2003.4-J

Dienstvereinbarung über die Nutzung von Internet und E-Mail im Bayerischen Staatsministerium der Justiz sowie bei den Gerichten, Staatsanwaltschaften und Justizbehörden in dessen Geschäftsbereich

Bekanntmachung des Bayerischen Staatsministeriums der Justiz vom 21. November 2007, Az. 1500 - VI - 1178/97

(JMBl. 2008 S. 2)

Zitiervorschlag: Bekanntmachung über die Dienstvereinbarung über die Nutzung von Internet und E-Mail im Bayerischen Staatsministerium der Justiz sowie bei den Gerichten, Staatsanwaltschaften und Justizvollzugsbehörden in dessen Geschäftsbereich vom 21. November 2007 (JMBl. 2008 S. 2)

Zur Gewährleistung der schutzwürdigen Interessen und Belange der Richterinnen und Richter, Staatsanwältinnen und Staatsanwälte, Beamtinnen und Beamten sowie Arbeitnehmerinnen und Arbeitnehmer (im Folgenden Beschäftigte) schließen das Bayerische Staatsministerium der Justiz und der in seinem Zuständigkeitsbereich gebildete Hauptpersonalrat beim Bayerischen Staatsministerium der Justiz, Hauptrichterrat der ordentlichen Gerichtsbarkeit sowie Hauptstaatsanwaltsrat (im Folgenden: Hauptpersonalvertretungen) gemäß Art. 73 in Verbindung mit Art. 75a Abs. 1 des Bayerischen Personalvertretungsgesetzes (BayPVG) und Art. 17 Abs. 2 Bayerisches Richtergesetz (BayRiG) im Sinne einer vertrauensvollen Zusammenarbeit auf Basis der Richtlinie über die Nutzung von Internet und E-Mail in der bayerischen Staatsverwaltung (BayITR-05) folgende Dienstvereinbarung:

1. Allgemeines

1.1

Die Nutzung von Angeboten im World-Wide-Web (WWW-Dienst) sowie das Senden und Empfangen von E-Mails (E-Mail-Dienst) gehören mittlerweile zu den nicht mehr hinweg zu denkenden Arbeitsmitteln in der täglichen Verwaltungspraxis. Im Rahmen der dienstlichen Aufgabenerfüllung dienen sie insbesondere der Förderung effizienter interner und externer Kommunikationsbeziehungen sowie einer breiten und beschleunigten Informationsbeschaffung. Angesichts der allgemeinen Gefahren im Zusammenhang mit der Nutzung elektronischer Kommunikationsdienste sind allerdings auch Kontrollen nötig, um den Anforderungen an eine sichere Datenverarbeitung Rechnung zu tragen und einem möglichen Missbrauch nachgehen zu können, ohne dass gleichzeitig die schutzwürdigen Interessen der Nutzer verletzt werden. Um die Nutzung des WWW-Dienstes und des E-Mail-Dienstes auch für private Zwecke nicht generell und umfassend auszuschließen, ist daher dafür Sorge zu tragen, dass diese Rahmenvorgaben im Sinne eines Grundschutzes beachtet werden.

1.2

Für das Bayerische Behördennetz, zu dem das Netz der bayerischen Justiz gehört, ist ein Internetzugang eingerichtet worden. Soweit die Beschäftigten der bayerischen Justiz zur Nutzung der Dienste des Internet berechtigt sind, können sie mit externen Stellen elektronisch kommunizieren.

Da im Internet von sich aus grundsätzlich keine Maßnahmen zur Sicherstellung der Integrität und Vertraulichkeit der übertragenen Daten und der Kommunikation sowie zur Authentizität der Kommunikationspartner vorgesehen sind, müssen die Nutzer des Internet die notwendigen Vorkehrungen zur Gewährleistung der Datensicherheit und des Datenschutzes selbst treffen.

