Name: _____

Organisationseinheit:_____

Kenntnisnahme- und Einwilligungserklärung

Die **Richtlinie über die dienstliche und private Nutzung der Telekommunikationsanlagen der Hessischen Landesverwaltung** habe ich zur Kenntnis genommen und werde die dort gemachten Vorgaben beachten.

_____

Ort, Datum Unterschrift

Ich möchte die von meiner Dienststelle zur Verfügung gestellten Telefonanlagen, sofern durch die Richtlinie zugelassen, in geringfügigem Umfang auch für private Zwecke nutzen.

Ich willige ein, dass zum Zwecke der Kontrolle der Einhaltung der Vorgaben dieser Richtlinie die während der Telekommunikation entstehenden Verbindungsdaten protokolliert werden. Ich bin damit einverstanden, dass diese Verbindungsdaten wie in der Richtlinie unter Punkt 5 beschrieben temporär gespeichert werden können.

Maßnahmen zur Gewährleistung der Cyber- und IT-Sicherheit

Die durchgeführten Maßnahmen zur Gewährleistung von Cyber- und IT-Sicherheit orientieren sich an den jeweils geltenden Standards des Bundesamtes für Sicherheit in der Informationstechnik und verbindlichen Beschlüssen des IT-Planungsrates. Die Umsetzung erfolgt durch das Zentrum für Informationssicherheit (Hessen 3C), ggf. in Zusammenarbeit mit weiteren für die Informationssicherheit zuständigen Organisationseinheiten sowie durch den Zentralen IT-Dienstleister des Landes Hessen. Im Rahmen der erforderlichen Maßnahmen zur Gewährleistung der Cyber- und ITSicherheit erfolgt eine Verarbeitung meiner personenbezogenen Daten im Rahmen der §§ 7–11 sowie 13 und 16 des Hessischen Gesetzes zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz – HITSiG).

Danach erfolgt eine Verarbeitung von personenbezogenen Daten im Rahmen der privaten Telefonnutzung in Form einer automatisierten Erhebung und Auswertung von Log- und Protokolldaten. Die Auswertung erfolgt zum Zwecke der Sammlung, Auswertung oder Untersuchung von Informationen über Risiken oder Vorkehrungen für die Informationssicherheit, zur Unterstützung, Beratung oder Warnung in Fragen der Informationssicherheit und zur Aufdeckung von Sicherheitslücken, Schadprogrammen oder erfolgten oder versuchten Angriffen auf die

Informationstechnik. Die Erhebung und Auswertung betrifft den Datenverkehr innerhalb des Landesnetzes und an den Übergabe- und Knotenpunkten des Landesdatennetzes. Grundsätzlich erfolgt keine Speicherung der erhobenen Daten. Sofern aufgrund von zureichenden tatsächlichen Anhaltspunkten weitere Auswertungen erforderlich werden, ist im Einzelfall eine Speicherung von bis zu 90 Tagen zulässig.

Die Auswertung der erhobenen Daten erfolgt grundsätzlich automatisiert und ohne Personenbezug, nach vorheriger Anonymisierung (sofern im Einzelfall möglich) bzw. Pseudonymisierung. Sie bedarf einer Anordnung durch die Leitung des Zentrums für Informationssicherheit nach juristischer Prüfung durch eine Beschäftigte oder einen Beschäftigten des Innenressorts mit Befähigung zum Richteramt. In diesem Zusammenhang ist das Aufbrechen von ggf. vorhandener Verschlüsselungen (SSL-Tunneln) erforderlich. Eine direkt personenbezogene oder nicht automatisierte Auswertung erfolgt sofern hinreichende tatsächliche Anhaltspunkte den Verdacht begründen, dass die Ursache in einem Schadprogramm liegt oder sich aus den Daten Hinweise auf ein Schadprogramm ergeben und die Datenverarbeitung zur Abwehr des Schadprogramms, zur Abwehr von Gefahren, die von dem Schadprogramm ausgehen oder zur Erkennung und Abwehr anderer Schadprogramme erforderlich ist.

Mit den oben genannten Maßnahmen sind Einschränkungen meines Rechts auf Fernmeldegeheimnis (Art. 10 GG und Art. 12 der Verfassung des Landes Hessen) sowie meines Rechts auf informationelle Selbstbestimmung verbunden. Damit bin ich einverstanden.

Mir ist bekannt, dass im Falle eines konkreten Verdachts einer missbräuchlichen Nutzung alle vorhandenen Protokolldateien, die aus der privaten Nutzung der Telekommunikations- bzw. Telefonanlagen resultieren, zur personenbezogenen Auswertung verwendet werden können. Zu diesem Zwecke kann die Anonymisierung bzw. Pseudonymisierung der Protokolldateien aufgehoben werden.

Mir ist bekannt, dass die Gestattung der Privatnutzung jederzeit eingeschränkt oder widerrufen werden kann. Auch ich kann diese Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen. Ab dem Zeitpunkt des Widerrufs darf ich die Telekommunikationsanlage dann nicht mehr für private Zwecke nutzen.

