
3. **Ist die private Nutzung des dienstlichen E-Mail-Zugangs erlaubt?**
4. **Wann ist eine E-Mail privat veranlasst?**
5. **Ist die gewerkschaftliche Nutzung von Internet und E-Mail privat veranlasst?**
6. **Was muss ich beim Umgang mit dienstlicher E-Mail beachten?**
7. **Ist eine rechtssichere Kommunikation auf elektronischem Weg möglich?**
8. **Was muss ich im Umgang mit dienstlich relevanten SMS beachten?**
9. **Müssen alle erhaltenen und gesendeten E-Mails archiviert werden?**
10. **Wie ist bei eingehenden E-Mails mit zweifelhaftem Absender, Inhalt oder zweifelhaften Anlagen umzugehen?**
11. **Hat die Dienststelle das Recht, sich zu allen erhaltenen und gesendeten E-Mails Zugang zu verschaffen?**
12. **Sind dienstliche Downloads erlaubt?**
13. **Ist die private Nutzung des Internet-Zugangs erlaubt?**
14. **Ist die Nutzung eines Web-Mail-Dienstes erlaubt?**
15. **Ist Chatten erlaubt?**
16. **Ist Online-Banking erlaubt?**
17. **Warum wurde privates Radiohören und Fernsehen verboten, aber keine Aussage zur Nutzung von Podcasts und Streaming-Angeboten bei Online-Nachrichten (z.B. Spiegel etc.) oder allgemein YouTube, Clipfish, MSN, kicker getroffen?**
18. **Darf die Dienststelle die Nutzung der Dienste Internet und E-Mail untersagen?**
19. **Welche Verbote bestehen im Hinblick auf die Nutzung von Internet und E-Mail?**
20. **Was ist eine Firewall?**
21. **Werden Filter oder ähnliche Sperren an der Firewall eingesetzt?**

22. **Warum werden nicht zentral automatisierte Beschränkungen des Internets vorgenommen?**
23. **Wann müssen E-Mails mit vertraulichen Daten verschlüsselt werden?**
24. **Funktioniert der Abwesenheits-Assistent (MS Outlook) auch außerhalb des Landesnetzes?**
25. **Wird die Internet- und E-Mail-Nutzung protokolliert?**
26. **Welche Daten werden protokolliert?**
27. **Was ist die TOP-30-Statistik?**
28. **Wie lange werden die Protokolldaten aufbewahrt?**
29. **Ist der Datenschutz Täterschutz?**
30. **Warum wurde das „Schwarze Brett“ abgeschaltet?**
31. **Welche Regelungen sind durch Dienstvereinbarungen oder ggf. Dienstanweisungen zu treffen?**
32. **Welche Fortbildungs-/Schulungsangebote zum Umgang mit Internet und E-Mail gibt es?**
33. **Wie kann ich die Informationsflut am Arbeitsplatz managen?**
34. **Was muss ich beim Umgang mit sozialen Netzwerken (Social Media) beachten?**

1. Sind neben der Richtlinie noch andere Regelungen zu beachten?

Ja, denn die Regelungen der Richtlinie müssen durch die Dienststellen für ihren Zuständigkeitsbereich in entsprechenden Dienstanweisungen oder Dienstvereinbarungen präzisiert und ergänzt werden. Insofern bestehen weitere (lokale) Regelungen zur Internet- und E-Mail-Nutzung.

2. Warum sind die in Anlage 1 der Richtlinie genannten Funktionalitäten zum Teil nicht nutzbar?

Die Ausgestaltung der örtlichen technischen Lösung (zum Beispiel Webbrowser an jedem Arbeitsplatz oder Webbrowser nur über Terminalserver) ist Aufgabe der jeweils fachlich zuständigen Stelle, die dabei auch den Schutzbedarf ihrer sonstigen IT-Verfahren und Daten zu berücksichtigen hat. Durch die individuellen Bedürfnisse

der Dienststellen und lokalen Bedingungen bzw. Besonderheiten (z.B. Fachverfahren) können deshalb Einschränkungen erfolgen.
Aufschluss darüber muss die Dienstvereinbarung geben.

3. Ist die private Nutzung des dienstlichen E-Mail-Zugangs erlaubt?

Nein, der E-Mail-Zugang ist ausschließlich für dienstliche Zwecke zulässig.

Würde der Arbeitgeber seinen Beschäftigten die private Nutzung von E-Mail erlauben, wäre er Anbieter der Telekommunikationsdienstleistung „E-Mail“ und zur Einhaltung des Fernmeldegeheimnisses (§ 88 Telekommunikationsgesetz, TKG) verpflichtet. Dieses erstreckt sich auf die näheren Umstände der Kommunikation (Beteiligte, Verbindungsdaten etc.) und deren Inhalt mit der Folge, dass der Zugriff des Arbeitgebers auf sämtliche Nutzerdaten unzulässig wäre.
Der Arbeitgeber dürfte dann weder E-Mails lesen (auch nicht im Notfall, etwa bei Erkrankung des Mitarbeiters ohne dessen Zustimmung) und Verbindungsdaten speichern, noch Vorschriften über die Benutzung des E-Mail-Kontos (z.B. Sichtung zweimal täglich, Weiterleitung an Vertretung bei Abwesenheit, u.s.w.) erlassen.

Sofern das dienstliche E-Mail-Postfach trotz des Verbots private Post enthält, wird diese wie dienstliche Post behandelt.
Der Absender einer privaten E-Mail an ein dienstliches Benutzerkonto in einer Behörde muss sich darüber im Klaren sein, dass eine Kenntnisnahme durch Dritte z.B. durch den Arbeitgeber möglich ist. Die E-Mail darf aber nicht vom Arbeitgeber gelöscht werden. Es muss dem Empfänger die Möglichkeit gegeben werden, in geeigneter Weise darüber zu verfügen (selbst löschen oder Weiterleitung an private Mailadresse).

4. Wann ist eine E-Mail privat veranlasst?

Die Abgrenzung sollte in erster Linie am **Zweck der Kommunikation** ausgerichtet sein: „dienstlich“ ist jede die Arbeit fördernde Nutzung der Kommunikationsmittel (vgl. Abschnitt 3 der Erläuterungen zur Richtlinie).

5. Ist die gewerkschaftliche Nutzung von Internet und E-Mail privat veranlasst?

Die Nutzung von Internet und E-Mail im Rahmen der gewerkschaftlichen Vereinigungsfreiheit entsprechend Artikel 9 Grundgesetz gilt als dienstlich veranlasst (siehe auch die Erläuterungen zu Nr. 3.7 der Richtlinie).

6. Was muss ich beim Umgang mit dienstlicher E-Mail beachten?

Eingehende E-Mails sind wie eingehende Post zu behandeln.
Die Verfahren dazu sind beispielsweise in Dienstanweisungen, Dienstvereinbarungen oder Geschäftsordnungen, wie der Gemeinsamen Geschäftsordnung (GGO) oder der Geschäftsordnung der Finanzämter (FAGO) ausführlich geregelt (oder noch zu regeln).
Weitere Hinweise enthalten die Erläuterungen zu Nr. 4.3 der Richtlinie.

Hinweis: Die Arbeitsgruppe IT gestützte Verwaltungsarbeit hat im Auftrag des Kooperationsausschuss automatisierte Datenverarbeitung Bund/Länder/Kommunaler Bereich (KoopA ADV) ein Grundsatzpapier mit Empfehlungen zum Umgang mit E-Mails bei elektronischer Aktenführung erarbeitet (Grundsatzpapier "E-Mails in elektronischen Akten"; siehe SHIP Allgemeines/Organisation/Aktenordnung Aktenführung).

Für den Bereich der Landesverwaltung Schleswig-Holstein gibt es keine übergreifende Regelung zu den formalen Anforderungen beim Versand von E-Mails. Mitunter enthalten Dienstvereinbarungen/-anweisungen Vorschriften zum Inhalt und Stil dienstlicher E-Mails (z.B. konkreten Betreff formulieren, Ursprungstexte entfernen, Funktionsadressen vorrangig verwenden, Parallelversand vermeiden, auf Rechtschreibung/Schreibstil etc. achten, einheitliche Signaturen verwenden, u.s.w.).

7. Ist eine rechtssichere Kommunikation auf elektronischem Weg möglich und inwieweit ist bei elektronischer Kommunikation Vertraulichkeit gewährleistet?

Gemäß § 52a Landesverwaltungsgesetz Schleswig-Holstein (LVwG) ist die Übermittlung elektronischer Dokumente zulässig, soweit die Empfängerin oder der Empfänger (beide Seiten: Behörde und Bürger) hierfür einen Zugang eröffnet. In Fällen, in denen die schriftliche Form vorgeschrieben ist, muss das elektronische

Dokument mit einer qualifizierten elektronischen Signatur verbunden werden. In anderen Fällen ist eine elektronische Signatur grundsätzlich nicht erforderlich.

Einfache E-Mail Kommunikation erfüllt nicht alle Ansprüche an eine vertrauliche Kommunikation (E-Mail ist die „Postkarte im Internet“). Für eine geschützte elektronische Kommunikation in Schleswig-Holstein stehen der „Schleswig-Holstein-Service“ (Government-Gateway) und das Elektronische Verwaltungs- und Gerichtspostfach (EGVP) zur Verfügung. Bisher ist - mit Ausnahme bestimmter Fachverwaltungen - die vertrauliche, elektronische Kommunikation nur für Verwaltungsleistungen, die unter den Anwendungsbereich der EU-Dienstleistungsrichtlinie fallen, und nur über den Einheitlichen Ansprechpartner und die zuständigen Behörden (soweit diese den Zugang eröffnet haben) möglich.

8. Was muss ich im Umgang mit dienstlich relevanten SMS beachten?

Die Behandlung von SMS lässt sich aus den allgemeinen Regelungen über das Führen von Akten ableiten. Bei der in dienstlichem Zusammenhang erhaltenen SMS handelt es sich um eine Information, die nicht anders zu behandeln ist als anderweitig erlangte Informationen, beispielsweise mittels eines Telefongesprächs oder im Rahmen einer dienstlichen Besprechung. Der Empfänger der Information muss für seinen Bereich eigenverantwortlich entscheiden, ob der erhaltenen Information eine dienstliche Relevanz zukommt, so dass eine Aufnahme einer Notiz in den Akten zweckmäßig ist. Das kann beispielsweise durch einen (Akten)Vermerk geschehen.

9. Müssen alle erhaltenen und gesendeten E-Mails archiviert werden?

Für den Bereich der Landesverwaltung Schleswig-Holstein gibt es keine übergreifende Regelung, dass sämtliche E-Mails zu archivieren wären. Einzelne Dienststellen haben Regelungen hierzu für ihren Bereich zur Klarstellung in verwaltungsinterne Anweisungen aufgenommen.
Soweit nicht durch Verwaltungsvorschrift, Dienstanweisung oder sonstigen Handlungsanweisungen geregelt (z.B. GGO, FAGO, Aktenordnung für die schleswig-holsteinische Landesverwaltung (AktenO) vom 08.06.1999, Handlungsanweisung zur

Aktenführung und zum Umgang mit papiergestützten und elektronischen Informationen und Dokumenten im Finanzministerium vom 01.07.2003), sind eingehende und ausgehende E-Mails im Rahmen der Aktenführungspflicht zu werten und, sofern ihr Inhalt Aktenrelevanz hat, zu den Akten zu nehmen (soweit Papierakten geführt werden, in ausgedruckter Form, soweit elektronische Akten geführt werden, elektronisch).

Hinweis: Die Arbeitsgruppe IT gestützte Verwaltungsarbeit hat im Auftrag des Kooperationsausschuss automatisierte Datenverarbeitung Bund/Länder/Kommunaler Bereich (KoopA ADV) ein Grundsatzpapier zu Aktenrelevanz erarbeitet (Grundsatzpapier "Aktenrelevanz von Dokumenten "; www.koopa.de[2]; siehe auch im SHIP unter Allgemeines/Organisation/Aktenordnung Aktenführung).