Die für die Nutzung des Internet in der bayerischen Justiz notwendigen Sicherheitsmaßnahmen wurden technisch realisiert und werden bei Änderungen der technischen Standards angepasst. Diese Maßnahmen gewährleisten das notwendige Sicherheitsniveau allerdings nur, wenn sie gemäß den nachfolgenden

Regelungen konsequent und gewissenhaft in der täglichen Arbeit durch jeden Einzelnen angewendet werden. Daher sind die Kenntnis und Einhaltung der nachfolgenden Regelungen durch jeden nutzungsberechtigten Beschäftigten eine wesentliche Voraussetzung für die Sicherheit dieses neuen Kommunikationsmittels und der IT-Infrastruktur der bayerischen Justiz.

Die Vernetzung der Arbeitsplätze bringt erhebliche Vorteile für die tägliche Arbeit. Sie birgt aber auch Risiken, die durch technische Sicherheitsvorkehrungen allein nicht beseitigt werden können, sondern die Mitwirkung der Beschäftigten erfordern.

Jede Missachtung und Nichteinhaltung dieser Regelungen gefährdet nicht nur die auf dem jeweiligen IT-System unmittelbar verarbeiteten Daten, sondern alle Daten in der Behörde, gegebenenfalls sogar auch Daten der anderen an das Justiznetz angebundenen Behörden.

2. Geltungsbereich

2.1

Die Dienstvereinbarung bezieht sich auf die Regelungen zur Nutzung von Internet (WWW-Dienst) und E-Mail (E-Mail-Dienst), die damit verbundene Protokollierung, Auswertung und Durchführung von Kontrollen und die Gewährleistung von Datenschutz und Datensicherheit im Bayerischen Staatsministerium der Justiz, bei den Gerichten, Staatsanwaltschaften und sonstigen Behörden im Geschäftsbereich des Bayerischen Staatsministeriums der Justiz sowie den Justizvollzugsbehörden.

3. Technische Ausstattung

3.1

Die für die Aufgabenerledigung erforderlichen IT-Einrichtungen (Hard- und Software), die in das Justiznetz eingebunden sind, werden für die Gerichte und Staatsanwaltschaften ausschließlich durch die Gemeinsame IT-Stelle der bayerischen Justiz - ggf. unter Beauftragung von Dienstleistern - zur Verfügung gestellt.

Auf die aktuell geltenden Regelungen zur Aufgabenabgrenzung zwischen der Gemeinsamen IT-Stelle der bayerischen Justiz und den Behörden wird Bezug genommen.

Abweichend hiervon wird die Beschaffung und Bereitstellung von IT-Einrichtungen für die Justizvollzugsbehörden gesondert geregelt.

3.2

Die Nutzung der IT-Einrichtungen ist grundsätzlich nur zu dienstlichen Zwecken zugelassen, soweit nicht im Rahmen dieser Dienstvereinbarung Ausnahmen vorgesehen sind.

3.3

Der Einsatz von privater Hardware (z.B. Soundkarte) und Software (z.B. Spiele) auf dem PC und im lokalen Netz ist unzulässig, weil dadurch Sicherheitslücken eröffnet werden können (vgl. § 10 Abs. 4 der Allgemeinen Geschäftsordnung für die Behörden des Freistaates Bayern - AGO).

3.4

Die Einrichtung und der Betrieb eines Anschlusses an ein öffentlich zugängliches Netz (mittels Datenübertragungseinrichtungen wie MODEM, ISDN-Einbaukarten usw.) sind nur auf Rechnern ohne Netzanbindung bzw. im Rahmen von Anwendungen zulässig, die vom Bayerischen Staatsministerium der Justiz freigegeben sind, weil ansonsten weitere, unkontrollierbare und ungesicherte Übergänge in das lokale Netz geschaffen werden. Dies gilt auch, wenn der betreffende Rechner sich nur temporär im Justiznetz befindet.