Diese Erklärung ersetzt alle bisherigen Einwilligungserklärungen, die zur Nutzung von Telekommunikations-/Telefonanlagen abgegeben worden sind.

Die Einwilligungserklärung wird in meine Personalakte aufgenommen.

_____

Ort, Datum Unterschrift

Name: _____

Organisationseinheit:_____

Kenntnisnahme- und Einwilligungserklärung

Die Richtlinie zur Nutzung von E-Mail und Internet in der Hessischen Landesverwaltung habe ich zur Kenntnis genommen und werde die dort gemachten Vorgaben beachten.

_____

Ort, Datum Unterschrift

Ich möchte die von meiner Dienststelle zur Verfügung gestellten Internet- und E-Mail-Dienste, sofern durch die Richtlinie zugelassen, in geringfügigem Umfang auch für private Zwecke nutzen.

Ich willige ein, dass mein privater E-Mail- und Internetverkehr in demselben Maße wie mein dienstlicher E-Mail- und Internetverkehr automatisch protokolliert wird. Ich bin damit einverstanden, dass diese Protokolldaten wie in der Richtlinie unter Punkt 4 beschrieben temporär gespeichert werden und stichprobenartig überprüft werden können. Bei einem konkreten Verdacht einer missbräuchlichen Nutzung können alle vorhandenen Protokolle zur personenbezogenen Auswertung verwendet werden und die Anonymität kann auch im Falle der Internetnutzung aufgehoben werden.

Ich gestatte ferner, dass meine privaten E-Mails bei möglicher Verseuchung mit Viren oder anderen Schadprogrammen sowie an mich adressierte unerwünschte oder unverlangt zugehende E-Mails – sog. Spam-Mails – automatisiert herausgefiltert und ggf. nicht zugestellt werden. Mir ist bekannt, dass dabei auch privat erwünschte E-Mails irrtümlich durch den Spamfilter ausgesondert werden können.

Sollten im Fall meiner Abwesenheit vom Arbeitsplatz an mich adressierte E-Mails an meine Vertretung weitergeleitet werden oder sie Zugriff auf mein Postfach nehmen, so billige ich das. Meine Vorgesetzte oder mein Vorgesetzter organisiert insbesondere für den Fall der ungeplanten Abwesenheit einen Zugriff auf mein E-Mail-Konto, wenn dies für einen ordnungsgemäßen betrieblichen Ablauf nötig sein sollte. Mir ist bewusst, dass dabei auch private E-Mails anderen Personen zur Kenntnis gelangen können.

Maßnahmen zur Gewährleistung der Cyber- und IT-Sicherheit

Die durchgeführten Maßnahmen zur Gewährleistung von Cyber und IT-Sicherheit orientieren sich an den jeweils geltenden Standards des Bundesamtes für Sicherheit in der Informationstechnik und verbindlichen Beschlüssen des IT-Planungsrates. Die Umsetzung erfolgt durch das Zentrum für Informationssicherheit (Hessen 3C), ggf. in Zusammenarbeit mit weiteren für die Informationssicherheit zuständigen Organisationseinheiten sowie durch den Zentralen IT-Dienstleister des Landes

Hessen. Im Rahmen der erforderlichen Maßnahmen zur Gewährleistung der Cyber- und IT-Sicherheit erfolgt eine Verarbeitung meiner personenbezogenen Daten im Rahmen der §§ 7–11 sowie 13 und 16 des Hessischen Gesetzes zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz – HITSiG).

Danach erfolgt eine Verarbeitung von personenbezogenen Daten im Rahmen der privaten Internetnutzung in Form einer automatisierten Erhebung und Auswertung von Log- und Protokolldaten. Die Auswertung erfolgt zum Zwecke der Sammlung, Auswertung oder Untersuchung von Informationen über Risiken oder Vorkehrungen für die Informationssicherheit, zur Unterstützung, Beratung oder Warnung in Fragen der Informationssicherheit und zur Aufdeckung von Sicherheitslücken, Schadprogrammen oder erfolgten oder versuchten Angriffen auf die Informationstechnik. Die Erhebung und Auswertung betrifft den Datenverkehr innerhalb des Landesnetzes und an den Übergabe- und Knotenpunkten des Landesdatennetzes. Grundsätzlich erfolgt keine Speicherung der erhobenen Daten. Sofern aufgrund von zureichenden tatsächlichen Anhaltspunkten weitere Auswertungen erforderlich werden, ist im Einzelfall eine Speicherung von bis zu 90 Tagen zulässig.

Die Auswertung der erhobenen Daten erfolgt grundsätzlich automatisiert und ohne Personenbezug, nach vorheriger Anonymisierung (sofern im Einzelfall möglich) bzw. Pseudonymisierung. Sie bedarf einer Anordnung durch die Leitung des Zentrums für Informationssicherheit nach juristischer Prüfung durch eine Beschäftigte oder einen Beschäftigten des Innenressorts mit Befähigung zum Richteramt. In diesem Zusammenhang ist das Aufbrechen von ggf. vorhandener Verschlüsselungen (SSL-Tunneln) erforderlich. Eine direkt personenbezogene oder nicht automatisierte Auswertung erfolgt sofern hinreichende tatsächliche Anhaltspunkte den Verdacht begründen, dass die Ursache in einem Schadprogramm liegt oder sich aus den Daten Hinweise auf ein Schadprogramm ergeben und die Datenverarbeitung zur Abwehr des Schadprogramms, zur Abwehr von Gefahren, die von dem Schadprogramm ausgehen oder zur Erkennung und Abwehr anderer Schadprogramme erforderlich ist.