10. Wie ist bei eingehenden E-Mails mit zweifelhaftem Absender, Inhalt oder zweifelhaften Anlagen umzugehen?

In diesem Fall ist **unverzüglich** die zuständige Stelle (IT-Stelle, Sicherheits-management) zu informieren. Wer diese Aufgabe wahrnimmt, ist in der jeweiligen Dienstelle zu klären und in der (lokalen) Dienstvereinbarung festzulegen.

11. Hat die Dienststelle das Recht, sich zu allen erhaltenen und gesendeten E-Mails Zugang zu verschaffen?

Die Dienststelle hat - unter Beachtung bestimmter Verfahrensregeln - das Recht, sich alle erhaltenen oder gesendeten E-Mails vorlegen zu lassen.

Der Arbeitgeber darf stichprobenartig prüfen, ob das Surfen bzw. E-Mail-Versenden dienstlicher Natur ist. Ein- und ausgehende E-Mail darf gleichermaßen zur Kenntnis genommen werden wie übriger dienstlicher Schriftverkehr. Vorgesetzte könnten auch verfügen, dass ihnen die Mitarbeiterinnen und Mitarbeiter jede ein- und ausgehende E-Mail einzeln zur Kenntnisnahme zuleiten.
(Die Kontrolle der Vollständigkeit könnte durch entsprechende Protokollierung erfolgen. Diese Protokollierung und der Umgang mit den Protokollinformationen müssen vorher in einer Dienstvereinbarung festgelegt werden.)

12. Sind dienstliche Downloads erlaubt?

[1] abgelöst durch IT-Planungsrat
[2] abgelöst durch IT-Planungsrat

Soweit in Dienstvereinbarungen und -anweisungen nichts anderes geregelt ist und kein Sicherheitsrisiko besteht, sind dienstlich veranlasste, kostenfreie Downloads zulässig. In anderen Fällen ist eine Erlaubnis der Administration und der/des Vorgesetzten einzuholen.
Inwieweit die Erzeugung/Speicherung von privaten Dateien auf dem Arbeitsplatz-Computer zulässig ist, ist üblicherweise in lokalen Regelungen fest gelegt.

13. Ist die private Nutzung des Internet-Zugangs erlaubt?

Die Richtlinie gibt Rahmenbedingungen vor, nach denen eine private Nutzung erlaubt ist. Diese müssen durch (lokale) Dienstvereinbarungen konkretisiert werden. Grundsätzlich muss die Nutzung des Dienstes eigenverantwortlich und angemessen erfolgen, darf dienstlichen Interessen nicht entgegenstehen und nicht dem Ansehen schaden bzw. verbotene Inhalte betreffen (siehe auch Nr. 3 und 5 der Richtlinie zur Nutzung von Internet und E-Mail und die Erläuterungen dazu).

Die Frage, wo die Grenzen der privaten Nutzung liegen und inwieweit diese dienstlichen Interessen nicht entgegensteht, unterliegt ressortspezifischen Gegebenheiten, ist z.T. einzelfallabhängig und kann nicht durch die Richtlinie übergreifend und abschließend getroffen werden. Zeitliche oder sonstige (z.B. inhaltliche) Vorgaben bzw. Einschränkungen der Internetnutzung, die über den Regelungsbereich nach Nr. 3 und 5 der Richtlinie hinaus gehen, können nicht durch eine Rahmenrichtlinie festgelegt werden und sind bei entsprechender Notwendigkeit ressort- bzw. dienststellenspezifisch in den jeweiligen Dienstvereinbarungen zu regeln.

14. Ist die Nutzung eines Web-Mail-Dienstes erlaubt?

Die Nutzung eines (kostenlosen) Web-Mail-Dienstes für private E-Mail ist eine private Internetnutzung und insofern zulässig, soweit dienstliche Interessen nicht entgegenstehen (siehe Nr. 14).
Konkrete Festlegungen oder Einschränkungen zeitlicher und inhaltlicher Art müssen ggf. durch die Dienststelle in der jeweiligen Dienstvereinbarung erfolgen.

15. Ist privates Chatten erlaubt?

Soweit die lokale Dienstvereinbarung nicht konkrete Regelungen enthält, gelten die allgemeinen Grundsätze (vgl. 3.4 der Richtlinie sowie Abschnitt 3 der Erläuterungen zur Richtlinie): die Aktivitäten dürfen dienstlichen Interessen nicht entgegenstehen.

16. Ist Online-Banking erlaubt?

Soweit die Dienstvereinbarung nicht konkrete Regelungen enthält, gelten die allgemeinen Grundsätze (vgl. 3.4 der Richtlinie sowie Abschnitt 3 der Erläuterungen zur Richtlinie): die Aktivitäten dürfen dienstlichen Interessen nicht entgegenstehen.
Da mit dem Angebot der privaten Nutzung kein Anspruch auf Verfügbarkeit des Dienstes und Betreuung verbunden ist, übernimmt der Arbeitgeber bei etwaigem Schadenseintritt keine Haftung!

17. Warum wurde privates Radiohören und Fernsehen verboten, aber keine Aussage zur Nutzung von Podcasts und Streaming-Angeboten bei Online-Nachrichten (z.B. Spiegel etc.) oder allgemein YouTube, Clipfish, MSN, kicker getroffen?

Detailregelungen zur Internetnutzung sind in einer Rahmenrichtlinie nicht umsetzbar und vor allem durch die dynamische Entwicklung im Bereich der Internetdienste auch nicht praktikabel.
Privates Radiohören und Fernsehen ist insbesondere aus technischen Gründen (Belastung des Landesnetzes), aber auch unter Berücksichtigung anderer Aspekte, z.B. Beeinträchtigung anderer Mitarbeiterinnen und Mitarbeiter, nicht im dienstlichen Interesse.
Soweit für andere Internetdienste eine Vergleichbarkeit gegeben ist, kann in analoger Anwendung entschieden werden, anderenfalls gelten die allgemeinen, durch die Richtlinie festgelegten Grundsätze. Über die Zulässigkeit der privaten Nutzung etwa von Streamingangeboten kann, sofern erforderlich, die jeweilige Dienststelle ausdrückliche Festlegungen treffen. Nach den Feststellungen im Evaluationsbericht ist die konkrete Ausgestaltung der Internetnutzung ressort- bzw.

dienststellenspezifisch durch die einzelnen Dienststellen vorzunehmen.
Zum Umgang mit sozialen Netzwerken, siehe Nr. 34.

18. Darf die Dienststelle die Nutzung der Dienste Internet und E-Mail untersagen?

Wenn Dienstvorgesetzte einzelne Arbeitsplätze in ihrem Verantwortungsbereich von der generellen oder privaten Nutzung der Dienste Internet / E-Mail ausschließen wollen, muss dies begründet und mit den jeweils zuständigen Vertretungsgremien abgestimmt werden.

19. Welche Verbote bestehen im Hinblick auf die Nutzung von Internet und E- Mail?

Die Richtlinie zur Nutzung von Internet und E-Mail sieht folgende Einschränkungen und Verbote vor (Einzelheiten sind durch Dienstvereinbarung oder -anweisung festzulegen):

- die private Nutzung des Internet darf dienstlichen Interessen nicht entgegenstehen
- für private E-Mail ist ein (kostenloser) Web-Mail-Dienst zu nutzen
- Verbote nach Nr. 5.1- 5.3 der Richtlinie.

Die private Nutzung ist ferner eingeschränkt auf die Benutzung von Webseiten (Dienste http/https).

Die Nutzung des dienstlichen E-Mail-Benutzerkontos für private E-Mail ist unzulässig.

20. Was ist eine Firewall?

Die Dataport Firewall schützt das Landesnetz Schleswig-Holstein, an das die Dienststellen der Landesverwaltung sowie große Teile der kommunalen Verwaltung angeschlossen sind. Die Firewall besteht aus einem sorgfältig ausgewählten System von Hard- und Software, das auf verschiedenen Netzwerkebenen wirkt und bietet einen geschützten und schützenden Zugangspunkt des Landesnetzes zum Internet.

Weitere Informationen enthält die Leistungsbeschreibung „Internet-Zugang für die unmittelbare Landesverwaltung Schleswig-Holstein über den Dataport Firewall Altenholz“ (verfügbar unter SHIP/Allgemeines/Informationstechnik/IT-Regelungen). Die Vereinbarung nach § 59 MBG „Richtlinie zur Nutzung von Internet und E-Mail" enthält u.a. Regelungen zu Art, Umfang und Verwendung der an der Firewall protokollierten Daten.

21. Werden Filter oder ähnliche Sperren an der Firewall eingesetzt?

Das Firewall-System besteht aus mehreren Komponenten: einem externen und internen Paketfilter sowie Proxies (Ersatzdienste), die auf Bastion-Hosts („Servern“) ablaufen. Diese schützen das Netz von Dataport und die Teilnehmernetze am Landesnetz Schleswig-Holstein durch Einschränkungen der Verbindungen vom und zum Internet auf zulässige Dienste anhand von Kommunikationsbedingungen (z.B. die Einschränkung auf bestimmte IP-Adressen für Zielrechner einer Verbindung). Im Rahmen des Sicherheitsmanagements wird fortlaufend Angriffen aus dem Internet entgegengewirkt. Weitere Informationen enthält die Leistungsbeschreibung "Internet-Zugang für die unmittelbare Landesverwaltung Schleswig-Holstein über den Dataport Firewall Altenholz“ (verfügbar unter SHIP/Allgemeines/Informationstechnik/IT-Regelungen).

Die sicherheitstechnischen Rahmenbedingungen, das Schutzniveau und die protokollierten Informationen sind im Sicherheitskonzept der Dataport-Firewall festgelegt.

Das Firewall-System bietet für elektronische Post ebenfalls Schutz vor der Übertragung gefährlicher Daten durch Inhalte-Filterung (z.B. Viren-Scanner, SPAM-Filter). Die Leistungen des "E-Mail-Filters" sind in der Leistungsbeschreibung "Inhalte-Filterung von E-Mails für die unmittelbare Landesverwaltung Schleswig-Holstein am Dataport Firewall in Altenholz“ dargestellt (SHIP/Allgemeines/Informationstechnik/IT-Regelungen).

Der Einsatz von Contentfiltern oder die Sperrung unzulässiger Webseiten und/oder E-Mails erfolgt nicht. Unter Berücksichtigung von fachlichen Gesichtspunkten sowie

der bestehenden arbeits- und disziplinarrechtlichen sowie organisatorischen Regelungen (Dienstvereinbarungen), einer am Prinzip der Vertrauenskultur orientierten Bereitstellung der Dienste und unter Beachtung wirtschaftlicher Aspekte besteht derzeit keine Notwendigkeit dafür.

22. Warum werden nicht zentral automatisierte Beschränkungen des Internets vorgenommen?

Der Internetzugang ist ein Arbeitsmittel, welches an allen PC-Arbeitsplätzen zur Verfügung stehen soll und zu dienstlichen und privaten Zwecken genutzt werden kann. Durch die liberale Ausgestaltung der ressortübergreifend geltenden Regelungen wird den Anforderungen an einen modernen, zur Aufgabenbewältigung geeigneten Arbeitsplatz und an eine standardisierte IT-Servicelandschaft Rechnung getragen.
Landeseinheitliche Einschränkungen würden alle Nutzerinnen und Nutzer (= Arbeitsbereiche) gleichermaßen betreffen, sich nicht nur auf die private, sondern auch auf die dienstliche Internetnutzung auswirken und ressortspezifische Gegebenheiten/Erfordernisse nicht berücksichtigen.

23. Wann müssen E-Mails mit vertraulichen Daten verschlüsselt werden?

Ist der berechtigte Empfänger innerhalb des Landesnetzes oder über ein sicher gekoppeltes anderes Verwaltungsnetz zu erreichen, kann die E-Mail ohne weiteres versendet werden.

Wird die E-Mail mit vertraulichem Inhalt oder mit personenbezogenen Daten an einen berechtigten Empfänger außerhalb des Landesnetzes verschickt, so muss eine Verschlüsselung erfolgen. Eine Public-Key-Infrastruktur steht nicht zur Verfügung. Die Inhalte müssen als Anlagen beigefügt werden, die durch die Funktionen der entsprechenden Anwendungsprogramme (z.B. Verschlüsselung durch Kennwortvergabe) geschützt werden.