3.5

Es darf lediglich durch das Bayerische Staatsministerium der Justiz freigegebene bzw. genehmigte Software eingesetzt werden. Die Regelungen zum Kontrollierten Installieren gelten daneben.

Der Einsatz von Software in den Justizvollzugsbehörden ist in der Dienstanweisung vom 30. Oktober 2002, Az. 1518 - VIIa - 939/92, gesondert geregelt.

4. Sicherung des Systemzugangs

4.1

Die Büroräume sind bei Abwesenheit zu verschließen.

Bei Verlassen des Arbeitsplatzes soll der Zugang zum PC durch Kennwort gesichert (Sperren über „Strg-Alt-Entf“) bzw. soll der Kennwortschutz des Bildschirmschoners aktiviert werden.

4.2

Die Anmeldung am PC ist durch ein Kennwort zu sichern.

Das Kennwort sollte aus mindestens 6 - 8 Zeichen in einer Kombination aus Buchstaben und Ziffern bzw. Sonderzeichen bestehen, dabei sind auch Groß- und Kleinbuchstaben zulässig. Trivialwörter und Begriffe aus dem persönlichen Umfeld des Beschäftigten (z.B. Vornamen von Familienmitgliedern, Autokennzeichen u. ä.) sind zu vermeiden.

Das Kennwort ist mehrmals im Jahr (mindestens vierteljährlich) und bei Verdacht des Missbrauchs sofort zu ändern.

4.3

Es sind keine schriftlichen Aufzeichnungen der Kennwörter zulässig. Kennwörter dürfen nur in Ausnahmefällen an Zugangsberechtigte weitergegeben werden und sind anschließend unverzüglich zu ändern.

5. Nutzungsbedingungen für Internet und E-Mail

Im Bayerischen Staatsministerium der Justiz sowie bei den Gerichten, Staatsanwaltschaften und Justizvollzugsbehörden im Geschäftsbereich des Bayerischen Staatsministeriums der Justiz wird die Nutzung der WWW-Dienste und des E-Mail-Dienstes nach Maßgabe der nachfolgenden Bedingungen auch für private Zwecke (Privatnutzung) zugelassen.

5.1

Die Privatnutzung wird nur gestattet, solange und soweit die uneingeschränkte Verfügbarkeit der betroffenen IT-Systeme für dienstliche Zwecke vorrangig gewährleistet bleibt und keine haushaltsrechtlichen oder sonstigen übergeordneten Belange entgegenstehen. Ein Rechtsanspruch auf Privatnutzung von Internet und E-Mail besteht nicht. Die Privatnutzung von Internet und E-Mail kann in begründeten Fällen zeitweise oder ganz untersagt werden.

Es dürfen lediglich die Dienste des Internet genutzt werden, die bei der Installation zur Verfügung gestellt werden. Die Beschäftigten, die den Internetzugang sowie E-Mail privat nutzen wollen, müssen eine eigenhändig unterzeichnete Einwilligungserklärung gemäß dem Muster in der Anlage abgeben. Soweit ein Beschäftigter die Einwilligungserklärung nicht unterzeichnet, ist für diesen die private Nutzung der Internet- und E-Mail-Dienste nicht zulässig. Dies ist ebenfalls mit der Anlage zu bestätigen. Diese Erklärungen sind zum Personalakt zu nehmen.

5.2

Die Privatnutzung ist auf einen geringfügigen Umfang zu beschränken. Hiervon umfasst ist auch die Speicherung privater Daten und Downloads, sofern nicht die Sicherheit der IT-Systeme gefährdet ist.

5.3

Die Privatnutzung darf nicht zur Verfolgung gewerblicher oder geschäftsmäßiger Interessen erfolgen; die Privatnutzung für Rechtsgeschäfte des täglichen Lebens ist zugelassen.

