

IT-Handbuch

für die Verwaltung der
Freien und Hansestadt Hamburg

Telekommunikationsrichtlinie (TK-RL)

Richtlinie zur Gestaltung und Benutzung der
Telekommunikation in der Verwaltung der
Freien und Hansestadt Hamburg
(Telekommunikationsrichtlinie - TK-RL)

vom 9. Dezember 2009 (MittVw 2010 Seite 2),
zuletzt geändert am 7. November 2013

Die für die Grundsatzangelegenheiten der Informationstechnik zuständige Behörde erlässt diese Richtlinie aufgrund der Ermächtigung des Senats vom 21.9.2004.

1. Allgemeines

1.1 Telekommunikationsnetz

- (1) Die Freie und Hansestadt Hamburg (FHH) hat ihre eigene Telekommunikationsinfrastruktur (Hamburgisches Telekommunikationsnetz – TK-Netz) mit Gesetz vom 08. Januar 2004 in ein Sondervermögen unter dem Namen „Sondervermögen Hamburgisches Telekommunikationsnetz“ überführt. Das Sondervermögen unterliegt der Aufsicht der für die Finanzen zuständigen Behörde.
- (2) Das Sondervermögen wird von Dataport – Anstalt öffentlichen Rechts – verwaltet. Dataport ist insoweit Betreiber des TK-Netzes. Der Betrieb des TK-Netzes erfolgt nicht für die Öffentlichkeit.
- (3) Für die Telekommunikation der Behörden und Ämter der FHH untereinander wird das Hamburgische Telekommunikationsnetz (Hamburgisches TK-Netz) als regionales Netz betrieben. Das Hamburgische TK-Netz ist die Gesamtheit der Vermittlungseinrichtungen, Übertragungswege und Anschalteinrichtungen, die dem inneren Dienst der FHH gewidmet sind und als privates Telekommunikationsnetz grundstücks- und organisationseinheitenübergreifend betrieben wird. Diesem Netz können direkt angeschlossene Endeinrichtungen und selbständig betreibbare Telekommunikationseinrichtungen auf einzelnen Grundstücken besonders zugerechnet werden. Als Bestandteil des Hamburgischen TK-Netzes gelten auch Telekommunikationseinrichtungen Dritter, soweit sie ausschließlich für die in Satz 2 genannten Zwecke genutzt werden.
- (4) Für einzelne Organisationseinheiten oder Aufgabenbereiche der FHH können lokale Netze als Teilnetze auf einzelnen Grundstücken oder für Verbindungen in Organisationseinheiten durch die zuständigen Behörden oder Ämter (lokale

Netzbetreiber) betrieben werden. Ein lokales Netz umfasst Übertragungswege, Vermittlungseinrichtungen oder Datenverarbeitungs(DV)-Anlagen, Endeinrichtungen und gegebenenfalls eine eigene Administration und Benutzerbetreuung regelmäßig auf einem Grundstück. Es kann auch gebäude- oder grundstücksübergreifend angelegt sein.

- (5) Lokale Netze der FHH können über definierte Anschalteneinrichtungen mit dem Hamburgischen TK-Netz verbunden werden. Soweit zur Realisierung grundstücksübergreifender lokaler Netze entsprechende Verbindungen erforderlich sind, sind die Übertragungswege im Rahmen des Hamburgischen TK-Netzes bereitzustellen.

1.2 Geltungsbereich

- (1) Diese Richtlinie gilt für alle Dienststellen der Freien und Hansestadt Hamburg. Andere Stellen und Einrichtungen der FHH, die ihre Telekommunikation über das Hamburgische TK-Netz betreiben, sind nach Maßgabe der mit Dataport geschlossenen schriftlichen Vereinbarungen zur Einhaltung dieser Richtlinie verpflichtet.
- (2) Diese Richtlinie regelt die Kommunikation der in Absatz 1 genannten Stellen mit Hilfe der Kommunikationstechnik. Die Regelungen umfassen die Gestaltung der sprachlichen und nicht-sprachlichen Telekommunikation, die Ausstattung mit Telekommunikationseinrichtungen und -diensten sowie deren Einführung, Ersatz, Betrieb und Nutzung.
- (3) Soweit mit DV-Anlagen gleichzeitig auch Telekommunikation möglich ist, bleiben die für die Nutzung von DV-Verfahren geltenden Vorschriften unberührt.

1.3 Grundsätze

- (1) Für die Telekommunikation können Arbeitsplätze mit den für die Nutzung von Telekommunikationsdiensten erforderlichen Endeinrichtungen ausgestattet werden. Hierzu gehören auch Telearbeitsplätze. Bei der Benutzung der Telekommunikationseinrichtungen und -dienste ist die wirtschaftliche, recht- und ordnungsmäßige Übertragung von Informationen zu gewährleisten. Dies beinhaltet insbesondere
 - den Schutz des Rechts auf informationelle Selbstbestimmung,
 - die Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme,
 - die Gewährleistung des Brief-, Post- und Fernmeldegeheimnisses,
 - die Einhaltung ergonomischer Standards,
 - die Gewährleistung der Arbeitssicherheit und des sonstigen Beschäftigten-schutzes,
 - Schulung und Einweisung sowie
 - rechtzeitige Information der Beschäftigten über die bevorstehende Einführung neuer Telekommunikationseinrichtungen und -dienste.
 -
- (2) Für die Aufgabenerfüllung ist der Einsatz und die Nutzung von Telekommunikationseinrichtungen und -diensten, gegebenenfalls in unterschiedlichen Ausprägungen durch Leistungsmerkmale, nach Maßgabe dieser Richtlinie und des ansonsten geltenden Rechts zugelassen. Dabei ist die Gestaltung des Einsatzes

und der Nutzung von Telekommunikationseinrichtungen und -diensten unter Berücksichtigung derer kommunikativen Eigenarten an technischen und verwaltungsorganisatorischen Zweckmäßigkeiten auszurichten.

1.4 Begriffsbestimmungen

- **Abfrageeinrichtungen** sind besondere Endeinrichtungen in Telefonzentralen zur manuellen Mitwirkung an der Herstellung von Verbindungen im Telefondienst.
- **Anschalteeinrichtungen** sind technische Einrichtungen für den Anschluss von Endeinrichtungen oder anderen, nicht zum Netz gehörenden Telekommunikationseinrichtungen.
- **Anwendende Stellen** sind Organisationseinheiten, die im Rahmen ihrer sachlichen Aufgabenerfüllung IT-Anwendungen in Form von Telekommunikationsdiensten nutzen.
- **Mehrwertdienste** sind Telekommunikationsdienste, die neben der Informationsübertragung weitere Dienstleistungen in Form von Informationsangeboten oder anderen automatisierten Nutzungsmöglichkeiten zur Verfügung stellen.
- **Netzbetreiber** sind Organisationseinheiten, die Telekommunikationseinrichtungen und die dazugehörige Infrastruktur für die Nutzung von Telekommunikationsdiensten zur Verfügung stellen.
- **Telekommunikationsdienste** sind alle Dienstleistungen, die in Netzen eine Informationsübertragung in Form von Signalen, Sprache, Daten, Text und Bildern ermöglichen oder in Verbindung mit einer Informationsübertragung angeboten werden. Dies sind insbesondere der Telefondienst, Dienste für die elektronische Datenübertragung, Mehrwertdienste oder besondere Dienste der mobilen Kommunikation.
- **Telekommunikationseinrichtungen** sind Vermittlungseinrichtungen, Übertragungswege, Anschalteeinrichtungen und Endeinrichtungen mit den erforderlichen Hard- und Softwarekomponenten.

1.5 Verantwortlichkeiten

1.5.1 Grundsatzangelegenheiten

- (1) Die Finanzbehörde ist verantwortlich für die Entwicklung konzeptioneller Vorgaben für die Telekommunikation im Rahmen der Organisationspolitik des Senats. Dies umfasst insbesondere die Definition der Ziele, die Vorgabe von Rahmenbedingungen und Anforderungen, die Leitplanung, die Festlegung von Standards sowie das Initiieren und die Mitwirkung an behördenübergreifenden Pilotprojekten. Die Finanzbehörde wirkt an Rechtssetzungsverfahren des Bundes für den Bereich der Telekommunikation mit und vertritt die FHH gegenüber anderen Ministerien des Bundes und der Länder. Sie ist insoweit oberste Dienstbehörde.