Mit den oben genannten Maßnahmen sind Einschränkungen meines Rechts auf Fernmeldegeheimnis (Art. 10 GG und Art. 12 der Verfassung des Landes Hessen) sowie meines Rechts auf informationelle Selbstbestimmung verbunden. Damit bin ich einverstanden.

Mir ist bekannt, dass im Falle eines konkreten Verdachts einer missbräuchlichen Nutzung alle vorhandenen Protokolldateien, die aus der privaten Nutzung von E-Mail und Internet resultieren, zur personenbezogenen Auswertung verwendet werden können. Zu diesem Zwecke kann die Anonymisierung bzw. Pseudonymisierung der Protokolldateien aufgehoben werden.

Mir ist bekannt, dass die Gestattung der Privatnutzung jederzeit eingeschränkt oder widerrufen werden kann. Auch ich kann diese Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen. Ab dem Zeitpunkt des Widerrufs darf ich den Internetzugang und den E-Mail-Dienst dann nicht mehr für private Zwecke nutzen.

Diese Erklärung ersetzt alle bisherigen Einwilligungserklärungen, die zur Nutzung von E-Mail- und/oder Internetdiensten abgegeben worden sind.

Die Einwilligungserklärung wird in meine Personalakte aufgenommen.

Ort, Datum Unterschrift

HESSISCHE STAATSKANZLEI

869

Erteilung eines Exequaturs;

Herr Mubarak Bawa Syed, Generalkonsul der Republik Indien in Frankfurt am Main

Die Bundesregierung hat dem zum Leiter der berufskonsularischen Vertretung der Republik Indien in Frankfurt am Main ernannten Herrn Mubarak Bawa Syed am 27. Oktober 2023 das Exequatur als Generalkonsul erteilt.

Der Konsularbezirk umfasst die Länder Hessen, Nordrhein-Westfalen, Rheinland-Pfalz und Saarland.

Das dem bisherigen Generalkonsul, Herrn Amit Telang, am 12. August 2020 erteilte Exequatur ist erloschen.

Wiesbaden, den 6. November 2023

Hessische Staatskanzlei

StAnz. 47/2023 S. 1458

HESSISCHES MINISTERIUM DES INNERN UND FÜR SPORT

870

Richtlinie zur Nutzung von E-Mail- und Internetdiensten in der Hessischen Landesverwaltung;

Ergänzung der Anlage 1 und 2 „Kenntnisnahme- und Einwilligungserklärung“ sowie Verlängerung der Geltungsdauer

Bezug: E-Mail- und Internetrichtlinie vom 30. Januar 2012 (StAnz. S. 526), zuletzt geändert durch Erlass vom 5. Dezember 2022 (StAnz. S. 1416)

Die vorgenannte Richtlinie wird wie folgt geändert:

1. Die Anlagen 1 und 2 „Kenntnisnahme- und Einwilligungserklärung“ wurden jeweils hinsichtlich der Maßnahmen zur Gewährleistung der Cyber- und IT-Sicherheit ergänzt und werden nachstehend bekannt gemacht.
2. Die Geltungsdauer wird bis zum 31. Dezember 2025 verlängert.
3. Dieser Erlass tritt am Tage nach der Bekanntmachung in Kraft.

Wiesbaden, den 31. Oktober 2023

Hessisches Ministerium
des Innern und für Sport
Z 1 – 03d08-01-17/010
– Gült.-Verz. 30 –

StAnz. 47/2023 S. 1458

Anlage 1

Name:

Referat:

Kenntnisnahme- und Einwilligungserklärung

Die Richtlinie zur Nutzung von E-Mail und Internet in der Hessischen Landesverwaltung habe ich zur Kenntnis genommen und werde die dort gemachten Vorgaben beachten.

Ort, Datum Unterschrift

Ich möchte die von meiner Dienststelle zur Verfügung gestellten Internet- und E-Mail-Dienste, sofern durch die Richtlinie zugelassen, in geringfügigem Umfang auch für private Zwecke nutzen.

Ich willige ein, dass mein privater E-Mail- und Internetverkehr in demselben Maße wie mein dienstlicher E-Mail- und Internetverkehr automatisch protokolliert wird. Ich bin damit einverstanden, dass diese Protokolldaten wie in der Richtlinie unter Punkt 4 beschrieben temporär gespeichert werden und stichprobenartig überprüft werden können. Bei einem konkreten Verdacht einer missbräuchlichen Nutzung können alle vorhandenen Protokolle zur personenbezogenen Auswertung verwendet werden und die Anonymität kann auch im Falle der Internetnutzung aufgehoben werden.