5.4

Die Privatnutzung darf nicht zu Zwecken erfolgen, die die Interessen oder das Ansehen der Justiz oder des Freistaats Bayern in der Öffentlichkeit im Allgemeinen oder die Unabhängigkeit und Neutralität der Justiz gefährden sowie die Sicherheit des Behördennetzes beeinträchtigen können.

5.5 Regelungen für die Internetnutzung (WWW-Dienst)

5.5.1

Generell unzulässig sind,

– der Abruf kostenpflichtiger Internetseiten,

– das Abrufen, Verbreiten oder Speichern von Inhalten, die gegen persönlichkeitsrechtliche, datenschutzrechtliche, lizenz- und urheberrechtliche oder strafrechtliche Bestimmungen verstoßen,

– das Abrufen, Verbreiten oder Speichern von beleidigenden, verleumderischen, verfassungsfeindlichen, rassistischen, sexistischen, gewaltverherrlichenden oder pornografischen Äußerungen oder Abbildungen,

– Aktivitäten, die sich gegen die Sicherheit von IT-Systemen richten (z.B. Angriffe auf externe Webserver).

Daneben ist die Teilnahme an Netz- bzw. Onlinespielen, Auktionen und ähnlichen Vorgängen zu privaten Zwecken untersagt.

5.5.2

Generell unzulässig ist die Verwendung des intern genutzten Anmeldenamens (Benutzerkennung) und Anmeldepasswortes im Internet und der dienstlichen E-Mail-Adresse in öffentlichen „Chat-Räumen“ und ähnlichen öffentlichen Meinungsforen.

5.5.3

Untersagt ist ferner,

– fremde Zugriffsberechtigungen (wie z.B. Benutzerkennungen, Passwörter) und gegebenenfalls eingesetzte sonstige fremde Authentifizierungshilfsmittel (wie z.B. Chipkarten) auszuforschen, zu testen und zu nutzen,

– eigene Benutzerkennungen und auch sonstige Authentifizierungshilfsmittel für eine Benutzung durch Unberechtigte zur Verfügung zu stellen. Es wird ausdrücklich darauf hingewiesen, dass in einem derartigen Fall in den Protokolldaten (vgl. Ziffer 10) die Aktivitäten des unberechtigten Dritten - auch unzulässige - dem Anschlussinhaber zugeschrieben werden.

5.6 Regelungen für die E-Mail-Nutzung (E-Mail-Dienst)

5.6.1

Die Beschäftigten der bayerischen Justiz erhalten eine persönliche E-Mail-Adresse, die wie folgt aufgebaut ist:

vorname.nachname@behördenkürzel.bayern.de

(z.B. max.mustermann@stmj.bayern.de).

Einigen Stellen wird gegebenenfalls zusätzlich eine Funktionsadresse zugeteilt (z.B. Poststelle, Organisation, IuK, Presse u. a.).

Die E-Mail-Adressen werden im Adressbuch unter „Globales Adressbuch“ bereitgestellt.

5.6.2

Die Funktionsadresse „Poststelle“ ist die zentrale E-Mail-Adresse einer Behörde. Nachrichten, die an die zentrale Poststelle gerichtet sind, werden soweit möglich an den zuständigen Beschäftigten weitergeleitet. Anderenfalls wird die E-Mail ausgedruckt und in den normalen Geschäftsgang gegeben.

In den Justizvollzugsbehörden ist durch geeignete Maßnahmen sicherzustellen, dass der Eingang von E-Mails unter dieser Funktionsadresse regelmäßig überprüft wird (mindestens dreimal täglich - Früh-, Spät- und Nachtschicht, auch an Sonn- und Feiertagen, soweit zutreffend).

5.6.3

Die Manipulation von E-Mails (z.B. Verfälschung des Absenders oder des Inhalts) ist untersagt.

5.6.4

Die Nutzung jeglicher dienstlicher E-Mail-Adressen für parteipolitische Zwecke ist untersagt.