Voraussetzung für den Versand verschlüsselter E-Mails ist außerdem, dass die Empfängerin oder der Empfänger zur Entschlüsselung der elektronischen Post in der Lage ist.
Alternativ kann ggfs. eine Kommunikation über den Schleswig-Holstein Service (Government Gateway) oder das Elektronische Gerichts. und Verwaltungspostfach (EGVP) erfolgen (siehe auch Nr. 8).

24. Funktioniert der Abwesenheits-Assistent (MS Outlook) auch außerhalb des Landesnetzes?

Die externe Abwesenheitsbenachrichtigung steht künftig für alle Arbeitsplätze der „+1-Infrastruktur“ bereit.
Grundsätzlich wird von Abwesenheitsbenachrichtigungen nach außen abgeraten. Sollen diese dennoch erfolgen, wird folgender Text empfohlen:
„Leider bin ich zurzeit nicht erreichbar. Ihre E-Mail wird (/wird nicht) weitergeleitet. In dringenden Fällen benutzen Sie bitte das folgende (/unser) Posteingangsfach Behörde123@behörde.landsh.de.“

25. Wird die Internet- und E-Mail-Nutzung protokolliert?

Entsprechend Nr. 6 der Richtlinie werden zu den dort bestimmten Zwecken bestimmte Protokollinformationen auf den zentralen Servern der Firewall festgehalten. Daneben erfolgt auf lokalen Servern und Arbeitsplatzrechnern eine Datenspeicherung und Datensicherung (nicht Gegenstand Richtlinie, aber in den lokalen Dienstvereinbarungen darzustellen und zu regeln).

26. Welche Daten werden protokolliert?

Einzelheiten der Protokollierung an der Firewall (Art, Umfang, Anonymisierung, Aufbewahrung) sind in Anlage 1 der Richtlinie in der jeweils aktuellen Fassung festgelegt.
Die Protokollierung auf lokalen Servern und Arbeitsplatzrechnern ist in lokalen Dienstvereinbarungen festzulegen.

27. Was ist die TOP-30-Statistik?

Die so genannten TOP 30-Statistiken sind anonymisierte Landes- bzw. Ressortstatistiken. Sie liefern Anhaltspunkte über Art und Umfang der Nutzung der Dienste, etwaige Auffälligkeiten sowie Entwicklungen und Tendenzen der Internetnutzung.

Die Ressorts erhalten monatlich Auswertungen über die 30 am häufigsten aufgerufenen Internetseiten und über die 30 Internetseiten mit den höchsten Downloadmengen. Bei "Auffälligkeiten" können die Ressorts bei Dataport erfragen, aus welchem organisatorischen Bereich (z.B. Ministerium, nachgeordnete Behörde X,...) die Zugriffe kommen.

Das Recht auf informationelle Selbstbestimmung verbietet die verdachtslose (ggf. automatisierte) Vollkontrolle. Entsprechend anonymisiert sind die Darstellungen in der TOP-30-Statistik. Die TOP-30-Statistik kann aber Anhaltspunkte/Hinweise auf Verstöße gegen die Richtlinie liefern und somit eine anlassbezogene Überprüfung und die Einleitung des personenbezogenen Kontrollverfahrens rechtfertigen.

28. Wie lange werden die Protokolldaten aufbewahrt?

Die Speicherdauer der Protokolldaten der Firewall beträgt in der Regel 10 Tage. Abweichungen erfolgen im Rahmen des Kontrollverfahrens nach Nr. 6.4 der Richtlinie.
Die Speicherdauer der lokalen Protokolldaten ist in Dienstvereinbarungen festzulegen.

29. Ist der Datenschutz Täterschutz?

Nein.
Der Datenschutz dient dem Schutz der Grundrechte. Der Datenschutz gewährleistet, dass Daten entweder unverzüglich anonymisiert und gelöscht oder nur zu bestimmten Zwecken genutzt werden und dient damit dem Schutz unschuldiger Menschen.

Wer die einzelne unzulässige Handlung in den Mittelpunkt stellt, ignoriert, dass die Nachteile einer Totalprotokollierung deren Nutzen bei weitem überwiegen.
Selbst die dadurch angestrebte vollständige Ahndung der Einzelfälle rechtfertigt keine unverhältnismäßigen Maßnahmen. Ihr Nutzen steht außer Verhältnis zu ihren negativen Auswirkungen.
Eine (automatisierte) Vollkontrolle würde zudem die Mitarbeiterinnen und Mitarbeiter unter Generalverdacht stellen. Zum Schutz Unbeteiligter müssen Grundrechte und Verhältnismäßigkeit stets gewahrt bleiben.

30. Warum wurde das „Schwarze Brett“ im SHIP abgeschaltet?

Das Schwarze Brett bot den Beschäftigten die Möglichkeit, Dinge zu verschenken, zum Kauf anzubieten oder zu suchen, vergleichbar mit Kleinanzeigen in Tageszeitungen.
Bei Nutzung dieses Angebots waren bestimmte Hinweise zu beachten, die als so genannte "Spielregeln" im SHIP veröffentlicht wurden. Im Laufe der Zeit häuften sich leider die Verstöße gegen diese Spielregeln und erzeugten erheblichen Arbeitsaufwand. Das Schwarze Brett wurde im August 2003 abgeschaltet. Die Prüfung der Realisierungsmöglichkeiten hat ergeben, dass eine erneute Inbetriebnahme nur mit finanziellem und personellem Aufwand erfolgen kann, der unter den herrschenden Personaleinsparvorgaben nicht zu rechtfertigen ist.

31. Welche Regelungen sind durch Dienstvereinbarungen oder ggf. Dienstanweisungen zu treffen?

Das Dokument „Erläuterungen zur Richtlinie, Stand 01.01.2010“ enthält unter Tz. 2 (Umfang) Beispiele der regelungsbedürftigen Aspekte.
Den Beschäftigten müssen die Möglichkeiten des Kontrollpotenzials und Kenntnisse der Funktionsweise der IT-Komponenten offen gelegt werden.
Dienstvereinbarungen müssen deshalb insbesondere die Protokollierung auf lokaler Ebene, ferner das Verfahren der Missbrauchs- und personenbezogenen Kontrolle regeln.

Hinsichtlich der Datenspeicherung und Datensicherung auf lokalen Systemkomponenten, wie Servern, Proxy-Servern oder Arbeitsplatzrechnern ist u.a. festzulegen:

- welche Daten gesichert bzw. nicht gesichert werden
- wann die Sicherung erfolgt
- wie oft gesichert wird.

Entsprechend den Vorgaben des Datenschutzes sind die Rahmenvorgaben zum Kontrollverfahren durch die Richtlinie definiert. Diese müssen in den Ressorts weiter konkretisiert werden. Die Dienststellen müssen z.B. unter Beachtung datenschutzrechtlicher Bestimmungen und zusammen mit der Personalvertretung Verfahren zur (personalisierten Kontrolle) in eigener Zuständigkeit festlegen und bekannt geben.

Weitere Regelungen können zum Umgang mit elektronischer Post (E-Mail-Management) bzw. der Nutzung von MS Outlook und hinsichtlich der privaten Internetnutzung erfolgen.

32. Welche Fortbildungs-/Schulungsangebote zum Umgang mit Internet und E-Mail gibt es?

Die Ermittlung des Fortbildungsbedarfs und die Organisation des Fortbildungsangebotes sind Bestandteil des Fortbildungskonzeptes.
Die Anlage 2 der Richtlinie zur Nutzung von Internet und E-Mail sieht verschiedene Schulungsbausteine zur Nutzung von Internet und E-Mail vor, die bedarfsabhängig angeboten wurden bzw. werden.
In 2010 stehen den Mitarbeiterinnen und Mitarbeitern der Landesverwaltung u.a. folgende Fortbildungsangebote zur Verfügung: Outlook XP/2003 für Profis (KOMMA Seminarprogramm 2010), Outlook 2007- Informationsflut managen/Effizienter Arbeiten-Workshop (Dataport) und weitere unter SHIP/Allgemeines/Personal/ Fortbildung.

33. Wie kann ich die Informationsflut am Arbeitsplatz managen?

1. Machen Sie sich - ggf. unterstützt durch die Administration vor Ort - mit den Funktionalitäten von Internet und E-Mail vertraut.
2. Prüfen Sie, ob vielleicht Such- und Filterfunktionen das Sortieren von E-Mails erleichtern können. Überlegen Sie für Ihren Arbeitsplatz die Umstellung auf elektronische Aktenführung.

Beispiel: Der E-Mail-Filter im Firewall-System verfügt über einen SPAM-Test und markiert die betreffende E-Mail, indem dem Betreff die Zeichenkette„{SPAM}“ vorangestellt wird. Das E-Mail-Programm könnte beispielsweise so konfiguriert werden, dass alle E-Mails mit dieser Zeichenkette am Anfang des Betreffs in einen speziellen Ordner gelegt und nach wenigen Tagen automatisch gelöscht werden.

3. Sortieren Sie beim ersten Lesen vor. (Was ist wichtig oder unwichtig/ dringend oder hat Zeit/ kann gelöscht werden?)

Beispiel: Aktenrelevante E-Mails werden in elektronischen Akten abgelegt und sind dort leicht wieder zu finden, nicht-aktenrelevante E-Mails werden kurzfristig gelöscht.

4. Bestellen Sie verzichtbare Informationen ab oder prüfen Sie, welchen Verteilern Sie angehören und inwieweit dies notwendig ist.
5. Klären Sie Angelegenheiten mündlich anstelle des Austausches per E-Mail.
6. Legen Sie feste Zeiten für Routinearbeiten, z.B. die Sichtung der E-Mail-Eingänge fest und planen Sie Zeitpuffer in Ihren Tagesablauf ein, um auf unvorhergesehene Ereignisse reagieren zu können.
7. Nutzen Sie Fortbildungsangebote, die dabei helfen, den Büroalltag zu managen, den Arbeitsplatz zu optimieren und den effektiven Umgang mit Informationen zu erlernen. Diese finden Sie z.B. im SHIP (Allgemeines/Personal/Fortbildung) oder im AIS (Themen/Aus- und Fortbildung).

34. Was muss ich beim Umgang mit sozialen Netzwerken (Social Media) beachten?

Soziale Medien sind internetbasierte mediale Angebote, die auf sozialer Interaktion, nutzergenerierten Inhalten und den technischen Möglichkeiten des Web 2.0 basieren. Sie dienen der Kommunikation, Zusammenarbeit und dem Wissensmanagement. Einsatz finden können u. a. Blogs, Foren, Microblogging-Dienste wie etwa Twitter, soziale Netzwerke wie z.B. Facebook, Wikis wie Wikipedia, Video- und Bilderportale wie z.B. YouTube sowie Portale zum Austausch von

Medien.[3]Eine dienstliche Nutzung sozialer Medien – über die bestehenden Aktivitäten der Presse- und Informationsstelle der Landesregierung, der Pressestellen der Ministerien und deren Online-Redaktionen hinaus - ist gegenwärtig nicht vorgesehen.
Auch für die private Nutzung der sozialen Netzwerke gelten die allgemeinen Regelungen der Internetrichtlinie (ergänzt durch Dienstanweisungen/-vereinbarungen der Dienststellen) sowie die anerkannten Verhaltensregeln der öffentlichen Verwaltung. Die allgemeinen dienst- und arbeitsvertraglichen Pflichten sowie die Pflichten im Beamtenrecht und vergleichbaren Regelungen in den Tarifverträgen sind auch bei der Kommunikation in sozialen Netzwerken zu beachten. Selbstredend dürfen Amts- und Behördengeheimnisse, personenbezogene Daten oder Daten aus laufenden Verwaltungsverfahren nicht veröffentlicht werden; auch sind unwahre, beleidigende oder diskriminierende Äußerungen, insbesondere in Bezug auf andere Mitarbeiter und auf Führungskräfte nicht erlaubt.