Ich gestatte ferner, dass meine privaten E-Mails bei möglicher Verseuchung mit Viren oder anderen Schadprogrammen sowie an mich adressierte unerwünschte oder unverlangt zugehende E-Mails – sog. Spam-Mails – automatisiert herausgefiltert und ggf. nicht zugestellt werden. Mir ist bekannt, dass dabei auch privat erwünschte E-Mails irrtümlich durch den Spamfilter ausgesondert werden können.

Sollten im Fall meiner Abwesenheit vom Arbeitsplatz an mich adressierte E-Mails an meine Vertretung weitergeleitet werden oder sie Zugriff auf mein Postfach nehmen, so billige ich das. Meine Vorgesetzte oder mein Vorgesetzter organisiert insbesondere für den Fall der ungeplanten Abwesenheit einen Zugriff auf mein E-Mail-Konto, wenn dies für einen ordnungsgemäßen betrieblichen Ablauf nötig sein sollte. Mir ist bewusst, dass dabei auch private E-Mails anderen Personen zur Kenntnis gelangen können.

Maßnahmen zur Gewährleistung der Cyber- und IT-Sicherheit

Die durchgeführten Maßnahmen zur Gewährleistung von Cyber- und IT-Sicherheit orientieren sich an den jeweils geltenden Standards des Bundesamtes für Sicherheit in der Informationstechnik und verbindlichen Beschlüssen des IT-Planungsrates. Die Umsetzung erfolgt durch das Zentrum für Informationssicherheit (Hessen 3C), ggf. in Zusammenarbeit mit weiteren für die Informationssicherheit zuständigen Organisationseinheiten sowie durch den Zentralen IT-Dienstleister des Landes Hessen. Im Rahmen der erforderlichen Maßnahmen zur Gewährleistung der Cyber- und IT-Sicherheit erfolgt eine Verarbeitung meiner personenbezogenen Daten im Rahmen der §§ 7–11 sowie 13 und 16 des Hessischen Gesetzes zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz – HITSiG).

Danach erfolgt eine Verarbeitung von personenbezogenen Daten im Rahmen der privaten Internetnutzung in Form einer automatisierten Erhebung und Auswertung von Log- und Protokolldaten. Die Auswertung erfolgt zum Zwecke der Sammlung, Auswertung oder Untersuchung von Informationen über Risiken oder Vorkehrungen für die Informationssicherheit, zur Unterstützung,

Beratung oder Warnung in Fragen der Informationssicherheit und zur Aufdeckung von Sicherheitslücken, Schadprogrammen oder erfolgten oder versuchten Angriffen auf die Informationstechnik. Die Erhebung und Auswertung betrifft den Datenverkehr innerhalb des Landesnetzes und an den Übergabe- und Knotenpunkten des Landesdatennetzes. Grundsätzlich erfolgt keine Speicherung der erhobenen Daten. Sofern aufgrund von zureichenden tatsächlichen Anhaltspunkten weitere Auswertungen erforderlich werden, ist im Einzelfall eine Speicherung von bis zu 90 Tagen zulässig.

Die Auswertung der erhobenen Daten erfolgt grundsätzlich automatisiert und ohne Personenbezug, nach vorheriger Anonymisierung (sofern im Einzelfall möglich) bzw. Pseudonymisierung. Sie bedarf einer Anordnung durch die Leitung des Zentrums für Informationssicherheit nach juristischer Prüfung durch eine Beschäftigte oder einen Beschäftigten des Innenressorts mit Befähigung zum Richteramt. In diesem Zusammenhang ist das Aufbrechen von ggf. vorhandener Verschlüsselungen (SSL-Tunneln) erforderlich. Eine direkt personenbezogene oder nicht automatisierte Auswertung erfolgt sofern hinreichende tatsächliche Anhaltspunkte den Verdacht begründen, dass die Ursache in einem Schadprogramm liegt oder sich aus den Daten Hinweise auf ein Schadprogramm ergeben und die Datenverarbeitung zur Abwehr des Schadprogramms, zur Abwehr von Gefahren, die von dem Schadprogramm ausgehen oder zur Erkennung und Abwehr anderer Schadprogramme erforderlich ist.

Mit den oben genannten Maßnahmen sind Einschränkungen meines Rechts auf Fernmeldegeheimnis (Art. 10 GG und Art. 12 der Verfassung des Landes Hessen) sowie meines Rechts auf informationelle Selbstbestimmung verbunden. Damit bin ich einverstanden.

Mir ist bekannt, dass im Falle eines konkreten Verdachts einer missbräuchlichen Nutzung alle vorhandenen Protokolldateien, die aus der privaten Nutzung von E-Mail und Internet resultieren, zur personenbezogenen Auswertung verwendet werden können. Zu diesem Zwecke kann die Anonymisierung bzw. Pseudonymisierung der Protokolldateien aufgehoben werden.

Mir ist bekannt, dass die Gestattung der Privatnutzung jederzeit eingeschränkt oder widerrufen werden kann. Auch ich kann diese Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen. Ab dem Zeitpunkt des Widerrufs darf ich den Internetzugang und den E-Mail-Dienst dann nicht mehr für private Zwecke nutzen.