5.6.5

Bei eingehenden privaten E-Mails muss damit gerechnet werden, dass diese von anderen Beschäftigten im Rahmen der Erledigung dienstlicher Aufgaben (z.B. Vertretung, Systemadministration) zur Kenntnis genommen werden. Das Bayerische Staatsministerium der Justiz übernimmt gegenüber Dritten bezüglich der Inhalte und der Vertraulichkeit privater elektronischer Post (E-Mail) keine Gewähr. Die Privatnutzung von E-Mail-Diensten über private Webmail-Angebote ist im Rahmen der erlaubten Privatnutzung der Web-Dienste möglich.

5.6.6

E-Mails und sonstige Nachrichten mit den in Nr. 5.5.1 genannten Inhalten dürfen weder verfasst, gespeichert, ausgedruckt noch versendet oder der Öffentlichkeit in anderer Weise zugänglich gemacht werden.

5.6.7

Folgende Regelungen zur Behandlung von eingehenden dienstlichen E-Mail-Nachrichten sind zu beachten:

– Das E-Mail-Programm sollte ständig geöffnet sein, damit der Eingang neuer Nachrichten erkannt werden kann. Hierdurch wird auch sichergestellt, dass alle Beschäftigten zeitgerecht erreicht werden können.

– Bei vorhersehbarer Abwesenheit (z.B. Urlaub, Dienstreise u. a.) ist eine Vertretung sicherzustellen oder zumindest der elektronische Abwesenheitsassistent zu aktivieren.

Im Geschäftsbereich der Justizvollzugsbehörden sind entsprechende Abwesenheiten von Beschäftigten mit persönlicher E-Mail-Adresse an die örtliche IT-Leitung zu melden. Diese stellt sicher, dass sowohl der ursprüngliche Empfänger als auch sein Vertreter die E-Mail erhalten.

– Im Falle der nicht vorhersehbaren Abwesenheit (z.B. plötzliche Erkrankung) ist soweit möglich in Abstimmung mit dem Beschäftigten eine geeignete Regelung zu treffen.

– Eine automatische Weiterleitung des gesamten Posteinlaufs an E-Mail-Adressen, die außerhalb der jeweiligen Justizbehörde liegen (z.B. an einen privaten E-Mail-Anschluss über das Internet), ist aus Sicherheitsgründen untersagt. Ebenso ist die automatisierte Weiterleitung vom privaten E-Mail-Anschluss an das dienstliche Postfach unzulässig.

– Bei dezentral, nicht im Postfach der Poststelle eingehender E-Mail muss jeder Beschäftigte die weitere geschäftsmäßige Behandlung (ordnungsgemäße Bearbeitung der Eingänge, Registrierung vorgangsrelevanter Dokumente, Weitergabe in den Geschäftsgang) eigenverantwortlich entscheiden (siehe hierzu auch § 12 Abs. 6 AGO).

6. Virenschutz

6.1

Jede elektronische Kommunikation bringt das Risiko einer Infizierung durch Computerviren mit sich. Um dieses Risiko zu verringern, ist jeder Arbeitsplatzrechner mit einer Virenerkennungssoftware ausgestattet. Diese bietet jedoch keinen absolut verlässlichen Schutz, da grundsätzlich nur bekannte Viren und Viren, die ein bestimmtes Muster enthalten, erkannt werden. Bei der Nutzung des Internet und des E-Mail-Systems sind die Beschäftigten daher zu besonderer Sorgfalt verpflichtet.

6.2

E-Mails sollten möglichst nicht direkt geöffnet, sondern zuerst in der Vorschau betrachtet werden, um besser beurteilen zu können, ob es sich um eine verdächtige E-Mail handelt.

6.3

Bei folgenden Anzeichen sollte vor der Öffnung einer Anlage Kontakt mit dem Absender aufgenommen werden:

– Die E-Mail hat eine verdächtig wirkende Betreffzeile oder

– die Anlage hat ein unbekanntes oder potenziell gefährliches Dateiformat (bekannt sind z.B. .doc, .pdf, .xls, .ppt, .mdb, .tif, .zip, ...; potenziell gefährlich sind z.B. .exe, .vbs, .dot, .xlt).