Im Rahmen eines eigenverantwortlichen, bewussten privaten Umgangs sollte Folgendes beachtet werden:

- Ihre Äußerungen erfolgen ausschließlich als Privatperson und sind als persönliche/private Meinung zu kennzeichnen (in der ersten Person kommunizieren: „ich“ statt „wir“). Die Offenlegung von Einzelheiten Ihres Beschäftigungsverhältnisses und Ihrer Funktion in der Dienststelle ist nicht erlaubt. Ebenso wenig darf ein Verweis auf den offiziellen Auftritt der Dienststelle im jeweiligen sozialen Netzwerk aufgenommen werden.
- Argumentieren Sie immer sachlich und gehen Sie respektvoll mit anderen Diskussionsbeteiligten um; lassen Sie sich auch in hitzigen Debatten nicht zu unbedachten Äußerungen hinreißen.
- Beachten Sie bei Ihren Beiträgen gesetzliche Vorgaben wie z.B. Datenschutz, Urheber-und Markenrecht (z.B. Verweis auf fremde Inhalte mittels Link, keine Kopien fremden Materials).
- Bei Anfragen (z.B. von Seiten der Medien), die den dienstlichen Bereich betreffen, sind die vorhandenen Regelungen zu beachten. So werden Medienanfragen üblicherweise von der Pressestelle bearbeitet. Dies gilt auch für eventuelle negative oder positive Beiträge über Ihre Dienststelle.
- Beachten Sie die Nutzungsbedingungen der Netzwerke sowie sonstige Regeln der Communities/sozialen Plattformen.

[3] Lorenz-von-Stein-Institut: „Social Media Guidelines – Web 2.0 in der deutschen Verwaltung“

- Hinweise zur sicheren Verwendung von sozialen Netzwerken bietet das Bundesamt für Sicherheit in der Informationstechnik (www.bsi.bund.de) an.

Service Level Agreement

Internet E-Mail SH

Version: 1.2
Stand: 2.12.2015

Inhaltsverzeichnis

1 Einleitung

1.1 Aufbau des Dokumentes

Diese Anlage enthält die folgenden Kapitel:

Rahmenbedingungen (Kapitel 2): Regelung von allgemeinen Rechten und Pflichten von Auftraggeber und Dienstleister, Bestimmungen zur Laufzeit, Änderung bzw. Kündigung der Vereinbarung sowie Übergangsbestimmungen.

Leistungsbeschreibungen (Kapitel 3): Inhaltliche Beschreibung der bereitgestellten Leistungen sowie der für einen reibungslosen Betrieb erforderlichen Dienstleistungen.

1.2 Leistungsgegenstand

Gegenstand dieses Service Level Agreements ist die Leistung Internet-E-Mail SH.

Die Leistungen werden hinsichtlich der Leistungsqualität und des Leistungsumfangs im Kapitel 3 beschrieben.

2 Rahmenbedingungen

2.1 Mitwirkungsrechte und –pflichten

Die vom Auftragnehmer zugesagten Leistungen erfolgen auf Anforderung des Auftraggebers. Es sind Mitwirkungs- und Bereitstellungsleistungen des Auftraggebers erforderlich. Der Auftraggeber muss folgende Daten liefern und aktuell halten:

- Name und E-Mail-Adresse des IT-Verantwortlichen, der berechtigt ist, Einstellungen des E-Mail-Filters zu verändern bzw. zu beauftragen. Aktualisierungen senden Sie bitte an DataportFirewallSH@dataport.de
- Nennung der zum E-Mail-Versand genutzten Domains und Mailserver-IP-Adressen
- Aktivierung der Empfänger-Validierung am Kunden-Mailserver (wird empfohlen)

2.2 Ansprechpartner

2.2.1 Störungsbearbeitung

Bei technischen Störungen wenden Sie sich bitte an das Dataport-Callcenter unter der Rufnummer 0431/3295-444 und lassen Sie dort einen Incident generieren.

Störungsannahme: Montag bis Freitag von 6:30 – 18:00 Uhr

Betriebszeit: Montag bis Donnerstag von 8:00 – 17:00 Uhr, Freitag von 8:00 – 15:00 Uhr

Kann die Störungsbehebung nicht innerhalb der normalen Bearbeitungszeit beendet werden, so wird die Bearbeitung am nächsten Werktag (Mo-Fr) fortgesetzt.

2.2.2 Technischer Ansprechpartner

Bei technischen Fragen zum Produkt wenden Sie sich bitte an DataportFirewallSH@dataport.de

2.2.3 Vertraglicher Ansprechpartner

Bei vertraglichen Fragen zum Produkt wenden Sie sich bitte an
DataportKundenbetreuungundVertrieb@dataport.de

3 Leistungsbeschreibung

3.1 E-Mail Transport

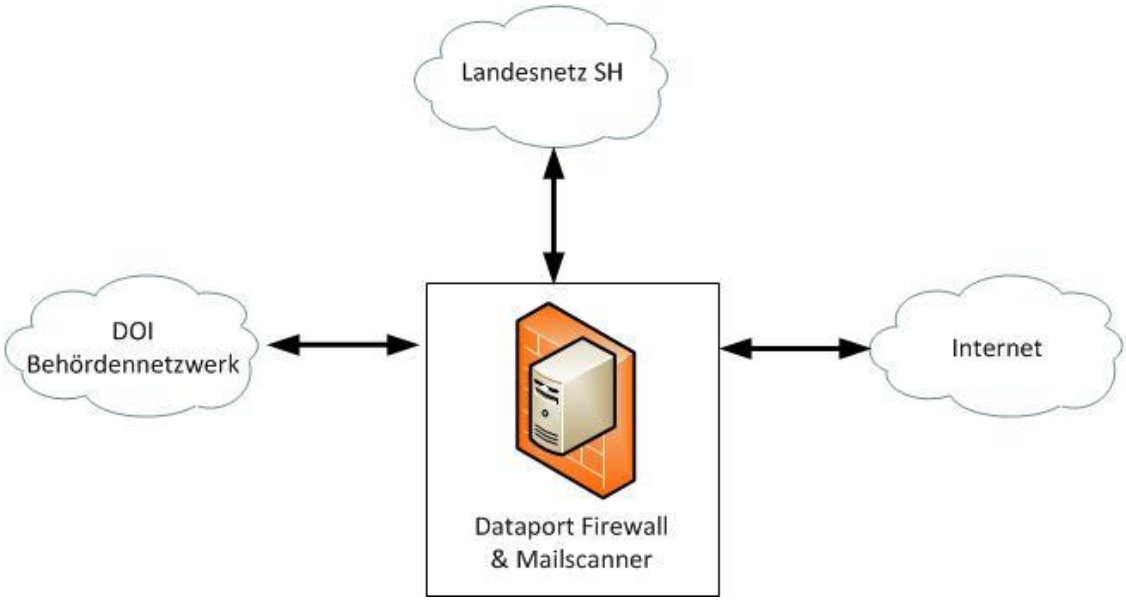
Die Ziele des Dienstes Internet E-Mail SH lauten:

- Die Kommunikation ist so einfach wie möglich und unterstützt die Nutzer bei ihrer Arbeit
- Die Sicherheitsanforderungen des Landesnetzes SH werden erfüllt
- Sichere Kommunikation ist auch mit Teilnehmern außerhalb des Landesnetzes möglich.

In den folgenden Abschnitten wird beschrieben, welche Maßnahmen der Auftragnehmer ergreift, um diese Ziele zu erreichen.

3.1.1 Übersicht

Der Auftragnehmer ermöglicht die E-Mail-Kommunikation der Systeme des Auftraggebers mit dem Internet. Hierbei betreibt der Auftraggeber i.d.R. einen eigenen E-Mail-Server im Landesnetz oder nutzt weitere Dienstleistungen des Auftragnehmers, welche ihm E-Mail-Server oder E-Mail-Postfächer zur Verfügung stellen. Beim E-Mail-Routing stellt der Auftragnehmer sicher, dass E-Mails aus verschiedenen Netzen (Internet, DOI, usw.) empfangen werden und an die Kunden-Mailserver/Postfächer im Landesnetz weitergeleitet werden. Ebenso werden E-Mails von Kunden-Clients oder Kunden-Mailservern entgegengenommen und an ihr Ziel weitergeleitet.



Damit E-Mails aus dem Internet korrekt an die Kundenserver übermittelt werden können, liefert der Auftraggeber neben seinem Domainnamen die IP-Adresse des zuständigen Mailservers, an den die E-Mails durch den Auftragnehmer weitergeleitet werden. Sofern die DNS-Einstellungen vom Kunden verwaltet werden, stellt Dataport diesem die korrekten Einstellungen hierfür zur Verfügung. Sofern die DNS-Einstellungen durch den Auftragnehmer verwaltet werden, nimmt der Auftragnehmer diese Änderungen selbständig vor.

3.1.2 Routing nur von gültigen Absenderadressen

Problemstellung: Zuverlässigkeit und Vertrauenswürdigkeit des Dienstes hängen in hohem Maße davon ab, dass niemand versehentlich oder absichtlich E-Mails mit einer gefälschten Absenderadresse verschicken kann und dass Antworten auf eine E-Mail immer zugestellt werden können.

Absenderadressen werden auf Gültigkeit geprüft, bevor diese vom Dataport Mailrelay angenommen und weitergeroutet werden. So werden ausschließlich gültige Adressen bzw. Domains als Senderadresse aus internen Netzen akzeptiert.

Aufgrund der dezentralen Verwaltung von teilnehmenden Kunden-Mailservern ist es meist nicht möglich, die komplette E-Mail-Adresse zu validieren, da dem Dataport-Mailsystem nicht alle Empfänger-Postfächer bekannt sind.

Festlegung: Senderdomains dürfen nur von den Eigentümern der jeweiligen Domains verwendet werden. Der Auftraggeber teilt dem Auftragnehmer mit, welche Kombinationen von IP-Adressen und Domains zum Versand von E-Mails verwendet werden. Dataport transportiert nur E-Mails mit diesen genannten Kombinationen.

3.1.3 Routing an existierende Zieladressen

Problemstellung: E-Mails (insbesondere aus dem Internet) sollen nur angenommen und weitergeleitet werden, wenn die Zieladressen (auf dem Mailserver des Auftraggebers) auch existieren. Andernfalls kommt es zu sogenannten BOUNCE-Mails, wobei E-Mails zunächst angenommen werden und später eine Nicht-Zustellbarkeitsmeldung zurückgesendet wird. Dieses Verhalten soll nach Möglichkeit unterbunden werden, damit nur E-Mails für real existierende Postfächer angenommen und transportiert werden.

Im Normalfall ist es für den Auftragnehmer aufgrund der dezentralen Organisation der Mailserver im Landesnetz nicht ohne weiteres möglich schon bei der Annahme festzustellen, ob das Postfach auf dem Zielserver auch existiert. Der Mechanismus der Empfänger-Validierung ermöglicht es, die Existenz der Zielpostfächer schon vor Annahme der E-Mail zu überprüfen.

Empfehlung: Der Auftragnehmer empfiehlt dem Auftraggeber, auf dem E-Mailserver des Auftraggebers die Empfänger-Validierung zu aktivieren. Die Aktivierung wird empfohlen, ist jedoch keine ausdrückliche Pflicht des Auftraggebers.

3.1.4 Ablehnen von internen Adressen/Domains aus dem Internet

Problemstellung: Behördenadressen sind besondere Adressen, denn sie signalisieren eine besondere Vertrauenswürdigkeit. Betrüger machen sich diese Eigenschaft zunutze. Sie versenden E-Mails aus dem Internet ins Landesnetz und verwenden zur Täuschung eine Behördenadresse als Absender. Die Empfänger können eine Adressfälschung kaum erkennen.

Der rechtmäßige Ursprung einer E-Mail mit einer Landesnetz-Adresse kann nur im Landesnetz liegen, denn nur diese Systeme sind berechtigt, Nachrichten im Namen dieser Domänen zu versenden.

Festlegung: Der Auftragnehmer nimmt keine E-Mails mit internen Absenderadressen aus dem Internet entgegen. Die E-Mail wird direkt am Internetübergang durch einen REJECT-Fehlercode abgewiesen und gelangt nicht in den Verantwortungsbereich des Auftragnehmers bzw. eines Systems des Auftraggebers.