- (2) Die Finanzbehörde kann den Einsatz grundlegend neuer Telekommunikationsdienste, Telekommunikationstechniken und Leistungsmerkmale nach Prüfung der rechtlichen, finanziellen, organisatorischen und sozialen Auswirkungen freigeben und dabei die dauerhafte Nutzung zulassen. Sie wird den Katalog der Leistungsmerkmale in der Anlage L entsprechend dem Stand der Technik fortzuschreiben. Eine notwendige Beteiligung der Personalräte oder der Spitzenorganisationen der Gewerkschaften und Berufsverbände nach Maßgabe des Hmb-PersVG in der jeweils geltenden Fassung bleibt unberührt.
- (3) Zur Vorbereitung der Maßnahmen nach Absatz 2 kann die Finanzbehörde Telekommunikationseinrichtungen, -dienste und Leistungsmerkmale einschließlich der grundlegenden Ergänzung und Erweiterung von Programmen zeitlich und inhaltlich begrenzt probeweise einsetzen lassen. Die von der Pilotierung betroffenen Stellen der hamburgischen Verwaltung sowie die Beschäftigten sind vorher über den probeweisen Einsatz zu informieren; dem Personalrat ist Gelegenheit zur Stellungnahme zu geben, damit ein Einfluss auf die Gestaltung der Pilotierung möglich ist. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit ist rechtzeitig gemäß der Richtlinie zur Beteiligung des Hamburgischen Datenschutzbeauftragten in der jeweils geltenden Fassung zu unterrichten. Die Pilotierung soll mit einem Bericht abgeschlossen werden, der neben der Auswertung der praktischen Ergebnisse auch die Erfahrungen der betroffenen Stellen, Personalräte und Beschäftigten enthält.
- (4) Soweit ein in dieser Richtlinie vorgesehenes Einvernehmen zwischen Organisationseinheiten nicht hergestellt werden kann, entscheidet die Finanzbehörde abschließend.

1.5.2 Allgemeine Angelegenheiten des Aufgabenvollzuges

- (1) Anwendende Stellen, die im Rahmen ihrer sachlichen Aufgabenerfüllung IT-Anwendungen in Form von Telekommunikationsdiensten nutzen, sind - innerhalb ihrer Zuständigkeit für die sachliche Aufgabenerledigung - verantwortlich für:
 1. Ermittlung des Bedarfs an Telekommunikationseinrichtungen und -diensten, einschließlich der Festlegung der notwendigen Leistungsmerkmale,
 2. Ausstattung der Arbeitsplätze mit Telekommunikationseinrichtungen,
 3. Beantragung von Berechtigungsklassen für Endeinrichtungen, insbesondere für Ferngespräche,
 4. Anordnung der befristeten Speicherung von ungekürzten Verbindungsdaten nach Maßgabe von Ziffer 2.3 Absatz 7 dieser Richtlinie,
 5. Vergabe von Berechtigungen oder Festlegung der Benutzerprofile bei der Verarbeitung sensibler Daten oder der Nutzung von Mehrwertdiensten,
 6. Einhaltung der telekommunikationsrechtlichen Regelungen und Vorgaben,
 7. Gewährleistung des Datenschutzes und der gesicherten, wirtschaftlichen, recht- und ordnungsmäßigen Nutzung durch technische und organisatorische Maßnahmen,

8. Prüfung der Voraussetzungen für die Nutzung von Leistungsmerkmalen nach Maßgabe dieser Richtlinie,
 9. Schulung und Einweisung der Beschäftigten in die gesetzlichen und sonstigen Regelungen sowie in die Benutzung der Telekommunikationseinrichtungen und –dienste,
 10. Bereitstellung geeigneter Technikräume für Telekommunikationseinrichtungen und die dazugehörige Infrastruktur zur unentgeltlichen Nutzung des Netzbetreibers.
- (2) Die anwendenden Stellen bleiben für die ordnungsgemäße Erledigung der Aufgaben auch dann verantwortlich, wenn sie diese einem Dritten übertragen.
- (3) Für die Bedienung von Telefonzentralen (Abfrageeinrichtungen), die mehrere Stellen unterstützen, ist die Stelle verantwortlich, der die Hausverwaltung des Grundstücks obliegt, auf dem die dazugehörige Vermittlungseinrichtung betrieben wird. Mit der für die Bedienung der Abfrageeinrichtung verantwortlichen Stelle ist über alle Maßnahmen, die den Umfang des Telefondienstes beeinflussen, Einvernehmen herzustellen. Vereinbarungen nach § 94 HmbPersVG über den telefonischen HamburgService bleiben unberührt.
- (4) Netzbetreiber und anwendende Stellen sind dafür verantwortlich, dass organisatorische und technische Sicherungsmaßnahmen getroffen, insbesondere die Beschäftigten auf korrekte Benutzung, Risiken und Problembereiche hingewiesen werden. Alle Beschäftigten sind verpflichtet, die vorgegebenen organisatorischen Sicherungsmaßnahmen einzuhalten und die technischen Sicherungsmaßnahmen (z. B. Schlüssel, Passwörter usw.) zu nutzen. Sie haben die anwendende Stelle auf Mängel oder Schwachstellen im Sicherheitskonzept hinzuweisen.

1.5.3 Betriebliche Angelegenheiten

- (1) Dataport ist als Netzbetreiber verantwortlich für die Planung, Errichtung, Instandhaltung, Optimierung und den Betrieb des Hamburgischen TK-Netzes sowie für die Unterstützung der anwendenden Stellen und der lokalen Netzbetreiber. Dataport hat geeignete Vorsorgemaßnahmen zur Behebung von Störungen und Ausfällen zu treffen. Konkrete Pflichten und Rechte Dataports als Netzbetreiber werden in einer Vereinbarung zwischen der FHH und Dataport geregelt.
- (2) Lokale Netzbetreiber nehmen die betrieblichen Angelegenheiten ihrer lokalen Netze wahr. Sie sind für die Planung, Errichtung, technische Weiterentwicklung, Instandhaltung und den Betrieb ihrer lokalen Netze verantwortlich. Sie haben geeignete Vorsorgemaßnahmen zur Behebung von Störungen und Ausfällen zu treffen. Neue lokale Netze sind nach Maßgabe der IT-Planungen einzurichten. Lokale Netzbetreiber sind in der Regel zugleich anwendende Stellen.
- (3) Anwendende Stellen sind für die ordnungsgemäße und wirtschaftliche Benutzung von Telekommunikationseinrichtungen verantwortlich.
- (4) Lokale Netzbetreiber können für ihren Wirkungsbereich Verträge mit öffentlichen Telekommunikationsdienste-Anbietern abschließen, wenn sie sich auf die sprachliche Telekommunikation oder auf Telekommunikationsdienste ohne

Verbindung zum Hamburgischen TK-Netz beschränken und wenn dies wegen besonderer Dringlichkeit, des Erfordernisses spezieller Fachkenntnisse oder zur Abwendung von finanziellen Nachteilen erforderlich ist. Sie haben hierzu das Einvernehmen mit Dataport herzustellen. Das Einvernehmen ist nicht erforderlich für die Bereiche der Polizei, der Feuerwehr und des Verfassungsschutzes.

1.5.4 Vergabeangelegenheiten

Bei Aufträgen zur Lieferung bzw. Bereitstellung von Telekommunikationseinrichtungen und Telekommunikationsdiensten sind die vergaberechtlichen Vorschriften zu beachten. Sofern die Vergabe nicht selbst von Dataport durchgeführt wird, ist Dataport bei der Vorbereitung der Auftragsvergabe zu beteiligen.

1.5.5 Entscheidungskompetenz

Soweit nach dieser Richtlinie Entscheidungen erforderlich sind, die einzelne Beschäftigte oder Fragen betreffen, die der Beteiligung nach dem HmbPersVG unterliegen, trifft sie der Leiter der Dienststelle oder ein zu dessen Vertretung bestimmter entscheidungsberechtigter Beamter oder Angestellter. Die Verantwortlichkeit des Beauftragten für den Haushalt bleibt unberührt.

1.5.6 Überörtliche Aufgaben

Unberührt bleibt die Verantwortlichkeit der Behörden und Organisationen mit Sicherheitsaufgaben insbesondere für die Nutzung von Funkdiensten. Unberührt bleiben auch Verantwortlichkeiten, die sich aus Rechtsvorschriften des Bundes oder aus vertraglichen Verpflichtungen der Freien und Hansestadt Hamburg gegenüber den Europäischen Gemeinschaften, dem Bund oder den anderen Bundesländern ergeben.

2. Benutzung der Telekommunikationseinrichtungen und -dienste

2.1 Allgemeines

- (1) Der Telekommunikation ist der Vorzug vor anderen Versand- oder Kommunikationsformen zu geben, wenn und soweit rechtliche oder sonstige Gründe den Einsatz nicht ausschließen oder unzumutbar erscheinen lassen.
- (2) Für die Telekommunikation der anwendenden Stellen untereinander ist das Hamburgische TK-Netz zu benutzen. Öffentliche oder private Telekommunikationsnetze Dritter dürfen nur benutzt werden, wenn der gewünschte Teilnehmer nicht oder nicht rechtzeitig über das Hamburgische TK-Netz erreicht werden kann oder der Dienst nicht angeboten wird.
- (3) Originale sind beim elektronischen Versand von Dokumenten nur dann nachzusenden, wenn dies aufgrund von Rechtsvorschriften oder wegen der Bedeutung der Sache erforderlich ist.