6.4

Falls beim Öffnen eines mittels E-Mail erhaltenen Dokuments das Virenerkennungsprogramm einen Virus meldet, ist unverzüglich - ohne weitere Aktivitäten am System vorzunehmen - die IT-Beratungsstelle (IBS) bzw. in den Justizvollzugsbehörden die örtliche IT-Leitung und die IT-Leitstelle bei der Bayerischen Justizvollzugsschule Straubing zu informieren.

6.5

Aufforderungen zur Weiterleitung von Warnungen, Mails und Anhängen an Freunde, Bekannte oder Kollegen (insbesondere „Kettenbriefe“) ist nicht zu folgen, sondern sie sind im Bereich der Gerichte und Staatsanwaltschaften nur an die IT-Beratungsstelle (IBS) (E-Mail: pcprobleme@justiz-ibs.bayern.de) zu senden. Es handelt sich hierbei meist um irritierende und belästigende Mails mit Falschmeldungen (sog. Hoax).

In den Justizvollzugsbehörden sind die örtliche IT-Leitung und die IT-Leitstelle bei der Bayerischen Justizvollzugsschule Straubing vorab zu unterrichten.

6.6

Die Beschaffung von Programmen oder von ausführbaren Programmroutinen (auch Updates) aus dem oder über das Internet bzw. deren Installation über USB-Stick, CD-ROM oder DVD ist aus Sicherheitsgründen nicht zulässig.

7. Verschlüsselung der Datenübertragung (kryptographische Schutzmaßnahmen)

7.1

Die Übertragung von sensiblen, schutzwürdigen und insbesondere von personenbezogenen Daten über das Internet ist zur Wahrung der Vertraulichkeit zu verschlüsseln. Dabei obliegt es dem die Übertragung veranlassenden Beschäftigten zu beurteilen, ob eine Verschlüsselung notwendig ist.

7.2

Die Anwendung zusätzlicher Sicherheitsmaßnahmen (z.B. digitale Signatur) wird gesondert vom Bayerischen Staatsministerium der Justiz geregelt.

8. Sicherheitsrelevante Ereignisse

8.1

Alle sicherheitsrelevanten Ereignisse (wie z.B. unerklärliches Systemverhalten, Verlust oder Veränderung von Daten und Programmen, Verfügbarkeit nicht explizit freigegebener Dienste, Verdacht auf Missbrauch der eigenen Benutzerkennung usw.) sind im Bereich der Gerichte und Staatsanwaltschaften unverzüglich - ohne eigene Aufklärungsversuche - an die IT-Beratungsstelle (IBS) (E-Mail: pcprobleme@justiz-ibs.bayern.de) zu melden.

Für den Bereich der Justizvollzugsbehörden sind die Meldungen nach Rücksprache mit der örtlichen IT-Leitung direkt an die IT-Leitstelle bei der Bayerischen Justizvollzugsschule Straubing zu melden.

8.2

Der IT-Sicherheitsbeauftragte bzw. die IBS informieren die Beschäftigten über sicherheitsrelevante Ereignisse.

9. Information und Schulung der Beschäftigten

Die Beschäftigten werden, neben den unter Ziffer 8.2 genannten Ereignissen, über die besonderen Datensicherheitsprobleme bei der Nutzung der elektronischen Kommunikationssysteme unterrichtet. Sie werden für den sicheren und wirtschaftlichen Umgang mit diesen Systemen qualifiziert.

10. Protokollierung

10.1

Der gesamte Datenverkehr des WWW-Dienstes wird auf Basis der aufgerufenen Internetseiten (sog. URL) bei der Firewall des Rechenzentrums Nord am Übergang des Justiznetzes zum allgemeinen Bayerischen Behördennetz automatisch protokolliert.