3.1.5 Routing in DOI (Deutschland-Online-Infrastruktur)

Alle Domains, die Bestandteil dieses Vertrages sind, werden automatisch als Teilnehmer am DOI-Netz gemeldet. Somit ist es möglich, dass deutsche Verwaltungen bundesländerübergreifend über die sichere Infrastruktur der deutschen Verwaltungen ihre E-Mails austauschen, ohne dass diese über das Internet gesendet werden.

3.2 E-Mail Filterung

3.2.1 Mögliche Gefahren

Die E-Mail-Kommunikation ist mit einer Vielzahl an möglichen Gefahren verbunden, welche durch die E-Mail-Filterung eingedämmt werden sollen. Unerwünschte E-Mails, z.B. SPAM, Viren/Trojaner (nachfolgend Schadsoftware/Malware genannt) oder ausführbare Dateien werden hierbei besonders betrachtet.

Der Auftragnehmer hat die Einhaltung gesetzlicher Vorgaben insbesondere des TKG sicherzustellen. Dies bedeutet u.a. dass:

- empfangene E-Mails dem Empfänger stets zugestellt werden
- Inhalte von E-Mails niemals verändert werden
- der Auftragnehmer sich über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus keine Kenntnis vom Inhalt der Kommunikation verschafft

Dies macht es erforderlich, möglichst viele SPAM-E-Mails und E-Mails mit gefährlichen Inhalten schon vor dem Empfang abzulehnen. In den nachfolgend dargestellten Verfahren erfolgen Überprüfungen bzw. Auswertungen ausschließlich automatisiert.

3.2.2 Maßnahmen gegen gefährliche Anlagen

Anlagen von E-Mails stellen ein potenzielles Sicherheitsrisiko dar, insbesondere wenn es sich hierbei um ausführbare Dateien z.B. (.exe, .com, .pif, .scr, usw.) handelt. Bei diesen Dateien kann es sich um Schadcode handeln, der unbemerkt den PC des Empfängers infizieren und z.B. schutzwürdige Daten stehlen könnte.

Um derartige gefährliche Inhalte zu erkennen, wird zunächst geprüft, um welche Form von Dateiextension bzw. Dateityp es sich handelt. Wird hierbei festgestellt, dass es sich um eine potenziell gefährliche Dateiextension handelt, so wird die E-Mail direkt am Internetübergang abgewiesen, bevor sie in den Verantwortungsbereich des Auftragnehmers gelangt. Standardmäßig wird lediglich die Dateiextension anhand des Dateinamens geprüft. Die automatische Prüfung der Anlagen durch entsprechende Software erfolgt bei Dateianlagen sowie in Dateiarchiven, z.B. zip-Dateien. Eine weitergehende Prüfung, ob es sich tatsächlich um einen bestimmten Dateitypen (Prüfung anhand des Dateiinhaltes) handelt, ist bei gesonderter Beauftragung möglich.

Sofern die Prüfung anhand der Dateiextension bzw. des Dateityps nicht zur Ablehnung geführt hat, wird im nächsten Schritt die E-Mail mit Hilfe eines Virenscanners untersucht. Sofern Schadsoftware erkannt wurde, führt dies ebenfalls zum direkten Abweisen der E-Mail.

3.2.3 Maßnahmen gegen SPAM

Neben den direkten Gefahren durch Anlagen werden im Folgenden alle weiteren Formen unerwünschter Inhalte wie z.B. Massenwerbung oder auch E-Mails mit gefährlichen Links allgemein als SPAM bezeichnet.

Der Auftragnehmer setzt eine Vielzahl von Maßnahmen ein, die eng miteinander verzahnt sind und in ihrer Summe zu einem wirksamen Spamschutz beitragen. Zu diesen Maßnahmen gehören u.a. die Prüfung auf die Einhaltung des SMTP-Protokolls laut RFC-Vorgaben, DNS-Blacklists, Greylisting, Content-Filterung, Reputationsdatenbanken sowie manuell erstellte Filter. Da sich die Muster der SPAM-Mails oftmals stündlich verändern, ist es nicht auszuschließen, dass – insbesondere zu Beginn einer neuen Welle - einige der ersten SPAM-Mails an die Empfänger zugestellt werden. Für diesen Fall stellt der

Auftragnehmer ein Service-Postfach zur Verfügung, über das SPAM-Mails gemeldet werden können, um z.B. Dataport-eigene Filterregeln zu implementieren (siehe 3.2.7).

3.2.4 Ablehnen von unerwünschten E-Mails

Die Erkennung auf unerwünschte E-Mails wird während des Empfangs aus dem Internet durchgeführt. Entscheiden die umfangreichen Prüfmechanismen, dass es sich um eine unerwünschte E-Mail handelt, so erhält der aus dem Internet einliefernde Mailserver umgehend (vor der Empfangsquittierung) eine entsprechende Fehlermeldung (REJECT), sodass die E-Mail nicht in den Verantwortungsbereich des Auftragnehmers und somit auch nicht nachgelagert in den Verantwortungsbereich des Auftraggebers gelangt. Der Absender erhält von seinem Provider (E-Mail-Dienstleister) eine entsprechende Fehlermeldung, dass die E-Mail nicht zugestellt werden konnte. Sollte es sich hierbei um eine Fehleinstufung handeln, so stehen die in 3.2.6 beschriebenen Maßnahmen zur Verfügung, um die E-Mail bei einem erneuten Zustellungsversuch dennoch zuzustellen.

3.2.5 Ausnahmedefinition

In einigen Ausnahmefällen kann es jedoch gewünscht sein, dass bestimmte Postfächer von der zuvor beschriebenen Filterung ausgenommen werden. Der jeweils berechtigte Ansprechpartner des Auftraggebers kann über das Funktionspostfach DataportFirewallSH@dataport.de eine Filter-Ausnahme beantragen. Hierbei ist es möglich für einzelne Empfängeradressen oder Domains die Spam-Filterung, die Filterung von gefährlichen Anhängen (banned content) oder auch die Virenfilterung abzuschalten, sodass die Inhalte ungefiltert das Empfängerpostfach erreichen.

3.2.6 Zustellung von Mails im Ausnahmefall / False-Positives

Es kann im Einzelfall vorkommen, dass eine E-Mail fälschlicherweise als SPAM klassifiziert und abgelehnt wird. Ebenso kann der Fall eintreten, dass z.B. eine legitime .exe Datei an einen Empfänger im Landesnetz zugestellt werden soll.

Um Anlagen aus dem Internet zu empfangen, die aufgrund der in 3.2.2 bis 3.2.4 beschriebenen Maßnahmen generell blockiert werden würden, z.B. „programm.exe“ ist es ausreichend, wenn der Absender die Datei z.B. in „programm.xxx“ umbenennt. Der Empfänger muss die ursprüngliche Benennung wiederherstellen, um das Programm ausführen zu können. Eine weitere Möglichkeit stellt die Verschlüsselung der Anlage mit einer zusätzlichen Software dar (z.B. WinZIP). Bei Versand einer Datei z.B. „programm.exe“ in einer verschlüsselten Archivdatei z.B. „archiv.zip“ oder „archiv.rar“ ist darauf zu achten, dass auch die Dateinamen verschlüsselt werden, da ansonsten die Prüfung des Archives die erhaltene „.exe“ Datei anhand des Namens erkennen würde.

Sollte eine E-Mail aus anderen Gründen nicht den Empfänger erreichen, wird der Auftragnehmer das Problem nach Erstellung eines Störungstickets durch das Dataport Callcenter zu beheben versuchen.

3.2.7 SPAM melden

Da sich die Muster der SPAM-Mails oftmals stündlich verändern, ist es nicht auszuschließen, dass dennoch gelegentlich eine SPAM-Mail zugestellt wird. In diesem Fall bittet der Auftragnehmer darum, die betreffende E-Mail zur Analyse an spam@landsh.de zu senden. Es ist hierbei wichtig, dass die E-Mail als Anhang versandt wird (nicht mittels „weiterleiten“), damit die ursprünglichen Kopfzeilen der SPAM-E-Mail erhalten bleiben (In Outlook ist die betreffende Mail zu markieren und dann STRG+ALT+F zu drücken, um die E-Mail als Anlage weiterzuleiten). Der Auftragnehmer wird so in die Lage versetzt, eigene Filterregeln zu entwerfen.

3.2.8 Regelmäßige Anpassung der Filterregeln

Der Auftragnehmer passt im Rahmen des laufenden Betriebs die bestehenden Filterregeln eigenständig an. Dies umfasst u.a. die Erstellung und Anpassung von Content-Filter Regeln, das manuelle Erstellen von Blockier-Regeln von Spam-Versendern, z.B. anhand der Absenderadresse, der einliefernden IP-Adresse bzw. des IP-Subnetz aus dem Internet, etc. Eine gesonderte Benachrichtigung des Auftraggebers bei Anpassungen dieser Regeln ist nicht erforderlich.

Abweichend hiervon darf der ITSB des Auftragnehmers im Bedrohungsfall kurzfristig eigenständig weitere Maßnahmen beauftragen und Ausnahmen genehmigen. Das ZIT wird umgehend informiert. Dieses Vorgehen ist ausführlich im Dokument „Sperren im Internet Firewall“ geregelt.

3.2.9 Zukünftige Anpassungen

Grundlegende Änderungen der Filtermaßnahmen, z.B. dem Einsatz neuer Techniken, werden in Abstimmung mit dem ZIT durchgeführt.

3.2.10 Filterregeln abhängig von der Quelle

Die vorhergehende Beschreibung bezieht sich im Regelfall auf E-Mails, die aus dem Internet empfangen werden, da hier die Hauptbedrohung zu erwarten ist.

Auch E-Mails aus Drittnetzen, wie z.B. dem DOI (Deutschland-Online-Infrastruktur) werden auf Bedrohungen untersucht, jedoch mit toleranteren Filterregeln bearbeitet.

Auch ausgehende E-Mails von Systemen des Auftraggebers an andere Teilnehmer im Landesnetz oder an Drittnetze, wie z.B. das Internet, werden auf SPAM/Schadsoftware untersucht, jedoch ebenfalls mit toleranten Filterregeln. Dies ist notwendig, um einen SPAM-Versand über die Mailsysteme des Auftragnehmers zu vermeiden und dient gleichzeitig der Reputationssicherung des Absenders. Die Filterung von ausgehenden E-Mails erfolgt z.T. im Post-Queue Verfahren, d.h. die E-Mail wird ggf. zunächst durch das Mailsystem des Auftragnehmers angenommen und nach Spam-Einstufung zurückgewiesen (BOUNCE). Dieses Verhalten ist jedoch nur in Sonderfällen (ausgehender SPAM-Versand) zu erwarten.

3.3 Protokollierung

Von einer transportierten E-Mail werden folgende Daten in eine Logdatei geschrieben: Datum, Uhrzeit, Einliefernder Host (Name+IP) , Absender-Adresse, Empfänger-Adresse, Menge der übertragenen Daten, Statuscode, Mail-ID auf dem nächsten Mailserver, Prüfungen der Spambewertung (welche Regeln haben angeschlagen) + Diagnoseinformationen zur Spam/Virenprüfung, bei Anhängen (Dateiname und Typ des Anhangs), Betreff der E-Mails (nur anlassbezogen zur Gefahrenabwehr insbesondere bei Spamfluten).

Nach 10 Tagen werden die protokollierten Daten gelöscht.

4 Glossar

Content-Filterung – eine E-Mail besteht aus Kopfzeilen (Header) mit Angaben zum Transport der E-Mail und dem eigentlichen zu übertragenden Inhalt (Content). Dieser Inhalt kann automatisiert von Anti-Spam- und Anti-Viren-Software untersucht und bewertet werden.

DNS – (Domain Name System) – ein Namensdienst, der die Zuordnung von Domainnamen (z.B. landsh.de) zu ihren IP-Adressen verwaltet. Für die Zustellung von E-Mails ist es erforderlich, dass im DNS zum Domainnamen die richtige IP-Adresse des zuständigen Mailservers hinterlegt wird.