2.2 Brief-, Post- und Fernmeldegeheimnis

- (1) Das Brief-, Post- und Fernmeldegeheimnis sowie das Recht auf informationelle Selbstbestimmung werden bei der Telekommunikation zwischen den Stellen der hamburgischen Verwaltung sowie bei der Verarbeitung von Betriebs-, Teilnehmer- und Verbindungsdaten gewährleistet. Vertrauliche Dokumente sind bei der Informationsübertragung durch geeignete Sicherungsmaßnahmen zu schützen. Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses durch Rechtsvorschriften bleiben unberührt.
- (2) Sowohl die übermittelten Informationen als auch die näheren Umstände der Telekommunikation sind vor unzulässiger Kenntnisnahme und Nutzung zu schützen. Anspruch auf diesen Schutz haben stets beide Teilnehmer der Telekommunikation, neben den Beschäftigten also auch die Bürgerinnen und Bürger sowie Unternehmen. Unzulässig ist z. B. das Mithören von Telefongesprächen - Privat- und Dienstgespräche - durch Vorgesetzte ohne Einwilligung des Beschäftigten und des Gesprächspartners. Auch das unbefugte Lesen von Briefen, Texten, Daten und Bildern auf Bildschirmen oder von ausgedruckten Inhalten aus Speichermedien ist nicht zulässig.
- (3) Wer Kenntnis vom Inhalt eines Telefongesprächs oder eines Dokuments erhält, ohne Empfänger zu sein, ist zur Verschwiegenheit verpflichtet.
- (4) Beschäftigte, die im Rahmen der Aufgaben von Netzbetreibern erweiterte Zugriffsrechte oder Einwirkungsmöglichkeiten besitzen und nicht Amtsträger sind, sind auf die gewissenhafte Erfüllung ihrer Obliegenheiten nach dem Gesetz über die förmliche Verpflichtung nichtbeamteter Personen vom 2.3.1974 (Verpflichtungsgesetz) in der jeweils geltenden Fassung zu verpflichten. Die Niederschrift über die förmliche Verpflichtung ist zur Personalakte zu nehmen. Lieferanten und Auftragnehmer von Wartungsaufgaben sind vertraglich zur Geheimhaltung zu verpflichten.
- (5) Die anwendenden Stellen prüfen, ob die in Absatz 1 genannten Rechte unter Berücksichtigung der besonderen Anforderungen einzelner Arbeitsplätze gewahrt bleiben, soweit die in Anlage L genannten Leistungsmerkmale zur Verfügung stehen. Die anwendenden Stellen haben bei Unverträglichkeit unverzüglich eine Nutzung einzelner Leistungsmerkmale für die betreffenden Endeinrichtungen auszuschließen.

2.3 Sicherungsmaßnahmen

- (1) Es sind die Sicherungsmaßnahmen zu treffen, die erforderlich sind, um die in Ziffer 2.2 Absätze 1 und 2 genannten Rechte zu schützen sowie die Datensicherheit zu gewährleisten. Dabei sind sowohl die schutzwürdigen Interessen Dritter als auch die der Beschäftigten zu sichern.
- (2) Art und Umfang der Sicherungsmaßnahmen haben sich an der Sensibilität der Informationen und personenbezogenen Daten sowie der Funktionalität und der Leistungsfähigkeit der Telekommunikationseinrichtungen und -dienste unter Beachtung des Grundsatzes der Verhältnismäßigkeit zu orientieren. Bei programmierbaren Telekommunikationseinrichtungen sind die gleichen Maßstäbe anzulegen, die für die automatisierte Verarbeitung personenbezogener Daten gelten.

- (3) Vermittlungseinrichtungen sind durch technische und organisatorische Maßnahmen gegen unbefugten Zugang zu schützen. Die Netzbetreiber regeln die Einzelheiten des Zugangs, der Einrichtung, Wartung, Instandsetzung und Administration. Dabei sind Angaben über die ausführenden Personen, die vorgenommenen Eingriffe in den Betrieb der Vermittlungseinrichtungen und erkannte Störungen nachprüfbar zu dokumentieren.
- (4) Zentrale Telekommunikationseinrichtungen - wie Vermittlungseinrichtungen -, die in separaten Räumen aufgestellt sind, müssen durch besondere Vorrichtungen zur Raumsicherung (z. B. Sicherheitsschlösser, elektronische Sicherungen) gesichert sein. Das gilt auch für die Betriebsterminals, über die diese Einrichtungen verwaltet, gesteuert, aktiviert oder deaktiviert werden.
- (5) Wenn zentrale Telekommunikationseinrichtungen in Gebäuden untergebracht sind, deren Hausverwaltung von einer Stelle wahrgenommen wird, die nicht gleichzeitig Netzbetreiber ist, trägt der Netzbetreiber die Kosten der Raumsicherung, soweit sie über die im Gebäude üblichen Sicherungsmaßnahmen hinausgehen.
- (6) Die Gestaltungs- und Eingriffsrechte in den Leistungsumfang von Vermittlungseinrichtungen sind auf einen für den Betrieb unerlässlichen Personenkreis zu beschränken. Manipulationen und Missbrauch sind durch organisatorische und technische Maßnahmen (Zugangslisten, Identifikationskarten, Passwörter o.ä.) zu unterbinden. Für die Nutzung der technischen Zugangs- und Zugriffskontrollmechanismen ist die Richtlinie zur Verwaltung von Passwörtern (Passwortrichtlinie - Passwort-RL) in der jeweils geltenden Fassung entsprechend anzuwenden.
- (7) Auf Einzelbindungsnachweise für Telekommunikationsdienste ist grundsätzlich zu verzichten. Zur Aufklärung von Unstimmigkeiten sowie des Verdachts eines Dienstvergehens oder einer Verletzung arbeitsvertraglicher Pflichten können beim Netzbetreiber befristet Einzelbindungsnachweise mit ungekürzten Verbindungsdaten beantragt werden. Der zuständige Personalrat ist zu unterrichten.

2.4 Nutzung durch Dritte

- (1) Behördenbesuchern kann ausnahmsweise gestattet werden, dienstliche Telefon- und Telefaxeinrichtungen zu nutzen, wenn der Dienstbetrieb dadurch nicht gestört wird und keine nennenswerten Kosten entstehen. Auf eine Kostenerstattung wird verzichtet.
- (2) Dritten kann im Einzelfall ein drahtloser Zugang zum Internet auf ihren eigenen Endgeräten gewährt werden, wenn ein dienstliches Interesse besteht und durch technische und organisatorische Maßnahmen die erforderliche Datensicherheit gewährleistet wird, d.h. mit Ausnahme des Internetzugangs der Zugriff auf das Hamburgische TK-Netz ausgeschlossen wird.
- (3) Dritten, die in Verwaltungsgebäuden oder öffentlichen Einrichtungen ihre Geschäfts- oder Betriebsräume haben, dürfen keine Anschaltseinrichtungen oder Endeinrichtungen des Hamburgisches TK-Netzes oder lokaler Netze zur Verfügung gestellt werden.

- (4) Dritten kann über den Zugang zum Internet gemäß Absatz 2 hinaus ein Zugang mit ihren eigenen Endgeräten zum Hamburgischen TK-Netz gewährt werden, wenn hierfür im Einzelfall ein dienstliches Interesse besteht und die erforderliche Datensicherheit durch technische und organisatorische Maßnahmen gewährleistet ist. Eine Sicherheitskonzeption legt Einzelheiten fest, insbesondere die Anforderungen an die Authentifizierung, detaillierte Zugriffsregelungen, technische Vorkehrungen in der Infrastruktur sowie die Festlegung zulässiger Endgeräte. Dritte, die beim Zugang auf das Hamburgische TK-Netz ihren Geschäfts- oder Betriebsaufgaben nachgehen, sollen solche Endgeräte einsetzen, die sie in ihrem eigenen dienstlichen Kontext verwenden. Die Verpflichtung zur Einhaltung der IT-Vorschriften der Freien und Hansestadt Hamburg ist gesondert mit den Dritten zu vereinbaren.

2.5 Einzelregelungen für zugelassene Telekommunikationsdienste

2.5.1 Telefondienst

- (1) Die anwendenden Stellen bestimmen, für welche Endeinrichtungen Berechtigungsklassen für Ferngespräche durch den Netzbetreiber einzurichten sind.
- (2) Bei Anschlüssen im Telefondienst, für die keine Entgelte erhoben werden, entscheidet die anwendende Stelle über eine generelle Freischaltung. Eine Freigabe dienstlich notwendiger, kostenpflichtiger Verbindungen kann über Kurzwahlruffnummern oder andere Freigabemöglichkeiten erfolgen.
- (3) Dienststellen mit Beratungsaufgaben, die bei telefonischer Beratung den Anrufern aus Rechtsgründen, oder weil dies sonst üblich ist, Anonymität gewähren, sind auf deren Antrag mit Fernsprengeräten ohne Display auszustatten oder es ist für die entsprechenden Endeinrichtungen die Unterdrückung der Rufnummern der anrufenden Teilnehmer sicherzustellen.