Bei der Nutzung des E-Mail-Dienstes wird der Laufweg der E-Mail (Absender, Adressat und Zeitpunkt der Versendung/des Empfangs) automatisch protokolliert. Inhalte und Anhänge von E-Mails werden nicht protokolliert.

Die Protokolle werden bis zum Ende des Halbjahres aufbewahrt, das dem Halbjahr der Protokollierung folgt, somit längstens ein Jahr. Die Löschung der Protokolldaten wird protokolliert.

10.2

Zur Aufklärung technischer Probleme können im Netzwerk Verkehrsdaten erfasst werden. Eine Auswertung der übertragenen Inhalte darf nicht erfolgen. Verkehrsdaten, die zur Fehleranalyse aufgezeichnet werden, werden gelöscht, sobald sie für die Auswertung nicht mehr benötigt werden.

10.3

Die Protokolldaten dienen ausschließlich zur Datenschutzkontrolle, zur Verfolgung von Missbrauch, zur Datensicherung, Optimierung des Netzes und zur Sicherstellung eines ordnungsgemäßen Betriebes des Justiznetzes bzw. der Systeme.

10.4

Auf die Protokolldateien haben die bei der Justiznetz-Firewall eingesetzten Beschäftigten des Rechenzentrums Nord Zugriff.

10.5

Die Verwalter des Internet- und E-Mail-Systems müssen mit den Bestimmungen des Fernmeldegeheimnisses im Telekommunikationsgesetz und den datenschutzrechtlichen Vorschriften vertraut und auf Einhaltung des Datenschutzes verpflichtet sein. Darüber hinaus werden sie hinsichtlich der Einhaltung des Fernmeldegeheimnisses und des Datenschutzes auf etwaige strafrechtliche Konsequenzen bei Verstößen hingewiesen.

11. Kontrollen und Rechte der Beschäftigten

11.1

Zur Überwachung der Einhaltung der Nutzungsregelungen und zur Abwendung einer Gefahr für das Justiznetz sowie zur Sicherstellung der Verfügbarkeit des Internet können unter Beachtung der Verhältnismäßigkeit sowie der datenschutzrechtlichen Vorschriften Kontrollen, insbesondere Stichproben- und Verdachtskontrollen durchgeführt werden.

11.1.1

Die Kontrollen werden auf Anordnung des für die Sicherheit des Justiznetzes zuständigen Beschäftigten (sog. Ressort-CERT) durch die bei der Justiznetz-Firewall eingesetzten Beschäftigten nicht personenbezogen durchgeführt.

11.1.2

Falls sich aufgrund der in Ziffer 11.1.1 genannten Kontrollen oder durch konkrete Tatsachen in anderer Weise ein begründeter Verdacht auf einen dienst-, arbeits- oder datenschutzrechtlichen Verstoß ergibt, können unter Beachtung der Verhältnismäßigkeit sowie der datenschutzrechtlichen Vorschriften personenbezogene Missbrauchskontrollen durchgeführt werden.

11.1.3

Durch Maßnahmen nach Ziffer 11.1.2 gewonnene Daten werden auf Anordnung des für die Sicherheit des Justiznetzes zuständigen Beschäftigten (sog. Ressort-CERT) durch die bei der Justiznetz-Firewall eingesetzten Beschäftigten ausgewertet und der zuständigen Stelle übergeben. Der von der Kontrolle betroffene Beschäftigte ist von der zuständigen Stelle über Umfang, Zweck und Ergebnis einer solchen Missbrauchskontrolle zu unterrichten und ihm ist vor der Einleitung weiterer Maßnahmen Gelegenheit zur Stellungnahme zu geben, soweit nicht Gründe der Unaufschiebbarkeit oder der Geheimhaltung einer Maßnahme entgegenstehen. Die zuständige Personalvertretung ist unverzüglich zu unterrichten, sofern dies durch den Beschäftigten beantragt wird. Der Beschäftigte ist hierüber zu belehren. Unterlagen sind nach Gebrauch unverzüglich zu vernichten, soweit Rechtsvorschriften nicht entgegenstehen.