DNS-Blacklist (RBL) - eine Liste von IP-Adressen, die dafür bekannt sind, dass über die zugehörigen Server unerwünschte Spam- oder Schadcode-Mails versendet werden. Wird laufend erneuert und nicht mehr aktive Server werden meist nach 24 Stunden wieder von der Liste entfernt.

DOI – Deutschland-Online-Infrastruktur , eine deutschlandweite Kommunikations-Infrastruktur für alle Behörden der Deutschen Verwaltung, siehe auch http://www.bva.bund.de

Greylisting – eine RFC-konforme Möglichkeit die Annahme von E-Mails von unbekannten Servern zu verzögern. Bis zum Zeitpunkt des erneuten Einlieferungsversuchs ist der einliefernde Server eventuell bereits als Spamversender in einschlägigen Reputationsdatenbanken erkannt worden. Diese Maßnahme trägt zur Spamvermeidung bei und hat keine Auswirkungen auf regelmäßige Kommunikation.

Phishing E-Mail – E-Mails, ähnlich wie Spam-E-Mails versendet, aber einen seriösen Hintergrund vortäuschend, um den Empfänger zu Eingabe persönlicher Daten (Bankdaten, Passwörter aller Art) zu bewegen und somit „abzufischen“. Oft wird ein gewisser Zeitdruck vorgetäuscht, damit der Empfänger nicht zu lange über die Authentizität nachdenkt.

Mailrelay – ein Mailserver, der E-Mails für nachgelagerte Server entgegennimmt und an diese weiterleitet.

MX-Record – der MX-Record einer Domain zeigt im DNS auf den Namen bzw. die IP-Adresse des Servers, der E-Mails für diese Domain entgegennimmt.

Reputationsdatenbanken – Eine öffentliche Datenbank, welche typische Merkmale von Spam-Versendern oder Spam-Mails enthält. Dies sind z.B. IP-Adressen von Spam-versendenden Servern oder eine Datenbank mit Hash-Werten bekannter Spam-Signaturen.

REJECT – bezeichnet die Abweisung einer E-Mail vor der endgültigen Empfangs-Quittierung. Dies hat nicht nur Performance-Gründe, sondern verhindert auch, dass eine E-Mail in den Verantwortungsbereich des Auftragnehmers gerät und nach dem Telekommunikationsgesetz zwingend zugestellt werden muss.

RFC – Request For Comment, aber deutlich mehr als nur ein Vorschlag für die Umsetzung eines Internet-Dienstes, sondern eher eine Referenz bzw. Spezifikation wie dieser Dienst umzusetzen ist, damit alle Internet-Teilnehmer diesen Dienst nutzen können (RFC-Konformität).

Routing – Weiterleitung, Beförderung, z.B. von E-Mails durch ein Mailrelay

Schadcode – Programmcode (aber z.B. auch bösartige Office-Macros), der für den Benutzer unerwünschte bzw. schädliche Aktionen oftmals unbemerkt ausführt. Der Schadcode kann z.B. Daten löschen oder schutzwürdige Daten (Zugangsdaten, personenbezogene Daten) an Dritte im Internet senden.

Spam – Spam- oder Junk-Mail sind unerwünschte E-Mails, die meistens in Massen verschickt werden und unverlangte Werbung, meist mit unseriösen Angeboten, enthalten. Die Grenze zu Phishing-Mails ist fließend.

TKG – Telekommunikationsgesetz – Das TKG regelt technische Aspekte der Telekommunikation, insbesondere sollen das Fernmeldegeheimnis und der Datenschutz bei einer Telekommunikation gewährleistet werden.

5 Änderungsverzeichnis (nur für den internen Bedarf)

Version	Änderungs-datum	Gliederungs-punkt	Erläuterung der Änderung	Autor/in
1.0.0	30.6.2015		Erstellung	
1.1	06.11.2015		Änderungswünsche des ZIT vom 22.07. eingearbeitet.	
1.2	2.12.2015		Info zur Protokollierung hinzugefügt	

Service Level Agreement

Internet-Zugang über die Dataport Firewall SH

Version: 1.2
Stand: 2.12.2015

Inhaltsverzeichnis

1 Einleitung

1.1 Aufbau des Dokumentes

Diese Anlage enthält die folgenden Kapitel:

Rahmenbedingungen (Kapitel 2): Regelung von allgemeinen Rechten und Pflichten von Auftraggeber und Dienstleister, Bestimmungen zur Laufzeit, Änderung bzw. Kündigung der Vereinbarung sowie Übergangsbestimmungen.

Leistungsbeschreibungen (Kapitel 3): Inhaltliche Beschreibung der bereitgestellten Leistungen sowie der für einen reibungslosen Betrieb erforderlichen Dienstleistungen.

1.2 Leistungsgegenstand

Gegenstand dieses Service Level Agreements ist die Leistung „Internet-Zugang über die Dataport Firewall SH“.

Die Leistungen werden hinsichtlich der Leistungsqualität und des Leistungsumfangs im Kapitel 3 beschrieben.

2 Rahmenbedingungen

2.1 Mitwirkungsrechte und –pflichten

Die vom Auftragnehmer zugesagten Leistungen erfolgen auf Anforderung des Auftraggebers. Es sind Mitwirkungs- und Bereitstellungsleistungen des Auftraggebers erforderlich. Der Auftraggeber muss folgende Daten liefern und aktuell halten:

- Name und E-Mail-Adresse des IT-Verantwortlichen, der berechtigt ist, Einstellungen der Proxy-Konfigurationen zu verändern bzw. zu beauftragen. Aktualisierungen senden Sie bitte an DataportFirewallSH@dataport.de
- Nennung der für den Internet-Zugang genutzten IP-Adressen bzw. Netzkreise
- Mitarbeit bei der Säuberung von infizierten PC-Clients (Schadcode / Malware)

2.2 Ansprechpartner

2.2.1 Störungsbearbeitung

Bei technischen Störungen wenden Sie sich bitte an das Dataport-Callcenter unter der Rufnummer 0431/3295-444 und lassen Sie dort einen Incident generieren.

Störungsannahme: Montag bis Freitag von 6:30 – 18:00 Uhr

Betriebszeit: Montag bis Donnerstag von 8:00 – 17:00 Uhr, Freitag von 8:00 – 15:00 Uhr

Kann die Störungsbehebung nicht innerhalb der normalen Bearbeitungszeit beendet werden, so wird die Bearbeitung am nächsten Werktag (Mo-Fr) fortgesetzt.

2.2.2 Technischer Ansprechpartner

Bei technischen Fragen zum Produkt wenden Sie sich bitte an DataportFirewallSH@dataport.de

2.2.3 Vertraglicher Ansprechpartner

Bei vertraglichen Fragen zum Produkt wenden Sie sich bitte an
DataportKundenbetreuungundVertrieb@dataport.de

3 Leistungsbeschreibung

3.1 Internet-Dienste

Der Zugang zum Internet wird über eine mehrfach gesicherten Firewall zentral für das Landesnetz Schleswig-Holstein bereitgestellt. Das vorliegende Dokument beschreibt die zentral implementierten Sicherungsmaßnahmen. Diese Maßnahmen gelten für alle Systeme innerhalb der gesicherten Zone und stellen den nötigen Schutz vor aktiven Angriffen von außen sicher.

Dataport bietet den Zugang zu ausgewählten Diensten des Internet. Der Zugang erfolgt über ein Firewall-System, das die Einhaltung der Protokolle gewährleistet und den Anwender vor aktiven Zugriffen von Angreifern aus dem Internet schützt. Die Planung und den Betrieb dieser Infrastruktur verantwortet Dataport im Auftrage des Landes Schleswig-Holstein.
Um den sicherheitstechnischen Stand und die besondere Beachtung des Datenschutzes zu dokumentieren, hat Dataport dieses Produkt vom ULD (Unabhängiges Landeszentrum für Datenschutz in Schleswig-Holstein) zertifizieren lassen. Der Internetzugang von Dataport wurde im November 2003 erstmals mit dem Gütesiegel des ULD ausgezeichnet. Diese Zertifizierung wird regelmäßig erneuert.

3.2 Leistung

Das Produkt "Dataport Firewall SH" besteht aus mehreren Komponenten: Externe und interne Paketfilter sichern das dazwischen liegende Netzsegment, in dem Proxies (Application Layer Gateways) für Dienste auf Basis der Protokolle SMTP, HTTP und FTP bereitgestellt werden. Alle Komponenten sind zur Erhöhung der Verfügbarkeit redundant ausgelegt (teilweise mehrfach zwecks Lastverteilung).

Dataport betreibt die erforderlichen Netz- und Systemkomponenten in sicheren Systemräumen. Durch technische und organisatorische Maßnahmen ist der Zugang zu diesen Komponenten streng reglementiert.

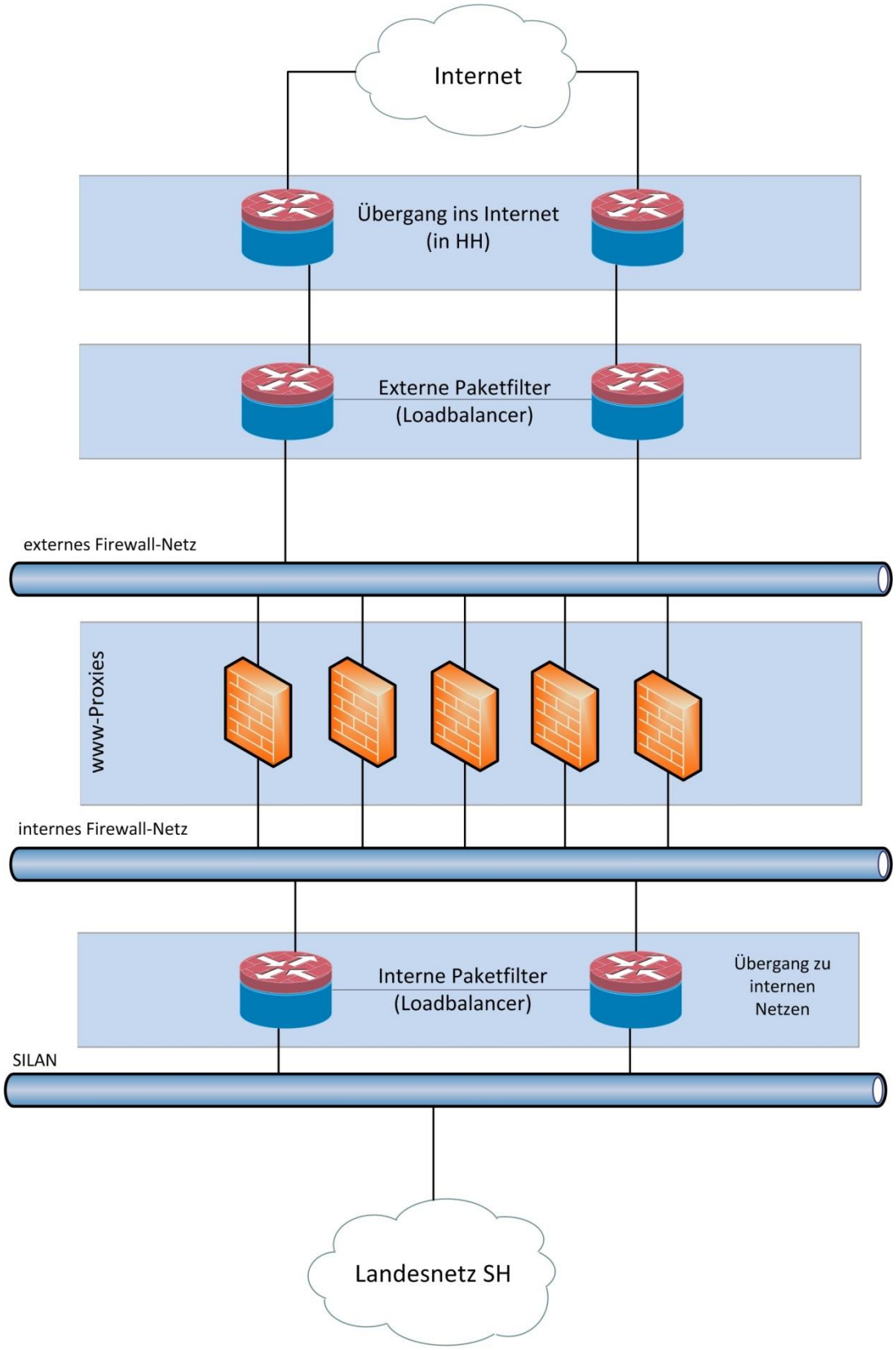


Abbildung 1: Dataport Firewall-Infrastruktur am Standort Altenholz

Die Produktkomponenten (Paketfilter und Proxies) schützen das Netz von Dataport und die Teilnehmernetze am Landesnetz Schleswig-Holstein durch Einschränkung der Verbindungen zum Internet auf zulässige Dienste anhand von Kommunikationsbedingungen wie z.B. die Einschränkung auf bestimmte IP-Adressen für Zielrechner einer Verbindung, die Zugehörigkeit eines IP-Paketes zu einer bestehenden Verbindung oder dem protokollkonformen Aufbau eines IP-Paketes.