2.5.2 Elektronischer Versand von Dokumenten

- (1) Gegen die unbefugte Einsichtnahme und die irrtümliche Zustellung der Dokumente sind geeignete technische und organisatorische Maßnahmen zu treffen. Die Endeinrichtungen für diese Dienste dürfen nicht unkontrolliert zugänglich sein.
- (2) Zur Gewährleistung der Sicherheit der beim elektronischen Dokumentenversand eingesetzten Rechner sind die für den jeweiligen Rechnertyp geltenden Sicherheitsbestimmungen (z.B. PC-RL, Passwort-RL) zu beachten. Die eingesetzten Rechner müssen über einen wirksamen Viren-Schutz verfügen. Die Maßnahmen umfassen nicht nur die Überprüfung der eingegangenen Dokumente, sondern auch die Gegenmaßnahmen nach einem Virenbefall.
- (3) Die Funktion „Weiterleitung“ darf nur verwendet werden, wenn gewährleistet ist, dass die Dokumente nicht von Unbefugten gelesen werden.
- (4) Enthält das Dokument besonders sensible Daten, insbesondere sensible personenbezogene Daten, ist durch geeignete Maßnahmen die missbräuchliche Kenntnisnahme seines Inhaltes auszuschließen; ggf. müssen die Dokumente zur Übertragung verschlüsselt werden.

2.5.2.1 Elektronische Post (E-Mail)

2.5.2.1.1 Organisation der elektronischen Post (E-Mail)

- (1) Der elektronische Postdienst wird über das Hamburgische TK-Netz durch Data-port betrieben. Außenverbindungen werden ausschließlich über einen zentralen Mailserver realisiert.
- (2) Wird die elektronische Post (E-Mail) im Umfeld sensibler Anwendungen eingesetzt, so sind nach den Anforderungen des Einzelfalles technische und/oder organisatorische Maßnahmen vorzusehen, um den unerlaubten, insbesondere versehentlichen Versand von Dokumenten mit sensiblen Inhalten auszuschließen. Erforderlichenfalls ist der Postversand aus der sensiblen Anwendung oder der Versand von Anlagen insgesamt zu unterbinden.
- (3) Zur Sicherstellung eines ordnungsgemäßen Geschäftsganges ist festzulegen, wie die Postfächer, die keiner bestimmten Person zugeordnet sind (Funktionspostfächer wie z.B. "Poststelle", "Geschäftsstelle" o.ä.), überwacht und die Weiterverteilung der eingegangenen Post sichergestellt wird.
- (4) Falsch adressierte oder unzustellbare Post ist nach Information des Absenders zu löschen. Über deren Inhalt ist Verschwiegenheit zu wahren.
- (5) Der Versand bzw. die Weiterleitung digitaler Kettenbriefe und Massen-E-Mails mit nicht-dienstlichem Inhalt sind unzulässig.
- (6) Zur Gewährleistung der Betriebssicherheit und der Verfügbarkeit der elektronischen Post dürfen Maßnahmen eingesetzt werden, die den Versand bzw. die Zustellung eingehender als gefährdend oder belästigend erkannter E-Mails verhindert (SPAM-Filter). Eingehende E-Mails, bei denen Zweifel über ihren gefährdenden oder belästigenden Charakter bestehen, sind dem Empfänger in einem Quarantänebereich zur weiteren Bearbeitung zur Verfügung zu stellen.

2.5.2.1.2 Administration der elektronischen Post (E-Mail)

Die für die elektronische Post eingesetzte Software ist so zu konfigurieren, dass jeder Benutzer unter seiner Benutzerkennung nur die Möglichkeit hat, sein eigenes Postfach und die seiner Benutzerkennung zugeordneten Postfächer (Funktionspostfächer und Vertreter-Postfächer) zu öffnen. Der Zugang ist durch Vergabe eines den Anforderungen der Passwort-Richtlinie entsprechenden Passwortes abzusichern.

2.5.2.1.3 Benutzung der elektronischen Post (E-Mail)

- (1) Der Benutzer hat sein elektronisches Postfach regelmäßig (mindestens einmal arbeitstäglich) auf eingegangene Post zu kontrollieren. Elektronische Posteingänge sollten - soweit möglich - elektronisch weiterverarbeitet werden. Die Post ist, soweit es sich nicht um persönliche Mitteilungen handelt, im vorgeschriebenen Geschäftsgang zu bearbeiten. Soweit dies aus Gründen der Revisionsicherheit und für das Verständnis oder das Nachvollziehen der Bearbeitung eines Vorganges erforderlich ist, sind E-Mails entsprechend den geltenden Regelungen zu den Akten nehmen.

- (2) Bei einer absehbaren Abwesenheit vom Arbeitsplatz (z.B. wegen Urlaub, Dienstreise oder Dienstgang, Fortbildung, Abwesenheit auf Grund entsprechender Arbeitszeitverteilung), die länger als einen Arbeitstag dauert, sind die Absender von E-Mails in geeigneter Weise, z.B. durch Einstellen des Abwesenheitsassistenten, über die zu erwartende Dauer der Abwesenheit, die getroffene Vertretungsregelung und darüber zu unterrichten, ob und ggf. an wen die E-Mails weitergeleitet werden.
- (3) Bei unvorhersehbarer Abwesenheit vom Arbeitsplatz, die länger als drei Tage dauert (z.B. bei Erkrankung), kann der zuständige Amtsleiter oder eine von ihm beauftragte Person die Einschaltung des Abwesenheits- und Vertretungsassistenten veranlassen oder, falls dies im Einzelfall nicht ausreicht, um die Bearbeitung elektronischer Posteingänge sicherzustellen, weitere Maßnahmen treffen (insbesondere Öffnung des Postfaches). Als „privat“ gekennzeichnete oder als solche erkennbare Nachrichten dürfen von der Vertretung nicht geöffnet werden. Wird ein solcher Eingang versehentlich geöffnet oder ergibt sich erst bei versehentlicher Lektüre, dass die Nachricht privater Natur ist, ist die Nachricht unverzüglich zu schließen und der Inhalt vertraulich zu behandeln. Dies gilt auch, falls es vergessen wurde, die notwendigen Vorkehrungen bei einer länger als drei Tage andauernden Abwesenheit zu treffen. Über die getroffenen Maßnahmen ist der Besitzer bzw. die Besitzerin des Postfachs unverzüglich nach Rückkehr zu informieren.
- (4) Beim Versand elektronischer Post, die sich nicht an bestimmte Personen richtet, ist als Adressat ein Funktionspostfach (z.B. „Poststelle“ bzw. „Geschäftsstelle“) zu wählen, um die sichere und termingerechte Kenntnisnahme zu gewährleisten.
- (5) Beim Versenden von Anlagen ist besondere Aufmerksamkeit auf die korrekte Auswahl der Anlagen zu richten. Vorhandene technische Möglichkeiten zur Vermeidung von Irrtümern (z.B. Dokumentenversand aus dem Dokument heraus) sind zu nutzen.
- (6) Zum Nachweis des Versands elektronischer Post kann die Möglichkeit der Zustellbestätigung genutzt werden.
- (7) Anlagen sind soweit möglich in den gemäß der IT-Architektur-RL standardisierten Formaten zu versenden. Die Verantwortung für notwendige Konvertierungen trägt der Empfänger.
- (8) Der direkte Versand ausführbarer Programme sowie das Ausführen empfangener ausführbarer Programme aus der Postfunktion heraus sind untersagt.
- (9) Besonders sensible, insbesondere sensible personenbezogene Daten, dürfen über die elektronische Post nur verschlüsselt versandt werden, soweit nicht durch andere Maßnahmen eine gleichwertige Sicherheit gewährleistet ist.

2.5.2.2 Fernkopieren (Telefax, E-Fax)

- (1) Bei der Übermittlung von Informationen über den Telekommunikationsdienst Fernkopieren (Telefax und E-Fax) trägt der Absender die Verantwortung für die vertrauliche Versendung der Informationen. Daher sollten

- alle der Sicherheit dienenden Einrichtungen des Gerätes genutzt werden, insbesondere die Anzeige des erreichten Anschlusses, und
- durch persönliche Anwesenheit am Gerät gewährleistet werden, dass kein Unbefugter die zu versendenden Daten einsehen kann.

Nach der Übermittlung von Informationen über Telefax und E-Fax trägt der Empfänger die Verantwortung für die weitere vertrauliche Behandlung der Informationen, insbesondere ist beim Empfang einer Sendung der Absender über fehlende Seiten oder andere aufgetretene Störungen zu informieren.

- (2) Sensible Daten, insbesondere sensible personenbezogene Daten, sollen nicht per Telefax oder E-Fax versandt werden.
- (3) Ist der Versand sensibler Daten erforderlich, soll
 - mit dem Empfänger der konkrete Zeitpunkt der Übermittlung vereinbart werden und
 - während des Versands oder des Empfangs durch die persönliche Anwesenheit am Gerät gewährleistet werden, dass kein Unbefugter die Daten einsehen kann.
- (4) Medizinische Gutachten, Krankenberichte oder andere ärztliche Dokumente mit personenbezogenen Angaben dürfen aus Gründen des Datenschutzes und wegen einer etwaigen Verletzung der ärztlichen Schweigepflicht grundsätzlich nicht als Telefax oder E-Fax versandt werden. Derartige Unterlagen dürfen ausnahmsweise nur dann per Telefax oder E-Fax versandt werden, wenn dies zur Wahrnehmung gesetzlich zugewiesener Aufgaben unbedingt erforderlich oder zur Abwehr von Gefahren für Leib und Leben geboten ist.