Diese Erklärung ersetzt alle bisherigen Einwilligungserklärungen, die zur Nutzung von E-Mail- und/oder Internetdiensten abgegeben worden sind.

Die Einwilligungserklärung wird in meine Personalakte aufgenommen.

_____ _____

Ort, Datum Unterschrift

Anlage 2

Name:

Funktion:

Kenntnisnahme- und Einwilligungserklärung für die inner- und außerbehördlichen Interessenvertretungen, die Gleichstellungsbeauftragte, die behördliche Datenschutzbeauftrage oder den behördlichen Datenschutzbeauftragten sowie die Mitglieder der Landesregierung und die Staatssekretärinnen und Staatssekretäre

Die Richtlinie zur Nutzung von E-Mail und Internet in der Hessischen Landesverwaltung habe ich zur Kenntnis genommen und werde die dort gemachten Vorgaben beachten.

_____ _____

Ort, Datum Unterschrift

Ich möchte die von meiner Dienststelle zur Verfügung gestellten Internet- und E-Mail-Dienste, sofern durch die Richtlinie zugelassen, in geringfügigem Umfang auch für private Zwecke nutzen.

I. Für die inner- und außerbehördlichen Interessenvertretungen, die Gleichstellungsbeauftragte, die behördliche Datenschutzbeauftragte oder den behördlichen Datenschutzbeauftragten

Ich willige ein, dass mein privater E-Mail- und Internetverkehr in demselben Maße wie mein dienstlicher E-Mail- und Internetverkehr automatisch protokolliert wird.

Die Überprüfung unterbleibt bei einem Funktionspostfach, das ich als Mitglied der inner- und außerbehördlichen Interessenvertretung, als Gleichstellungsbeauftragte oder als behördliche Datenschutzbeauftragte oder behördlicher Datenschutzbeauftragter verwende. Bei einem konkreten Verdacht einer missbräuchlichen Nutzung können alle vorhandenen Protokolle zur personenbezogenen Auswertung verwendet werden und die Anonymität kann auch im Falle der Internetnutzung aufgehoben werden.

Ich gestatte ferner, dass meine privaten E-Mails bei möglicher Verseuchung mit Viren oder anderen Schadprogrammen sowie an mich adressierte unerwünschte oder unverlangt zugehende E-Mails – sog. Spam-Mails – automatisiert herausgefiltert und ggf. nicht zugestellt werden. Mir ist bekannt, dass dabei auch privat erwünschte E-Mails irrtümlich durch den Spamfilter ausgesondert werden können.

Sollten im Fall meiner Abwesenheit vom Arbeitsplatz an mich adressierte E-Mails an meine Vertretung weitergeleitet werden oder sie Zugriff auf mein persönliches Postfach nehmen, so billige ich das. Meine Vorgesetzte oder mein Vorgesetzter organisiert insbesondere für den Fall der ungeplanten Abwesenheit einen Zugriff auf mein persönliches E-Mail-Konto, wenn dies für einen ordnungsgemäßen betrieblichen Ablauf nötig sein sollte. Mir ist bewusst, dass dabei auch private E-Mails anderen Personen zur Kenntnis gelangen können.

Der Zugriff meiner Vorgesetzten oder meines Vorgesetzten ist für ein Funktionspostfach, das ich als Mitglied der inner- und außerbehördlichen Interessenvertretung, als Gleichstellungsbeauftragte oder als behördliche Datenschutzbeauftragte oder behördlicher Datenschutzbeauftragter verwende, untersagt.

Maßnahmen zur Gewährleistung der Cyber- und IT-Sicherheit

Die durchgeführten Maßnahmen zur Gewährleistung von Cyber- und IT-Sicherheit orientieren sich an den jeweils geltenden Standards des Bundesamtes für Sicherheit in der Informationstechnik und verbindlichen Beschlüssen des IT-Planungsrates. Die Umsetzung erfolgt durch das Zentrum für Informationssicherheit (Hessen 3C), ggf. in Zusammenarbeit mit weiteren für die Informationssicherheit zuständigen Organisationseinheiten sowie durch den Zentralen IT-Dienstleister des Landes Hessen. Im Rahmen der erforderlichen Maßnahmen zur Gewährleistung der Cyber- und IT-Sicherheit erfolgt eine Verarbeitung meiner personenbezogenen Daten im Rahmen der §§ 7–11 sowie 13 und 16 des Hessischen Gesetzes zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz – HITSiG).

Danach erfolgt eine Verarbeitung von personenbezogenen Daten im Rahmen der privaten Internetnutzung in Form einer automatisierten Erhebung und Auswertung von Log- und Protokolldaten. Die Auswertung erfolgt zum Zwecke der Sammlung, Auswertung oder Untersuchung von Informationen über Risiken oder Vorkehrungen für die Informationssicherheit, zur Unterstützung, Beratung oder Warnung in Fragen der Informationssicherheit und zur Aufdeckung von Sicherheitslücken, Schadprogrammen oder erfolgten oder versuchten Angriffen auf die Informationstechnik. Die Erhebung und Auswertung betrifft den Datenverkehr innerhalb des Landesnetzes und an den Übergabe- und Knotenpunkten des Landesdatennetzes. Grundsätzlich erfolgt keine Speicherung der erhobenen Daten. Sofern aufgrund von zureichenden tatsächlichen Anhaltspunkten weitere Auswertungen erforderlich werden, ist im Einzelfall eine Speicherung von bis zu 90 Tagen zulässig.