11.1.4

Sollen Kontrollen nach Ziffer 11.1.2 auf Grund von Ersuchen der Behördenleitung durchgeführt werden, gilt Ziffer 11.1.3 entsprechend.

11.2

Unberührt bleiben Kontrollen und Auswertungen bei Maßnahmen zum Vollzug von Rechtsvorschriften (z.B. Auswertungen im Rahmen strafrechtlicher Ermittlungsverfahren).

11.3

Im Übrigen wird der gesamte Datenverkehr mit dem Internet (WWW-Dienst und E-Mail) nicht zur Leistungs- und Verhaltenskontrolle verwendet.

11.4

Werden Vorkommnisse bekannt, die geeignet sind, die Interessen oder das Ansehen des Freistaats Bayern zu beeinträchtigen, so hat die verantwortliche Stelle umgehend geeignete Maßnahmen zur Aufklärung der Vorkommnisse zu ergreifen und erforderlichenfalls unverzüglich für Abhilfe zu sorgen.

12. Personalvertretungen

12.1

Die Hauptpersonalvertretungen haben, soweit es zur Durchführung ihrer Aufgaben erforderlich ist, jederzeit das Recht auf Auskunft und Information in sämtliche das Internet (WWW-Dienst) und E-Mail (E-Mail-Dienst) betreffenden Fragen. Dies gilt auch für die damit verbundenen Fragen, die sich aus der Protokollierung, Auswertung und Durchführung von Kontrollen sowie der Gewährleistung von Datenschutz und

Datensicherheit ergeben. Hiervon unberührt bleiben entsprechende Rechte der Personalvertretungen bei den Anwendungsbehörden in deren Zuständigkeitsbereich.

12.2

Im Übrigen werden den Hauptpersonalvertretungen Auswertungen zur Verfügung gestellt, soweit dies für die Durchführung ihrer Aufgaben erforderlich ist.

13. Sanktionen

Verstöße gegen diese Dienstvereinbarung können dienst- und arbeitsrechtliche sowie auch strafrechtliche Konsequenzen haben.

14. Übertragung von Aufgaben des IT-Betriebs an Dienstleister

Soweit das Bayerische Staatsministerium der Justiz Aufgaben des IT-Betriebs an Dienstleister (z.B. private Unternehmen, staatliche Rechenzentren) überträgt, stehen diesen die Befugnisse nach Maßgabe der hierüber geschlossenen Dienstleistungsvereinbarungen zu.

15. Gleichstellungsklausel

Alle Personen-, Status- und Funktionsbezeichnungen in dieser Dienstvereinbarung gelten jeweils in männlicher und weiblicher Form.

16. Inkrafttreten, Laufzeit, Außerkrafttreten

16.1

Die Dienstvereinbarung tritt am 1. Dezember 2007 in Kraft. Sie kann mit einer Frist von sechs Monaten zum Ende eines Kalendermonats schriftlich gekündigt werden. In diesem Fall werden unverzüglich Verhandlungen zum Abschluss einer neuen Dienstvereinbarung aufgenommen.

16.2

Nach Außerkrafttreten der Dienstvereinbarung wegen Kündigung gelten ihre Regelungen bis zum Abschluss einer neuen Dienstvereinbarung weiter.

München, den 21. November 2007

Bayerisches Staatsministerium der Justiz	Hauptpersonalrat beim Bayerischen Staatsministerium der Justiz
Klotz Ministerialdirektor	Schmid Vorsitzender
	Hauptrichterrat der ordentlichen Gerichtsbarkeit
	Herrler Vorsitzender
	Hauptstaatsanwaltsrat

Stern

Vorsitzender

Anlagen

Anlage: Einwilligungserklärung