2.5.3 Informationsdienste

- (1) Anwendungen mit Verbindungen zu öffentlichen Informationsdatenbanken und Auskunftssystemen (Internet) werden nach Maßgabe der IT-Planungen zugelassen.
- (2) Unzulässig ist jede absichtliche oder wissentliche Nutzung von Informationsdiensten, die gegen geltende Rechtsvorschriften verstößt oder geeignet ist, die Sicherheit des TK-Netzes zu beeinträchtigen.
- (3) Die anwendenden Stellen können den Zugriff auf bestimmte Informationsangebote einschränken.
- (4) Die Finanzbehörde kann den Zugriff auf Informationsangebote, die dienstliche Belange verletzen, insbesondere solche mit pornografischen, sitten- oder rechtswidrigen Inhalten, ausschließen, soweit diese im Einzelfall nicht für dienstliche Zwecke benötigt werden.

2.5.4 Fernwirkdienste

- (1) Die nachfolgenden Bestimmungen regeln die Fernwirkdienste als Telekommunikationsdienste, so dass diese Bestimmungen unabhängig davon anzuwenden sind, ob es sich um eine DV-Anlage oder eine Telekommunikationseinrichtung im engeren Sinne handelt.

- (2) Telekommunikationsdienste zum Einwirken auf technische Anlagen und Geräte (Fernüberwachen, Ferndiagnosen, Fernmessen, Fernschalten oder Fernwartung) sind zulässig. Müssen personenbezogene Daten verarbeitet werden oder besteht Zugang zu personenbezogenen Daten, gilt Ziffer 4.1 Absatz 1 entsprechend.
- (3) Besondere Sorgfalt ist bei solchen Fernwirkdiensten geboten, bei denen
1. gemessene Leistungen oder Werte bestimmten Personen zugeordnet werden können,
 2. Personenangaben von Beschäftigten im Zusammenhang mit Arbeiten oder Kontrollen an überwachten oder überwachenden Anlagen automatisch aufgezeichnet werden,
 3. personenbezogene Daten oder vertrauliche Informationen den Benutzern von Fernwirkdiensten bekannt werden können.
- In den Fällen nach Nr. 1 und Nr. 2 sind die Betroffenen grundsätzlich vorher in Kenntnis zu setzen und über die Notwendigkeit und den Zweck der Aufzeichnung zu informieren.
- (4) Werden Aufgaben der Systemverwaltung einem Dritten außerhalb des TK-Netzes übertragen, der diese Aufgabe mit Hilfe von Fernwirkdiensten wahrnimmt (Fernwartung), so sind die erforderlichen organisatorischen und technischen Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit zu treffen und die Pflichten des Auftragnehmers schriftlich festzulegen. Bei der Fernwartung sind zur Gewährleistung der Datensicherheit mindestens folgende Maßnahmen vorzusehen:
1. Der Auftrag muss folgende Einzelheiten regeln:
 - a) Art und Umfang der Wartung,
 - b) Festlegen der zur Fernwartung berechtigten Personen,
 - c) Anmelden der Wartungsmaßnahme,
 - d) Bereitstellung und Benutzung von Kenn- und Passwörtern,
 - e) Verpflichtung auf Datengeheimnis und Verschwiegenheit,
 - f) Verbot der Datenweitergabe,
 - g) Verbot der Verwendung der Daten für andere als die durch den Auftrag festgelegten Zwecke,
 - h) Löschen sämtlicher Daten durch den Auftragnehmer, die bei der Fernwartung von der gewarteten Telekommunikationseinrichtung oder DV-Anlage übertragen oder auf andere Weise übermittelt wurden.
 2. Der Auftraggeber hat sicherzustellen, dass er vor Beginn einzelner Maßnahmen informiert wird, um die Eingriffe überprüfen und um zusätzliche Maßnahmen zur Datensicherung ergreifen zu können.
 3. Die Verbindung zum Auftragnehmer ist durch die fachlich zuständige Systemadministration aufzubauen oder zu ermöglichen. Manuelle Eingaben sind durch geeignete Maßnahmen zu verifizieren.
 4. Der Auftragnehmer arbeitet unter einer besonderen Wartungskennung.
 5. Der Auftragnehmer identifiziert und authentisiert sich durch Eingabe seiner Wartungskennung und seines Passwortes oder andere geeignete Maßnahmen.
 6. Die Fernwartungstätigkeiten sind von der fachlich zuständigen Systemadministration zu überwachen. Bei Unregelmäßigkeiten muss der Netzbetreiber die Fernwartungsverbindung abbrechen.
 7. Beim Einsatz neuer Versionen, Korrekturen oder Änderungen des Betriebssystems, von allgemeiner Software oder Anwendungssoftware im Wege der Fernwartung sind die Vorschriften der Freigaberichtlinie einzuhalten.

8. Der Zugriff auf den Produktionsbetrieb durch den Auftragnehmer im Rahmen der Fernwartung ist grundsätzlich auszuschließen. Test und Serviceprogramme des Auftragnehmers, die auf der Telekommunikationseinrichtung gespeichert sind, dürfen nur dem Auftragnehmer und dem Systemverwalter zugänglich sein.
9. Passwörter für Benutzerkennungen, System- oder Anwendungsdateien, von denen der Auftragnehmer ausnahmsweise Kenntnis erhalten hat, sind unmittelbar nach Beendigung der Maßnahme zu ändern.
10. Aufzeichnungen über Störungen, Speicherauszüge und Fernwirkmaßnahmen sind wie andere Betriebsdaten in Dateien der zu wartenden Telekommunikationseinrichtung abzulegen. Bei Bedarf veranlasst die fachlich zuständige Systemadministration die Datenübermittlung zum Auftragnehmer. Die Übermittlung von Dateien mit personenbezogenen Daten ist von autorisierten Beschäftigten freizugeben. Der Umfang der Protokollierung und die Speicherung von Betriebsdaten richten sich nach Ziffer 4.1. dieser Richtlinie.
11. Die Einhaltung der Sicherheitsmaßnahmen ist in unregelmäßigen Abständen zu überprüfen. Die mit der Überwachung der Fernwartung betrauten Beschäftigten sind regelmäßig im Hinblick auf diese Aufgabe zu schulen.

2.5.5 Mobile Kommunikation

- (1) Telekommunikationseinrichtungen für die mobile Kommunikation können zur Verbesserung der Mobilität sowie zur Sicherstellung der Information von Beschäftigten und der Kommunikation mit Beschäftigten außerhalb der eigenen Diensträume eingesetzt werden.
- (2) Bei programmgesteuerten mobilen Endeinrichtungen für den elektronischen Versand von Dokumenten sind Sicherheitskomponenten einzusetzen. Die für den jeweiligen Rechnertyp geltenden Sicherheitsbestimmungen (z.B. PC-RL) sind zu beachten.
- (3) Über die Bereitstellung und Nutzung von mobilen Endeinrichtungen mit unmittelbarem Anschluss an Netze Dritter entscheiden die anwendenden Stellen.

3. Leistungsmerkmale

- (1) Die anwendenden Stellen entscheiden über den Einsatz und das Aktivieren und Deaktivieren von Leistungsmerkmalen für ihren Aufgabenbereich.
- (2) Das Aktivieren und Deaktivieren von Leistungsmerkmalen sowie sonstige erforderliche technische Maßnahmen erfolgen auf Antrag der anwendenden Stelle durch den Netzbetreiber. Die Beschäftigten sind durch die anwendende Stelle auf die Regelungen hinzuweisen, die für die Nutzung der jeweiligen Leistungsmerkmale gelten.

3.1 Zulässigkeit von Leistungsmerkmalen

- (1) Die Benutzung der Telekommunikationseinrichtungen ist durch geeignete Leistungsmerkmale und technische Einrichtungen, soweit es den Grundsätzen wirtschaftlichen Verwaltungshandelns entspricht, zu erleichtern.

- (2) Im Telefondienst können Telekommunikationseinrichtungen mit den in der Anlage L genannten Leistungsmerkmalen nach Maßgabe dieser Richtlinie genutzt werden.
- (3) Für die nicht-sprachlichen Telekommunikationsdienste sind die Leistungsmerkmale zugelassen, die den in Anlage L genannten Leistungsmerkmalen entsprechen. Bestehen bei Leistungsmerkmalen anderer Telekommunikationseinrichtungen und -dienste Zweifel an der Zulässigkeit ihres Einsatzes, so ist die Entscheidung der Finanzbehörde herbeizuführen.
- (4) Die Beschäftigten sind auf die Regelungen hinzuweisen, die für die Nutzung der jeweiligen Leistungsmerkmale gelten.