Dabei werden Nutzungsdaten zu Abrechnungszwecken und zur Analyse von fehlerhaften oder unzulässigen Verbindungen sowie anonymisiert zu statistischen Zwecken in Protokollen gespeichert. Die Analyse und Erstellung von Statistiken erfolgt durch die Firewall-Administration. Die Nutzungsdaten zu Abrechnungszwecken werden in einem, von der Firewall getrennten Verfahren, der Dataport Rechnungsstelle zur Verfügung gestellt. Jede Analyse der Protokolldaten, die nicht zu diesen genannten Zwecken erfolgt, sondern aufgrund spezieller Anforderungen (z.B. zu Zwecken der Strafverfolgung) erforderlich wird, erfolgt im Rahmen einer eigenständigen Auftragsdatenverarbeitung und ist nicht Bestandteil der hier beschriebenen Leistung.

Die sicherheitstechnischen Rahmenbedingungen, das Schutzniveau und die protokollierten Informationen des hier beschriebenen Produktes sind im Sicherheitskonzept Dataport-Firewall festgelegt. Die technische Umsetzung des Sicherheitskonzeptes wird durch ein Betriebskonzept beschrieben. Da für alle Produktkomponenten im Sicherheitskonzept die gleichen technisch-organisatorischen Maßnahmen festgelegt wurden, werden diese in einem eigenen Abschnitt aufgeführt. Das Sicherheits- und Betriebskonzept kann auf Wunsch bei Dataport eingesehen werden.

3.3 Eingesetzte Softwarepakete

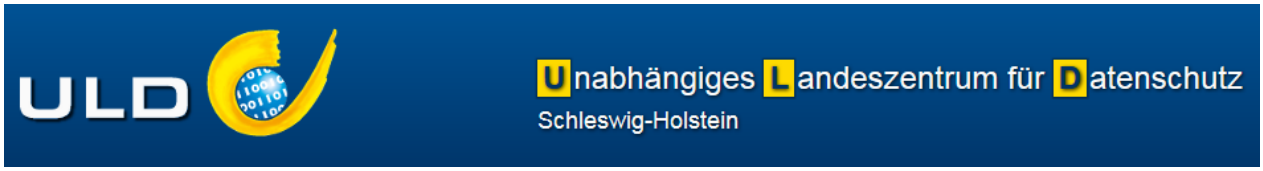
Das Produkt basiert auf Open Source Paketen. Deren weltweiter, breiter Einsatz gewährleistet eine fortlaufende Weiterentwicklung, schnelle Entdeckung von Sicherheitslücken und die schnelle Bereitstellung von Sicherheitspatches, die umgehend eingespielt werden. Eingesetzt werden:

- Linux als Betriebssystem
- Squid für HTTP
- ftp-proxy für FTP
- Postfix für SMTP

Hinzu kommen einige Zusatzpakete (z.B. bind, squidguard, sec usw.) sowie teilweise selbst Werkzeuge zur Überwachung des ordnungsgemäßen Betriebszustands, Anonymisierung, Auswertung und sonstige wiederkehrende Aufgaben.

3.4 Zweck und Einsatzbereich

Diese Produktkomponenten können von den Kunden zum Schutz ihrer eigenen Ressourcen im Netzwerk gegen unberechtigte Zugriffe aus dem Internet in Anspruch genommen werden. Die Zielsetzung, Gesamtkonzeption und Einsatzumgebung wurde im November 2003 vom ULD (Unabhängiges Landeszentrum für Datenschutz in Schleswig-Holstein) ausdrücklich empfohlen und mit dem Gütesiegel ausgezeichnet. Der rechtliche Rahmen zur Auditierung des Produkts bestand aus der Datenschutzauditverordnung Schleswig-Holstein (DSAVO), dem Landesdatenschutzgesetz Schleswig-Holstein (LDSG-SH) sowie dem Teledienstegesetz (TDG), dem Mediendienste-Staatsvertrag (MDStV) und Teledienstedatenschutzgesetz (TDDSG).



Für den Einsatz der Dataport-Firewall kam das ULD zu folgendem Ergebnis:

„Die Art und Weise des Betriebs - insbesondere die vorbildliche Sicherheit der Einsatzumgebung - sowie die Konfiguration des Produkts gewährleisten bei adäquater Transparenz in vollem Umfang eine auf notwendige Daten beschränkte Verarbeitung der IP-Pakete (Primärdaten) und Protokolldaten (Sekundärdaten)….“

4 Angaben zur Funktionalität

4.1 Funktionsumfang

Angeboten wird der Zugang zu den Diensten Internet („surfen“, HTTP), E-Mail (SMTP) und Dateitransfer (FTP). Für die Dienste HTTP und FTP erfolgt der Zugriff über sogenannte Proxy-Server. Der Proxy-Server setzt die Kommunikation zwischen dem Endanwender und dem Ziel im Internet um. Dadurch kommt es zu keiner direkten Verbindung zwischen dem genutzten Client und dem Internet. Für den Versand von E-Mail steht die Dataport-Firewall als Mail-Relay zur Verfügung.

4.2 Grenzwerte

Dataport ist mit einer redundanten 1 Gbit/s Standleitung an das Internet angeschlossen. Diese Bandbreite steht gemeinsam für alle Benutzer zur Verfügung. Bei Engpässen ist es möglich, die zur Verfügung stehende Bandbreite für bestimmte Benutzerkreise der Zeit von 9:00-16:00 Uhr begrenzen zu lassen.

Dataport überwacht automatisch die Auslastung zum Internet und baut den Anschluss entsprechend der Nutzungsverhalten ständig aus.

4.3 Sicherheit

Um gegen aktive Angriffe aus dem Internet gesichert zu sein, betreibt Dataport das Firewall-System als geschützten und schützenden Zugangspunkt zum Internet. Durch diesen Zugang können aus dem Internet keine aktiven Angriffe in die internen Netze und damit auch nicht bis zu einem Arbeitsplatzrechner vordringen. Ein Außenstehender kann keine Verbindung zu einem internen Rechner aufbauen.

Das Firewall-System bietet nur für zugelassene Arbeitsplatzrechner den Zugriff auf das Internet. Dadurch können die Berechtigungen innerhalb eines lokalen Netzes individuell vergeben werden. Die Verbindung von einem Arbeitsplatzrechner zum Internet erfolgt nicht direkt, sondern stellvertretend durch die Proxy-Server.

Das integrierte Mail-Gateway kann ein- und ausgehende E-Mails mit unerwünschten Inhalten bzw. unerwünschten Anhängen erkennen und abweisen (greylisting, blacklists und weitere, ständig aktualisierte Maßnahmen). Diese Leistungen sind in einer gesonderten Leistungsbeschreibung ausführlich beschrieben.
Wird Dataport davon in Kenntnis gesetzt oder erhält Dataport durch eigene Überwachungsmaßnahmen davon Kenntnis, dass Clients im Landesnetz von Schadcode befallen sind, behält sich Dataport vor, diese Clients umgehend zu sperren und die zuständigen Sicherheitsmanager zu informieren. Dies dient dem Schutz vor Datendiebstahl aus Kundennetzen sowie der Reputationssicherung der Dataport Firewalls (Gefahr des IP-Blacklistings). Ebenso behält sich Dataport vor, in Zusammenarbeit mit den zuständigen Sicherheitsmanagern Webseiten zu sperren, die mit hoher Wahrscheinlichkeit Schadcode anbieten bzw. verteilen.

4.4 Sicherheitskonzept

Dataport hat für den Zugang zu den Internet-Dienstleistungen ein Sicherheitskonzept erstellt, das auf Wunsch des Auftraggebers zur Einsichtnahme bei Dataport ausliegt.

4.5 Systemausfälle

Der Zugang zum Internet ist durchgehend verfügbar. Durch technische Maßnahmen (redundante Auslegung aller Systeme (automatische Überwachung und automatisches Fallback auf Backup-Systeme) wird versucht, die Auswirkung von Systemausfällen zu minimieren.

Dataport behält sich vor, Firewalls vom Netz zu trennen, wenn unbekannte Angriffe aus dem Internet auftreten oder die Vermutung besteht, dass Systeme unberechtigt genutzt werden, um z.B. interne Netze anzugreifen.

Falls E-Mailserver im Landesnetz oder Internet nicht erreichbar sind, so wird Dataport 24 Stunden lang versuchen, eine E-Mail zuzustellen. Danach wird die E-Mail als unzustellbar zum Absender zurückgesandt.

4.6 Protokollierung

Um den ordnungsgemäßen Betrieb und die Sicherheit der Systeme zu gewährleisten, werden folgende Verbindungsdaten laufend protokolliert:

HTTP(S): Datum, Uhrzeit, IP-Adresse des Arbeitsplatzes, HTTP-Methode, Status/Fehlercode, Menge der übertragenen Daten, URL (teilweise verkürzt, ohne Parameter), IP des Zielsystems, Datentyp. Bei HTTPS-Zugriffen können die HTTP-Methode und der Datentyp nicht protokolliert werden.

FTP: Datum, Uhrzeit, IP-Adresse des Arbeitsplatzes, Ziel-IP, Status/Fehlercode, Menge der übertragenen Daten, Namen der übertragenen Dateien

Gegen Mitternacht werden die protokollierten Client-IP-Adressen anonymisiert, indem das letzte Oktett auf „0“ gesetzt wird (Beispiel: aus 10.1.2.3 wird 10.1.2.0). Nach 10 Tagen werden die protokollierten Daten komplett gelöscht. Ein Teil der Daten wird vor der Löschung aggregiert (aufgerufene Domains, Datenmengen), um zu anonymisierten monatlichen Statistiken oder Abrechnungen verarbeitet zu werden. Eine detaillierte Beschreibung ist dem Sicherheitskonzept „Dataport Firewall SH“ zu entnehmen.

5 Glossar

DNS – (Domain Name System) – ein Namensdienst, der die Zuordnung von Domainnamen (z.B. landsh.de) zu ihren IP-Adressen verwaltet. Für die Zustellung von E-Mails ist es erforderlich, dass im DNS zum Domainnamen die richtige IP-Adresse des zuständigen Mailservers hinterlegt wird.

DNS-Blacklist (RBL) - eine Liste von IP-Adressen, die dafür bekannt sind, dass über die zugehörigen Server unerwünschte Spam- oder Schadcode-Mails versendet werden. Wird laufend erneuert und nicht mehr aktive Server werden meist nach 24 Stunden wieder von der Liste entfernt.

Mailrelay – ein Mailserver, der E-Mails für nachgelagerte Server entgegennimmt und an diese weiterleitet.

Malware – siehe Schadcode

Reputationsdatenbanken – Eine öffentliche Datenbank, welche typische Merkmale von Spam-Versendern oder Spam-Mails enthält. Dies sind z.B. IP-Adressen von Spam-versendenden Servern oder eine Datenbank mit Hash-Werten bekannter Spam-Signaturen.

Schadcode – Programmcode (aber z.B. auch bösartige Office-Macros), der für den Benutzer unerwünschte bzw. schädliche Aktionen oftmals unbemerkt ausführt. Der Schadcode kann z.B. Daten löschen oder schutzwürdige Daten (Zugangsdaten, personenbezogene Daten) an Dritte im Internet senden.