Die Auswertung der erhobenen Daten erfolgt grundsätzlich automatisiert und ohne Personenbezug, nach vorheriger Anonymisierung (sofern im Einzelfall möglich) bzw. Pseudonymisierung. Sie bedarf einer Anordnung durch die Leitung des Zentrums für Informationssicherheit nach juristischer Prüfung durch eine Beschäftigte oder einen Beschäftigten des Innenressorts mit Befähigung zum Richteramt. In diesem Zusammenhang ist das Aufbrechen von ggf. vorhandener Verschlüsselungen (SSL-Tunneln) erforderlich. Eine direkt personenbezogene oder nicht automatisierte Auswertung erfolgt sofern hinreichende tatsächliche Anhaltspunkte den Verdacht begründen, dass die Ursache in einem Schadprogramm liegt oder sich aus den Daten Hinweise auf ein Schadprogramm ergeben und die Datenverarbeitung zur Abwehr des Schadprogramms, zur Abwehr von Gefahren, die von dem Schadprogramm ausgehen oder zur Erkennung und Abwehr anderer Schadprogramme erforderlich ist.

Mit den oben genannten Maßnahmen sind Einschränkungen meines Rechts auf Fernmeldegeheimnis (Art. 10 GG und Art. 12 der Verfassung des Landes Hessen) sowie meines Rechts auf informationelle Selbstbestimmung verbunden. Damit bin ich einverstanden.

Mir ist bekannt, dass im Falle eines konkreten Verdachts einer missbräuchlichen Nutzung alle vorhandenen Protokolldateien, die

aus der privaten Nutzung von E-Mail und Internet resultieren, zur personenbezogenen Auswertung verwendet werden können. Zu diesem Zwecke kann die Anonymisierung bzw. Pseudonymisierung der Protokolldateien aufgehoben werden.

Mir ist bekannt, dass die Gestattung der Privatnutzung jederzeit eingeschränkt oder widerrufen werden kann. Auch ich kann diese Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen. Ab dem Zeitpunkt des Widerrufs darf ich den Internetzugang und den E-Mail-Dienst dann nicht mehr für private Zwecke nutzen.

Diese Erklärung ersetzt alle bisherigen Einwilligungserklärungen, die zur Nutzung von E-Mail- und/oder Internetdiensten abgegeben worden sind.

Die Einwilligungserklärung wird in meine Personalakte aufgenommen.

Ort, Datum Unterschrift

II. Für die Mitglieder der Landesregierung sowie die Staatssekretärinnen und Staatssekretäre

Ich willige ein, dass mein privater E-Mail- und Internetverkehr in demselben Maße wie mein dienstlicher E-Mail- und Internetverkehr automatisch protokolliert wird. Ich bin damit einverstanden, dass diese Protokolldaten wie in der Richtlinie unter Punkt 4 beschrieben temporär gespeichert werden. Die Internetnutzung kann stichprobenartig überprüft werden.

Bei einem konkreten Verdacht einer missbräuchlichen Nutzung können alle vorhandenen Protokolle zur personenbezogenen Auswertung verwendet werden und die Anonymität kann auch im Falle der Internetnutzung aufgehoben werden.

Ich gestatte ferner, dass meine privaten E-Mails bei möglicher Verseuchung mit Viren oder anderen Schadprogrammen sowie an mich adressierte unerwünschte oder unverlangt zugehende E-Mails – sog. Spam-Mails – automatisiert herausgefiltert und ggf. nicht zugestellt werden. Mir ist bekannt, dass dabei auch privat erwünschte E-Mails irrtümlich durch den Spamfilter ausgesondert werden können.

Maßnahmen zur Gewährleistung der Cyber- und IT-Sicherheit

Die durchgeführten Maßnahmen zur Gewährleistung von Cyber- und IT-Sicherheit orientieren sich an den jeweils geltenden Standards des Bundesamtes für Sicherheit in der Informationstechnik und verbindlichen Beschlüssen des IT-Planungsrates. Die Umsetzung erfolgt durch das Zentrum für Informationssicherheit (Hessen 3C), ggf. in Zusammenarbeit mit weiteren für die Informationssicherheit zuständigen Organisationseinheiten sowie durch den Zentralen IT-Dienstleister des Landes Hessen. Im Rahmen der erforderlichen Maßnahmen zur Gewährleistung der Cyber- und IT-Sicherheit erfolgt eine Verarbeitung meiner personenbezogenen Daten im Rahmen der §§ 7–11 sowie 13 und 16 des Hessischen Gesetzes zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz – HITSiG).