3.2 Einzelne Leistungsmerkmale im Telefondienst

Leistungsmerkmale können, soweit sie in dem Katalog der Anlage L enthalten sind, nach Maßgabe der nachfolgenden Bestimmungen insbesondere im Hinblick auf deren Art, die rechtlichen und verfahrensmäßigen Voraussetzungen und Bedingungen sowie die technische und organisatorische Gestaltung genutzt werden.

3.2.1 Aufschalten

Eingriffe in Verbindungen des Telefondienstes durch Aufschalten auf Verbindungen, insbesondere durch Beschäftigte an Abfrageeinrichtungen, dürfen nur in dringenden Fällen zur Abwicklung des Telefondienstes und im Rahmen betrieblicher Aufgaben vorgenommen werden. Es ist sicherzustellen, dass die betroffenen Teilnehmer durch ein deutliches Signal von dem Aufschalten Kenntnis erhalten.

3.2.2 Anrufumleitung

- (1) Bei Anrufumleitungen sind die betroffenen Beschäftigten soweit technisch möglich vor der Nutzung des Leistungsmerkmals zu unterrichten.
- (2) Durch die Anrufumleitungen dürfen schutzwürdige Belange der Anrufenden nicht gefährdet werden.

3.2.3 Selbsttätige Rufweitschaltung

Die Einführung dieses Leistungsmerkmals setzt voraus, dass schutzwürdige Belange Anrufender nicht entgegenstehen. Die betroffenen Beschäftigten sind soweit technisch möglich vor dem Aktivieren des Leistungsmerkmals zu unterrichten.

3.2.4 Freisprechen und Mithören

Das Mithören Dritter über Mithöreinrichtungen an der Endeinrichtung, z. B. Zweithörer, Lautsprecher, sind nur zulässig, wenn der Gesprächspartner vor der Nutzung des Leistungsmerkmals zugestimmt hat. Das Mithören im Wege der Raumüberwachung durch Telekommunikationseinrichtungen ist unzulässig. Geräte, die dieses Leistungsmerkmal unterstützen, müssen das Abschalten der Funktion durch den Benutzer ermöglichen.

3.2.5 Konferenzschaltungen

Konferenzschaltungen sind nur zulässig, wenn alle Gesprächspartner vor der Nutzung des Leistungsmerkmals zugestimmt haben.

3.2.6 Rufnummernanzeige

- (1) Die Beschäftigten haben Anzeigen oder Ausgaben von Verbindungsdaten anrunder oder angerufener externer Teilnehmer auf oder durch Endeinrichtungen gegen Kenntnisnahme durch Dritte zu schützen.
- (2) Die Anzeige der Rufnummern von Beschäftigten auf Endeinrichtungen angerufener Teilnehmer ist auf Antrag der Beschäftigten ohne Begründungszwang zu unterdrücken. In den Fällen, in denen aus technischen Gründen in der Vermittlungseinrichtung eine Unterdrückung im Einzelfall nicht möglich ist, entscheidet die anwendende Stelle generell über die Unterdrückung der Rufnummernanzeige für ihren Bereich. In diesem Fall ist ein Mitbestimmungsverfahren mit dem örtlichen Personalrat durchzuführen.

3.2.7 Sprachspeicher

- (1) Auf Antrag der anwendenden Stelle können Sprachspeicher im Rahmen der technischen Möglichkeiten zur Verfügung gestellt werden. Bei der Einrichtung von Sprachspeichern für Beschäftigtengruppen sind Anforderungen an die Vertraulichkeit zu beachten.
- (2) Das Aufzeichnen von Gesprächsinhalten ist dem Betroffenen vorher anzuzeigen. In Sprachspeichern aufgezeichnete Gespräche dürfen Dritten nur dann zur Kenntnis gebracht werden, wenn dies zur Aufgabenerfüllung erforderlich ist oder vorher das Einverständnis des Anrufenden eingeholt wurde. Satz 1 gilt nicht, wenn die Aufzeichnung aufgrund von Rechtsvorschriften zulässig ist oder aufgrund besonderer Umstände vom Einverständnis des Betroffenen ausgegangen werden kann.
- (3) Teilbereiche in Sprachspeichern (Sprachbox), die einzelnen Beschäftigten zur Aufzeichnung eingehender Telefongespräche zur Verfügung stehen, sind durch eindeutige Kennungen und durch Kennwörter - regelmäßig numerische Zeichenfolgen - vor unzulässigem Abhören, auch bei Fernabfragen, zu schützen. Sofern Sprachspeicher von verschiedenen Sprechstellen oder von externen Telekommunikationseinrichtungen geöffnet werden können, ist die Passwort-RL sinngemäß anzuwenden. Anrufbeantworter müssen folgende Mindestanforderungen erfüllen:
 1. dreistelliger frei programmierbarer Zugangscode (Passwort),
 2. keine "Notfallsicherung" (d.h. keine automatische Rückstellung des Zugangscodes auf einen Standardwert bei Stromausfall oder Störungen),
 3. Abbruch nach maximal 3 Fehlversuchen bei der Eingabe des Zugangscodes,
 4. abschaltbare Fernabfrage,
 5. keine bzw. abschaltbare Raumüberwachung.

3.2.8 Fangen einer Rufnummer

- (1) Über das Anzeigen oder Aufzeichnen von Rufnummern oder Kennungen anrunder Anschlüsse zur Abwehr von Störungen oder Belästigungen durch Aktivie-

zung entsprechender Leistungsmerkmale hat die anwendende Stelle im Rahmen gesetzlicher Bestimmungen zu entscheiden.

- (2) Bei Störungen und Belästigungen von außen veranlasst Dataport die Ermittlung des Verursachers. Das Aufzeichnen von Rufnummern durch Dienststellen der Polizei und Feuerwehr zum Zwecke der Gefahrenabwehr bleibt unberührt.

4. Telekommunikationsdaten

Betriebsdaten, Teilnehmerdaten und Verbindungsdaten dürfen unter Berücksichtigung der Anforderungen des Datenschutzes und der Datensicherheit auf Telekommunikationseinrichtungen und DV-Anlagen nach Maßgabe dieses Abschnittes verarbeitet werden.

4.1 Betriebsdaten

- (1) Betriebsdaten, von denen auf bestimmte oder bestimmbare Beschäftigte geschlossen werden kann, dürfen bei Erweiterungsmaßnahmen, Wartung oder Störungsbehebung nur erfasst werden, soweit dies aus technischen Gründen oder zur Gewährleistung der Betriebssicherheit erforderlich ist. Personenbezogene Daten sind nicht nur solche, die in Verbindung mit den Namen von Beschäftigten gespeichert werden, sondern auch solche, bei denen sich über Organisationskürzel, Ordnungsnummern, Gerätekennungen oder andere Identifikationsmerkmale Bezüge zu den Beschäftigten herstellen lassen, die diese Geräte nutzen oder bedienen.
- (2) Soweit Verkehrsmessungen zur Ermittlung des Bedarfs an Telekommunikationseinrichtungen Rückschlüsse auf einzelne Beschäftigte zulassen, sollen die Beschäftigten vorher informiert werden.
- (3) Die aktivierten Leistungsmerkmale, installierten Softwarekomponenten sowie die zur Durchführung des Betriebes und der Betriebssicherung notwendigen Angaben von Vermittlungseinrichtungen müssen jederzeit nachprüfbar sein; für DV-Anlagen gilt die Regelung entsprechend. Die Angaben sind zu dokumentieren.
- (4) Die Dateien und Unterlagen mit personenbezogenen Daten sind drei Monate nach der Auswertung zu löschen oder zu vernichten, soweit sie nicht für den laufenden Betrieb erforderlich sind. Die Dateien sind innerhalb der Löschfristen auszuwerten.

4.2 Teilnehmerdaten

- (1) Teilnehmerdaten dürfen für dienstliche Zwecke sowie zur Erleichterung der Kommunikation mit den Bürgern und Bürgerinnen sowie den Unternehmen und sonstigen Einrichtungen ihres Umfeldes verarbeitet werden.
- (2) Von den Beschäftigten dürfen
 1. Name, Vorname, Anrede, Titel/Grad
 2. Dienststelle

3. Dienstanschrift (Postleitzahl, Ort, Strasse, Hausnummer, Raum)
4. dienstliche Kontaktzeiten
5. dienstliche Funktionsbezeichnung, Abteilung, Leitzeichen
6. dienstliche Telefonnummer, Faxnummer, Mobiltelefonnummer
7. dienstliche E-Mail-Adresse
8. personenbezogene Berechtigungskennungen
9. Bezeichnung der Organisationseinheit
10. Angaben zum Aufgabengebiet

erhoben und in Dateien gespeichert werden.

Diese Teilnehmerdaten können in Verzeichnissen ausgedruckt und in üblicher Weise verbreitet werden, soweit nicht gesetzliche Bestimmungen einer Verarbeitung der Angaben ganz oder teilweise entgegenstehen. Eine kommerzielle Verwertung ist untersagt. Die Verbreitung oder Veröffentlichung der Teilnehmerdaten ist unzulässig, wenn durch die Verbreitung oder Veröffentlichung Beschäftigte aufgrund ihrer dienstlichen Aufgabe Gefährdungen oder Belästigungen durch Externe ausgesetzt sein oder diese Risiken nicht ausgeschlossen werden können.