Spam – Spam- oder Junk-Mail sind unerwünschte E-Mails, die meistens in Massen verschickt werden und unverlangte Werbung, meist mit unseriösen Angeboten, enthalten. Die Grenze zu Phishing-Mails ist fließend.

6 Änderungsverzeichnis (nur für den internen Bedarf)

Version	Änderungs-datum	Gliederungs-punkt	Erläuterung der Änderung	Autor/in
1.0.0	23.12.2004		Vertragsgrundlage, abgestimmte Fassung	
1.1	27.08.2007		Bandbreitenmanagement und Anbindung angepasst	
1.2	2.12.2015		Protokollierung aufgenommen	

Wissenstest

Liebe Kolleginnen und Kollegen,

mit den folgenden Fragen können Sie Ihr eigenes Wissen über die bestehenden Regelungen zur dienstlichen und privaten Nutzung von Internet und E-Mail testen.

Die richtigen Antworten finden Sie auf den letzten zwei Seiten.

Testen Sie Ihr Wissen			
Welche der folgenden Regelungen zur privaten Nutzung des dienstlichen E-Mail-Zugangs gelten Ihres Erachtens? (Mehrfachnennungen möglich)		Zutreffend Ja	nein
a	*Das Versenden privater E-Mails ist grundsätzlich verboten.*	☐	☐
b	*Das Versenden privater E-Mails ist grundsätzlich erlaubt.*	☐	☐
c	*Das Versenden privater E-Mails ist zeitlich begrenzt zugelassen.*	☐	☐
d	*Das Versenden privater E-Mails ist in den Pausen zugelassen.*	☐	☐
e	*Das Verschicken von E-Mails mit persönlichem Inhalt ist in Ausnahmefällen - bei dienstlicher Veranlassung- erlaubt.*	☐	☐
		☐	☐
f	*Das Versenden gewerkschaftlicher Informationen an einen globalen Verteilerkreis ist erlaubt.*	☐	☐
g	*Das Versenden gewerkschaftlicher Informationen an Gewerkschaftsmitglieder ist erlaubt.*	☐	☐
h	*Das Versenden gewerkschaftlicher Informationen ist grundsätzlich verboten.*	☐	☐
i	*Der Empfang privater E-Mails ist unzulässig.*	☐	☐
j	*Der Empfang privater E-Mails ist erlaubt.*	☐	☐
k	*Empfangene private E-Mails sind sofort zu löschen.*	☐	☐
l	*Absender privater E-Mails sind darum zu bitten, dies zu unterlassen.*	☐	☐

		Zutreffend Ja	nein
Welche der folgenden Regelungen zur dienstlichen E-Mail-Nutzung gelten Ihres Erachtens? (Mehrfachnennungen möglich)			
a	*Alle erhaltenen oder gesendeten E-Mails sind zu archivieren.*	☐	☐
b	*Die Dienststelle hat, unter Beachtung bestimmter Verfahrensregeln, das Recht, sich alle erhaltenen oder gesendeten E-Mails vorlegen zu lassen.*	☐	☐
c	*Die Dienststelle hat das Recht, sich alle dienstlichen E-Mails vorlegen zu lassen.*	☐	☐
d	*Die Dienststelle hat, unter Beachtung bestimmter Verfahrensregeln, das Recht, sich zu allen erhaltenen oder gesendeten E-Mails Zugang zu verschaffen.*	☐	☐
e	*E-Mails an und von Personalrat, Gleichstellungsbeauftragten, Schwerbehindertenvertretung unterliegen einem besonderen Schutz.*	☐	☐
f	*E-Mails an und von Personalrat, Gleichstellungsbeauftragten, Schwerbehindertenvertretung dürfen durch die Dienststelle generell eingesehen werden.*	☐	☐
Welche der folgenden Regelungen zur privaten Nutzung des dienstlichen Internet-Zugangs gelten Ihres Erachtens? (Mehrfachnennungen möglich)			
a	*Eine private Nutzung des Internet-Zuganges ist grundsätzlich verboten.*	☐	☐
b	*Eine private Nutzung des Internet-Zuganges ist grundsätzlich erlaubt, soweit dienstliche Interessen nicht entgegenstehen.*	☐	☐
c	*Eine private Nutzung des Internet-Zuganges unterliegt einer festen zeitlichen Grenze.*	☐	☐
d	*Eine private Nutzung des Internet-Zuganges ist nur in den Pausen zugelassen.*	☐	☐
e	*Eine private Nutzung ist nur in Ausnahmefällen - bei dienstlicher Veranlassung- erlaubt.*	☐	☐
f	*Die Nutzung eines Web-Mail-Dienstes ist erlaubt.*	☐	☐
Was gilt Ihres Erachtens "beim Versand von E-Mails mit vertraulichem Inhalt oder personenbezogenen Daten" an berechtigte Empfänger? (Mehrfachnennungen möglich)			
a	*Dies ist innerhalb des Landesnetzes grundsätzlich zulässig.*	☐	☐
b	*Dies ist innerhalb des Landesnetzes grundsätzlich ist nur in verschlüsselter Form zulässig.*	☐	☐
c	*Dies ist auch nach außerhalb des Landesnetzes ohne weiteres zulässig.*	☐	☐
d	*Dies ist nach außerhalb des Landesnetzes ist nur in verschlüsselter Form zulässig.*	☐	☐
e	*Dies ist nach außerhalb des Landesnetzes ist nur im E-Mail-Anhang zulässig.*	☐	☐
Welche der folgenden Regelungen zur Protokollierung der E-Mail- und Internet-Nutzung gelten Ihres Erachtens? (Mehrfachnennungen möglich)			
a	*Es erfolgt eine Protokollierung der E-Mail- und Internet-Nutzung.*	☐	☐
b	*Dataport übermittelt den Dienststellen detaillierte Protokolle.*	☐	☐
c	*Dataport übermittelt den Dienststellen anonymisierte Protokolle, die von diesen stichprobenartig ausgewertet werden.*	☐	☐
d	*Bei Hinweisen auf eine unzulässige Nutzung hat die Dienststelle ohne weiteres das Recht auf alle Verbindungs- und Inhaltsdaten zuzugreifen.*	☐	☐
e	*Bei Hinweisen auf eine unzulässige Nutzung ist eine gezielte Überprüfung nach einem gesondert festzulegenden Verfahren möglich.*	☐	☐

Die Antworten			
Welche der folgenden Regelungen zur privaten Nutzung des dienstlichen E-Mail-Zugangs gelten Ihres Erachtens? (Mehrfachnennungen möglich)		Zutreffend Ja	nein
a	*Das Versenden privater E-Mails ist grundsätzlich verboten.*	**x**	
b	*Das Versenden privater E-Mails ist grundsätzlich erlaubt.*		**x**
c	*Das Versenden privater E-Mails ist zeitlich begrenzt zugelassen.*		**x**
d	*Das Versenden privater E-Mails ist in den Pausen zugelassen.*		**x**
e	*Das Verschicken von E-Mails mit persönlichem Inhalt ist in Ausnahmefällen - bei dienstlicher Veranlassung- erlaubt.*	**x**	
f	*Das Versenden gewerkschaftlicher Informationen an einen globalen Verteilerkreis ist erlaubt.*		**x**
g	*Das Versenden gewerkschaftlicher Informationen an Gewerkschaftsmitglieder ist erlaubt.*	**x**	
h	*Das Versenden gewerkschaftlicher Informationen ist grundsätzlich verboten.*		**x**
i	*Der Empfang privater E-Mails ist unzulässig.* *Erläuterung: Den Empfang einer E- Mail von einem Einsender, der z.B. noch nicht belehrt wurde (siehe k), können die Mitarbeiterinnen und Mitarbeiter nicht verhindern. Davon unberührt bleibt es bei dem Grundsatz, dass die Nutzung von E- Mail ausschließlich für dienstliche Zwecke zulässig ist.*	**x**	
j	*Der Empfang privater E-Mails ist erlaubt.*		**x**
k	*Empfangene private E- Mail sind sofort zu löschen.* *Erläuterung: Die Nutzung von E- Mail ist ausschließlich für dienstliche Zwecke zulässig. Sofern die E- Mail unter MS- Outlook aufbewahrt wird, wird diese wie dienstliche E- Mail behandelt. Sofern dies nicht gewünscht ist, sollte sie gelöscht bzw. in die private Sphäre überführt werden.*		**x**
l	*Absender privater E-Mails sind darum zu bitten, dies zu unterlassen.*	**x**	

Welche der folgenden Regelungen zur dienstlichen E-Mail-Nutzung gelten Ihres Erachtens? (Mehrfachnennungen möglich)		Zutreffend Ja	nein
a	*Alle erhaltenen oder gesendeten E-Mails sind zu archivieren.*		**x**
b	*Die Dienststelle hat, unter Beachtung bestimmter Verfahrensregeln, das Recht, sich alle erhaltenen oder gesendeten E-Mail vorlegen zu lassen.*	**x**	
c	*Die Dienststelle hat das Recht, sich alle dienstlichen E-Mail vorlegen zu lassen.*	**x**	
d	*Die Dienststelle hat, unter Beachtung bestimmter Verfahrensregeln, das Recht, sich zu allen erhaltenen oder gesendeten E-Mail Zugang zu verschaffen.*	**x**	
e	*E-Mails an und von Personalrat, Gleichstellungsbeauftragten, Schwerbehindertenvertretung unterliegen einem besonderen Schutz.*	**x**	
f	*E-Mails an und von Personalrat, Gleichstellungsbeauftragten, Schwerbehindertenvertretung dürfen durch die Dienststelle generell eingesehen werden.*		**x**
Welche der folgenden Regelungen zur privaten Nutzung des dienstlichen Internet-Zugangs gelten Ihres Erachtens? (Mehrfachnennungen möglich)			
a	*Eine private Nutzung des Internet-Zuganges ist grundsätzlich verboten.*		**x**
b	*Eine private Nutzung des Internet-Zuganges ist grundsätzlich erlaubt, soweit dienstliche Interessen nicht entgegenstehen.*	**x**	
c	*Eine private Nutzung des Internet-Zuganges unterliegt einer festen zeitlichen Grenze.*		**x**
d	*Eine private Nutzung des Internet-Zuganges ist nur in den Pausen zugelassen.*		**x**

e	*Eine private Nutzung ist nur in Ausnahmefällen - bei dienstlicher Veranlassung- erlaubt.*		**x**
f	*Die Nutzung eines Web-Mail-Dienstes ist erlaubt.*	**x**	
Was gilt Ihres Erachtens "beim Versand von E-Mails mit vertraulichem Inhalt oder personenbezogenen Daten" an berechtigte Empfänger? (Mehrfachnennungen möglich)		Zutreffend Ja	nein
a	*Dies ist innerhalb des Landesnetzes grundsätzlich zulässig.*	**x**	
b	*Dies ist innerhalb des Landesnetzes grundsätzlich ist nur in verschlüsselter Form zulässig.*		**x**
c	*Dies ist auch nach außerhalb des Landesnetzes ohne weiteres zulässig.*		**x**
d	*Dies ist nach außerhalb des Landesnetzes ist nur in verschlüsselter Form zulässig.*	**x**	
e	*Dies ist nach außerhalb des Landesnetzes ist nur im E-Mail-Anhang zulässig.*		**x**
Welche der folgenden Regelungen zur Protokollierung der E-Mail- und Internet-Nutzung gelten Ihres Erachtens? (Mehrfachnennungen möglich)			
a	*Es erfolgt eine Protokollierung der E-Mail- und Internet-Nutzung.*	**x**	
b	*Dataport übermittelt den Dienststellen detaillierte Protokolle.*		**x**
c	*Dataport übermittelt den Dienststellen anonymisierte Protokolle, die von diesen stichprobenartig ausgewertet werden.*	**x**	
d	*Bei Hinweisen auf eine unzulässige Nutzung hat die Dienststelle ohne weiteres das Recht auf alle Verbindungs- und Inhaltsdaten zuzugreifen.*		**x**
e	*Bei Hinweisen auf eine unzulässige Nutzung ist eine gezielte Überprüfung nach einem gesondert festzulegenden Verfahren möglich.*	**x**	