Danach erfolgt eine Verarbeitung von personenbezogenen Daten im Rahmen der privaten Internetnutzung in Form einer automatisierten Erhebung und Auswertung von Log- und Protokolldaten. Die Auswertung erfolgt zum Zwecke der Sammlung, Auswertung oder Untersuchung von Informationen über Risiken oder Vorkehrungen für die Informationssicherheit, zur Unterstützung, Beratung oder Warnung in Fragen der Informationssicherheit und zur Aufdeckung von Sicherheitslücken, Schadprogrammen oder erfolgten oder versuchten Angriffen auf die Informationstechnik. Die Erhebung und Auswertung betrifft den Datenverkehr innerhalb des Landesnetzes und an den Übergabe- und Knotenpunkten des Landesdatennetzes. Grundsätzlich erfolgt keine Speicherung der erhobenen Daten. Sofern aufgrund von zureichenden tatsächlichen Anhaltspunkten weitere Auswertungen erforderlich werden, ist im Einzelfall eine Speicherung von bis zu 90 Tagen zulässig.

Die Auswertung der erhobenen Daten erfolgt grundsätzlich automatisiert und ohne Personenbezug, nach vorheriger Anonymisierung (sofern im Einzelfall möglich) bzw. Pseudonymisierung. Sie bedarf einer Anordnung durch die Leitung des Zentrums für Informationssicherheit nach juristischer Prüfung durch eine Beschäftigte oder einen Beschäftigten des Innenressorts mit Befähigung zum Richteramt. In diesem Zusammenhang ist das Aufbrechen von ggf. vorhandener Verschlüsselungen (SSL-Tunneln) erforderlich. Eine direkt personenbezogene oder nicht automatisierte Auswertung erfolgt sofern hinreichende tatsächliche Anhaltspunkte den Verdacht begründen, dass die Ursache in einem Schadprogramm liegt oder sich aus den Daten Hinweise auf ein Schadprogramm ergeben und die Datenverarbeitung zur Abwehr des Schadprogramms, zur Abwehr von Gefahren, die von dem Schadprogramm ausgehen oder zur Erkennung und Abwehr anderer Schadprogramme erforderlich ist.

Mit den oben genannten Maßnahmen sind Einschränkungen meines Rechts auf Fernmeldegeheimnis (Art. 10 GG und Art. 12 der Verfassung des Landes Hessen) sowie meines Rechts auf informationelle Selbstbestimmung verbunden. Damit bin ich einverstanden.

Mir ist bekannt, dass im Falle eines konkreten Verdachts einer missbräuchlichen Nutzung alle vorhandenen Protokolldateien, die aus der privaten Nutzung von E-Mail und Internet resultieren, zur personenbezogenen Auswertung verwendet werden können. Zu diesem Zwecke kann die Anonymisierung bzw. Pseudonymisierung der Protokolldateien aufgehoben werden.

Mir ist bekannt, dass die Gestattung der Privatnutzung jederzeit eingeschränkt oder widerrufen werden kann. Auch ich kann diese Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen. Ab dem Zeitpunkt des Widerrufs darf ich den Internetzugang und den E-Mail-Dienst dann nicht mehr für private Zwecke nutzen.

Diese Erklärung ersetzt alle bisherigen Einwilligungserklärungen, die zur Nutzung von E-Mail- und/oder Internetdiensten abgegeben worden sind.

Die Einwilligungserklärung wird in meine Personalakte aufgenommen.

Ort, Datum Unterschrift

871

Richtlinie über die dienstliche und private Nutzung der Telekommunikationseinrichtungen in der Landesverwaltung (Telekommunikationsrichtlinie);

Ergänzung der Anlage „Kenntnisnahme- und Einwilligungserklärung“ sowie Verlängerung der Geltungsdauer

Bezug: Telekommunikationsrichtlinie vom 21. Juni 2013 (StAnz. S. 890), zuletzt geändert durch Erlass vom 5. Dezember 2022 (StAnz. S. 1416)

Die vorgenannte Richtlinie wird wie folgt geändert:

1. Die Anlage „Kenntnisnahme- und Einwilligungserklärung“ wurde hinsichtlich der Maßnahmen zur Gewährleistung der Cyber- und IT-Sicherheit ergänzt und wird nachstehend bekannt gemacht.
2. Die Geltungsdauer wird bis zum 31. Dezember 2025 verlängert.
3. Dieser Erlass tritt am Tage nach der Bekanntmachung in Kraft.

Wiesbaden, den 31. Oktober 2023

Hessisches Ministerium des Innern und für Sport
Z 1-03d08-01-17/010
– Gült.-Verz. 30 –

StAnz. 47/2023 S. 1460

Anlage

Name:

Referat:

Kenntnisnahme- und Einwilligungserklärung

Die Richtlinie über die dienstliche und private Nutzung der Telekommunikationsanlagen der Hessischen Landesverwaltung habe ich zur Kenntnis genommen und werde die dort gemachten Vorgaben beachten.

Ort, Datum Unterschrift

Ich möchte die von meiner Dienststelle zur Verfügung gestellten Telefonanlagen, sofern durch die Richtlinie zugelassen, in geringfügigem Umfang auch für private Zwecke nutzen.

Ich willige ein, dass zum Zwecke der Kontrolle der Einhaltung der Vorgaben dieser Richtlinie die während der Telekommunikation entstehenden Verbindungsdaten protokolliert werden. Ich bin damit einverstanden, dass diese Verbindungsdaten wie in der Richtlinie unter Punkt 5 beschrieben temporär gespeichert werden können.