(3) Von anderen Teilnehmern und Unternehmen dürfen

1. Angaben, die auch in den öffentlichen Verzeichnissen der Anbieter von Telekommunikationsdiensten enthalten sind,
2. Rufnummern oder Kennungen einzelner Endeinrichtungen,
3. Namen und Anschriften der Telekommunikationspartner

erhoben und in Dateien gespeichert werden. Die Verbreitung oder Veröffentlichung dieser Daten ist unzulässig.

- (4) In Dateien und Verzeichnissen können auch Angaben ohne Personenbezug als Bezeichnung von Endeinrichtungen oder Anschlüssen genutzt werden. Die Verwendung dieser Angaben unterliegt keinen Beschränkungen.
- (5) Bei der automatisierten Abrechnung privater Ferngespräche ist eine Verarbeitung der Teilnehmerdaten nach Absatz 2 zulässig.
- (6) Teilnehmerdaten sind spätestens drei Monate nach dem Ausscheiden der Beschäftigten in den automatisierten Dateien zu löschen. In den Fällen nach Absatz 3 beginnt die Frist mit dem Zeitpunkt des Bekanntwerdens des Grundes für die Löschung.

4.3 Verbindungsdaten

4.3.1 Umfang der Verbindungsdaten

- (1) Von Verbindungen dürfen folgende Daten erhoben und in Dateien gespeichert werden:
 1. Anlass: dienstlich oder privat,
 2. Status der Informationsübertragung,
 3. Rufnummer oder Kennung des anrufenden Anschlusses, ersatzweise personenbezogene Berechtigungskennungen,
 4. Rufnummer oder Kennung des angerufenen Anschlusses, ersatzweise personenbezogene Berechtigungskennungen,
 5. Beginn und Ende der Verbindung mit Datum und Uhrzeit,
 6. in Anspruch genommener Telekommunikationsdienst nach Art und Umfang (Verbindungseinheiten, Datenmenge),
 7. Entgelt in Euro,
 8. bei Dienstgesprächen zusätzlich die zu belastende Kostenstelle.

Alle internen Verbindungen sind von der Verarbeitung und einer Auswertung ausgeschlossen.

- (2) Im Telefon- und Faxdienst sowie bei Internetverbindungen werden die Rufnummern bzw. die IP-Adressen grundsätzlich um die letzten drei Stellen gekürzt.
- (3) Bei der Übermittlung von Dokumenten im E-Mail-Verkehr werden die protokollierten E-Mail-Adressen grundsätzlich durch Wegfall des Namensteils (vor dem @) gekürzt. Ansonsten unterliegt bei der Übermittlung von Dokumenten die Aufzeichnung von Verbindungsdaten zum Nachweis des Versands, des Empfangs oder aus betrieblichen Anlässen keinen Beschränkungen.

4.3.2 Verarbeitung von Verbindungsdaten

- (1) Verbindungsdaten dürfen nur zur Kostenkontrolle, Statistik und zur Abrechnung privater Telefongespräche genutzt werden. Bei den nicht-sprachlichen Diensten dienen die Verbindungsdaten zusätzlich der Übermittlungskontrolle oder dem Nachweis einer Informationsübertragung. Daten verarbeitende Stelle ist die Beschäftigungsbehörde der Beschäftigten.
- (2) Die Verbindungsdaten sind getrennt für die Abrechnung privater Telefongespräche und die Kostenkontrolle und Statistik der dienstlichen Nutzung der Telekommunikationsdienste zu verarbeiten.
- (3) Für die Übermittlungskontrolle oder den Nachweis einer Informationsübertragung sind die geräte- oder dienstespezifischen Protokolle zu verwenden.

- (4) Die Verarbeitung der Verbindungsdaten wird durch den Netzbetreiber vorgenommen, der die Verbindungsdaten aufzeichnet, im Übrigen durch die anwendende Stelle, die die Abfrageeinrichtungen bedient.
- (5) Bei Kostenkontrollen ist der an der Auswertung beteiligte Personenkreis zu beschränken. Wird wegen des Verdachts einer missbräuchlichen Benutzung ermittelt, ist der zuständige Personalrat vor Beginn der Maßnahme zu informieren.

4.3.3 Löschen von Verbindungsdaten

- (1) Die für die Kostenkontrolle gespeicherten Verbindungsdaten dürfen nicht länger als drei Monate gespeichert werden. Schriftliche Aufzeichnungen sind nach drei Monaten zu vernichten.
- (2) Die für die Abrechnung privater Telefongespräche gespeicherten Daten sind unter Beachtung der Vorschriften des Haushaltsrechts zu löschen. Unterlagen und Dateien, die keine Kassenbelege sind, müssen spätestens drei Monate nach dem Versand des Abrechnungsbescheides vernichtet oder gelöscht werden.
- (3) Das Speichern verdichteter Daten, z.B. Monatsergebnisse je Organisationseinheit, oder die Aufbewahrung der daraus resultierenden Auswertungen ist über einen längeren Zeitraum zulässig, soweit die Daten keinen Bezug auf bestimmte oder bestimmbare Personen zulassen. Über den Zeitraum der Speicherung entscheidet die anwendende Stelle.

5. Dienstliche Nutzung privater Telekommunikationseinrichtungen

5.1 Grundsätze

- (1) Aus dienstlichem Anlass dürfen private Telekommunikationseinrichtungen verwendet werden, wenn dies aus dringenden dienstlichen Gründen erforderlich ist oder die Dienststelle dies genehmigt hat.
- (2) Der Anschluss und die Benutzung privater Endeinrichtungen an Anschalteinrichtungen dienstlicher Telekommunikationseinrichtungen sind unzulässig, sofern nichts anderes geregelt ist.
- (3) Wenn wegen der Besonderheit der Aufgabe die dienstliche Inanspruchnahme der privaten Telekommunikationseinrichtung den zumutbaren Umfang übersteigt oder nachgewiesen wird, dass dauerhaft der private Anschluss nahezu ausschließlich dienstlich genutzt wird, können Beschäftigte
 1. einen Nebenanschluss zu einem behördlichen Hauptanschluss (TK-Anlage),
 2. eine Endeinrichtung mit direktem Anschluss an das Hamburgische TK-Netz oder
 3. einen dienstlichen Telefonanschluss im Netz eines öffentlichen Anbieters von Telekommunikationsleistungen(Dienstanschlüsse) erhalten, wenn dies wirtschaftlich oder zweckmäßig ist. Technische Fragen sind mit dem jeweils verantwortlichen Netzbetreiber abzustimmen. Für die private Nutzung von Dienstanschlüssen gilt Ziffer 6 dieser Richtlinie.

- (4) Über die Einrichtung von Dienstanschlüssen in Wohnungen von Beschäftigten entscheidet unter Anlegen eines strengen Maßstabes der Beauftragte für den Haushalt bzw. eine von ihm autorisierte Stelle. Die einzurichtenden Dienstanschlüsse sind auf jederzeitigen Widerruf zu bewilligen. Die Anerkennung ist nach Ablauf eines Jahres auf ihre Notwendigkeit zu überprüfen. Bei Beschäftigten, bei denen die Voraussetzungen nach Absatz 3 nicht vorliegen, sind die bestehenden Dienstanschlüsse zurückzunehmen.

5.2 Erstattung der Aufwendungen für die dienstliche Nutzung privater Telekommunikationseinrichtungen

- (1) Die Erstattung von Auslagen der Beschäftigten beschränkt sich auf die unmittelbar mit der dienstlichen Benutzung zusammenhängenden Ausgaben, soweit die Auslagen nicht aufgrund anderer Vorschriften (z.B. Hamburgisches Reisekostengesetz) bei Dienstreisen und Dienstgängen erstattet werden.
- (2) Für die Erstattung haben die Beschäftigten die aufgewendeten Beträge der Dienststelle vierteljährlich schriftlich unter Vorlage der jeweiligen Rechnungsbelege mitzuteilen.
- (3) Das Erstattungsverfahren kann durch Zahlung einer Pauschale vereinfacht werden, wenn private Telekommunikationseinrichtungen dauerhaft und regelmäßig für dienstliche Zwecke in Anspruch genommen werden. Veränderungen in der Gewichtung privater und dienstlicher Nutzung sind seitens des Beschäftigten unangefordert der Dienststelle anzuzeigen.
- (4) Weist ein Beschäftigter unter Vorlage von Nachweisen der dienstlichen Einzelverbindungen nach, dass die aufgewendeten Kosten für die dienstliche Benutzung durch die Pauschale wiederholt nicht gedeckt sind, so ist die Pauschale angemessen anzupassen.
- (5) Die vollen Beträge der Fernmelderechnung sind den Beschäftigten unter Vorlage der Fernmelderechnung zu erstatten, wenn die bzw. der Beschäftigte erklärt, dass der Anschluss privat nicht benutzt wird. In Zweifelsfällen kann die Vorlage eines Einzelverbindungsnaachweises verlangt werden.
- (6) Über die Pauschalierung von erstattungsfähigen Aufwendungen nach Absatz 3 entscheidet unter Anlegen eines strengen Maßstabes der Beauftragte für den Haushalt bzw. eine von ihm autorisierte Stelle. Die Anerkennung der erstattungsfähigen Aufwendungen ist auf höchstens 2 Jahre zu befristen und kann bei Vorliegen der Voraussetzungen auf Antrag des Beschäftigten verlängert werden.

6. Private Nutzung dienstlicher Telekommunikationseinrichtungen

- (1) Die private Nutzung dienstlicher Telekommunikationseinrichtungen ist grundsätzlich unzulässig. Gelegentliche Nutzung für private Zwecke ist zulässig, wenn hierdurch dienstliche Belange nicht beeinträchtigt werden. Kostenpflichtige Telekommunikationsdienste, wie z.B. Telefonansagen oder –sonderdienste, dürfen für private Zwecke nicht in Anspruch genommen werden.
- (2) Die Beschäftigten sind verpflichtet, die für private Zwecke entstandenen Verbindungskosten zu erstatten. Zu diesem Zweck haben sie beim Vorliegen der tech-

nischen Möglichkeiten zur automatisierten Verarbeitung von Verbindungsdaten Vorwahl-Verbindungen (z.B. Ferngespräche, Mobilfunkgespräche) über die Eingabe einer entsprechenden Kennziffer als privat zu kennzeichnen.

- (3) Private Telefongespräche sollen den Beschäftigten in Rechnung gestellt werden. Die Dienststellen können jedoch auf die Abrechnung und Erstattung privater Verbindungsentgelte verzichten, wenn dies aus wirtschaftlichen Gründen gerechtfertigt ist, insbesondere wenn der Aufwand für die Rechnungsstellung und den Einzug der Entgelte den Ertrag durch die Erstattung übersteigt.
- (4) Die Dienststelle ist nicht verpflichtet, zum Nachweis der Richtigkeit ihrer Entgeltabrechnung für private Telefongespräche die vollständigen Rufnummern der angerufenen Anschlüsse vorzulegen.

7. Bereitstellung von Telekommunikationseinrichtungen und -diensten am Arbeitsplatz

7.1 Grundsätze

- (1) Die Arbeitsplätze sind entsprechend den Aufgaben und Tätigkeiten der Beschäftigten, den unterschiedlichen Arbeitsfeldern sowie der Organisation der verantwortlichen Stellen auszustatten und so zu gestalten, dass für die Beschäftigten eine möglichst geringe psychische und physische Belastung entsteht. Für Bildschirmarbeitsplätze gelten die entsprechenden Vorschriften zur Gewährleistung der Arbeitssicherheit, Ergonomie und des sonstigen Beschäftigtenschutzes.
- (2) Die technische Ausstattung mit Endeinrichtungen ergibt sich aus der jeweils dienststellenbezogenen zu treffenden Festlegung.

7.2 Anforderungen an die Telekommunikationseinrichtungen

- (1) Die installierten Endeinrichtungen, insbesondere Bildschirme und Drucker, haben den Regeln der Technik und den anerkannten Regeln der Arbeitssicherheit zu entsprechen.
- (2) Soweit für die Nutzung von Telekommunikationsdiensten Programme und Programmteile selbst entwickelt werden, sind die allgemein anerkannten Anforderungen der Softwareergonomie zu berücksichtigen. Bei der Vergabe von Aufträgen für Programme und Programmteile an Dritte ist eine Verwirklichung dieser Anforderungen nachdrücklich anzustreben. Bei der Auswahl konfektionierter Software sind die Anforderungen der Softwareergonomie im Rahmen der Angebote zu berücksichtigen.

7.3 Schulung und Einweisung

- (1) Die anwendenden Stellen haben die Beschäftigten rechtzeitig und ausreichend zu schulen, wenn grundlegend neue Telekommunikationseinrichtungen und -dienste am Arbeitsplatz bereitgestellt werden.
- (2) Den Spitzenorganisationen der Gewerkschaften und Berufsverbände ist Gelegenheit zu geben, an diesen Veranstaltungen teilzunehmen.

- (3) Eine Einweisung der Beschäftigten in die Benutzung der Telekommunikations-einrichtungen erfolgt, soweit es zur Nutzung des verfügbaren Leistungsumfanges notwendig ist und sich die Geräte am Arbeitsplatz befinden oder als regelmäßiges Arbeitsmittel dienen. Bei zentral oder dezentral aufgestellten dienstspezifischen Endeinrichtungen werden nur die für die Gerätebetreuung verantwortlichen Beschäftigten in die Benutzung eingewiesen. Die Bedienungsunterlagen sind beim Gerät aufzubewahren.

8. Übergangs- und Schlussbestimmungen

- (1) Diese Richtlinie tritt am 1. Februar 2010 in Kraft. Zum gleichen Zeitpunkt treten außer Kraft die vom Senat erlassene Richtlinie zur Gestaltung und Benutzung der Telekommunikation in der Verwaltung der Freien und Hansestadt Hamburg (Telekommunikationsrichtlinie - TK-RL) vom 26. Januar 1993 (MittVw Seite 219), zuletzt geändert am 19. Juni 1995 (MittVw Seite 141), und die von der Finanzbehörde erlassenen Durchführungsbestimmungen und Erläuterungen zur Telekommunikationsrichtlinie (TK-DB) vom 2. Mai 1994 (MittVw Seite 35), zuletzt geändert am 25. März 1996 (MittVw Seite 153).
- (2) Die anwendenden Stellen können im Hinblick auf besondere Anforderungen ergänzende Dienstanweisungen für ihren Zuständigkeitsbereich erlassen. Dienstanweisungen, die aufgrund der bisherigen TK-RL erlassen wurden, gelten als aufgrund dieser Richtlinie erlassen.

Anlage L

zur Telekommunikationsrichtlinie (TK-RL) vom 9. Dezember 2009

Zugelassene Leistungsmerkmale**Teil I****Merkmale, die nur unter den Voraussetzungen des Abschnitts 3.2 genutzt werden dürfen.**

1. Aufschalten
2. Anrufumleitung
 - 2.1 Feste Anrufumleitung
 - 2.2 Variable Anrufumleitung
3. Selbsttätige Rufweitschaltung
4. Freisprechen und Mithören
5. Konferenzschaltung
6. Rufnummernanzeige
 - 6.1 Anzeige beim Wählen
 - 6.2 Anzeige beim Anrufen
7. Sprachspeicher
8. Fangen einer Rufnummer

Teil II**Sonstige Merkmale**

9. Kurzansagen im Wartezustand
10. Musik im Wartezustand
11. Elektronisches Telefonbuch (s. Teilnehmerdaten)
12. Rufnummerngeber
 - 12.1 zentrale Kurzwahlnummer
 - 12.2 Gruppenkurzwahlnummer
 - 12.3 individuelle Kurzwahlnummer
13. Notizbuchfunktion
14. Zuteilen besonderer Art
15. Anrufübernahme in Gruppen
16. Sammelnummer für Endeinrichtungen
17. Selbsttätiger Rückruf

- 17.1 Rückruf im Besetztfall
- 17.2 Rückruf im Freifall
- 18. Wahlweise Zuordnung der Nachtschaltung
 - 18.1 Allgemeine Entgegennahme
 - 18.2 Einzelnachtschaltung
 - 18.3 Sammelnachtschaltung
- 19. Anrufliste
- 20. Briefkasten (Infoservice)
- 21. Direktes Ansprechen
- 22. Richtungsausscheidung für externe Wahl
- 23. Einschränkung des selbsttätigen Internverkehrs
- 24. Sperren abgehender Verbindungen (Wahlkontrolle)
- 25. Geschlossene Benutzergruppe
- 26. Permanente Verbindungen
- 27. Semipermanente Verbindungen
- 28. Kettengespräch
- 29. Abweichende Signalisierung
- 30. Wartestellung bei Internverbindung mit selbsttätiger Ruffolge
- 31. Anschaltung von Zusatzeinrichtungen
- 32. Wahlwiederholung
 - 32.1 Wahlwiederholungstaste
 - 32.2 Rufnummernspeicher
- 33. Abwurf von durchgewählten Amtsverbindungen
- 34. Selbsttätiger Verbindungsaufbau ohne Wahl
- 35. Anklopfen
- 36. Rückfragen bzw. Umlegen
- 37. Makeln
- 38. Parken
- 39. Anrufschutz
- 40. Verhindern des Anklopfens oder Aufschaltens
- 41. Umschaltung der Berechtigung
- 42. Gebührenanzeige bei der Endeinrichtung
- 43. Uhrzeit- und Datumsanzeige
- 44. Termineinrichtung
- 45. Textübermittlung
- 46. Persönliche Identifizierung
- 47. Anrufumleitung bei persönlicher Identifikation