Maßnahmen zur Gewährleistung der Cyber- und IT-Sicherheit

Die durchgeführten Maßnahmen zur Gewährleistung von Cyber- und IT-Sicherheit orientieren sich an den jeweils geltenden Standards des Bundesamtes für Sicherheit in der Informationstechnik und verbindlichen Beschlüssen des IT-Planungsrates. Die Umsetzung erfolgt durch das Zentrum für Informationssicherheit (Hessen 3C), ggf. in Zusammenarbeit mit weiteren für die Informationssicherheit zuständigen Organisationseinheiten sowie durch den Zentralen IT-Dienstleister des Landes Hessen. Im Rahmen der erforderlichen Maßnahmen zur Gewährleistung der Cyber- und IT-Sicherheit erfolgt eine Verarbeitung meiner personenbezogenen Daten im Rahmen der §§ 7–11 sowie 13 und 16 des Hessischen Gesetzes zum Schutz der elektronischen Verwaltung (Hessisches IT-Sicherheitsgesetz – HITSiG).

Danach erfolgt eine Verarbeitung von personenbezogenen Daten im Rahmen der privaten Telefonnutzung in Form einer automatisierten Erhebung und Auswertung von Log- und Protokolldaten. Die Auswertung erfolgt zum Zwecke der Sammlung, Auswertung oder Untersuchung von Informationen über Risiken oder Vorkehrungen für die Informationssicherheit, zur Unterstützung, Beratung oder Warnung in Fragen der Informationssicherheit und zur Aufdeckung von Sicherheitslücken, Schadprogrammen oder erfolgten oder versuchten Angriffen auf die Informationstechnik. Die Erhebung und Auswertung betrifft den Datenverkehr innerhalb des Landesnetzes und an den Übergabe- und Knotenpunkten des Landesdatennetzes. Grundsätzlich erfolgt keine Speicherung der erhobenen Daten. Sofern aufgrund von zureichenden tatsächlichen Anhaltspunkten weitere Auswertungen erforderlich werden, ist im Einzelfall eine Speicherung von bis zu 90 Tagen zulässig.

Die Auswertung der erhobenen Daten erfolgt grundsätzlich automatisiert und ohne Personenbezug, nach vorheriger Anonymisierung (sofern im Einzelfall möglich) bzw. Pseudonymisierung. Sie bedarf einer Anordnung durch die Leitung des Zentrums für Informationssicherheit nach juristischer Prüfung durch eine Beschäftigte oder einen Beschäftigten des Innenressorts mit Befähigung zum Richteramt. In diesem Zusammenhang ist das Aufbrechen von ggf. vorhandener Verschlüsselungen (SSL-Tunneln) erforderlich. Eine direkt personenbezogene oder nicht automatisierte Auswertung erfolgt sofern hinreichende tatsächliche Anhaltspunkte den Verdacht begründen, dass die Ursache in einem Schadprogramm liegt oder sich aus den Daten Hinweise auf ein Schadprogramm ergeben und die Datenverarbeitung zur Abwehr des Schadprogramms, zur Abwehr von Gefahren, die von dem Schadprogramm ausgehen oder zur Erkennung und Abwehr anderer Schadprogramme erforderlich ist.

Mit den oben genannten Maßnahmen sind Einschränkungen meines Rechts auf Fernmeldegeheimnis (Art. 10 GG und Art. 12 der Verfassung des Landes Hessen) sowie meines Rechts auf informationelle Selbstbestimmung verbunden. Damit bin ich einverstanden.

Mir ist bekannt, dass im Falle eines konkreten Verdachts einer missbräuchlichen Nutzung alle vorhandenen Protokolldateien, die aus der privaten Nutzung der Telekommunikations- bzw. Telefonanlagen resultieren, zur personenbezogenen Auswertung verwendet werden können. Zu diesem Zwecke kann die Anonymisierung bzw. Pseudonymisierung der Protokolldateien aufgehoben werden.

Mir ist bekannt, dass die Gestattung der Privatnutzung jederzeit eingeschränkt oder widerrufen werden kann. Auch ich kann diese Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen. Ab dem Zeitpunkt des Widerrufs darf ich die Telekommunikationsanlage dann nicht mehr für private Zwecke nutzen.

Diese Erklärung ersetzt alle bisherigen Einwilligungserklärungen, die zur Nutzung von Telekommunikations-/Telefonanlagen abgegeben worden sind.

Die Einwilligungserklärung wird in meine Personalakte aufgenommen.

Ort, Datum Unterschrift

HESSISCHES MINISTERIUM DER FINANZEN

872

Übertragung von Haushaltsermächtigungen in das Haushaltsjahr 2024

Bei der Übertragung von Haushaltsresten des Haushaltsjahres 2023 in das Haushaltsjahr 2024 sind neben den VV zu § 45 LHO die folgenden Ausführungen zu beachten:

1. Grundsätzliches

Der Gesamtbetrag der übertragenen Ausgabereste ist in den letzten Jahren bis auf rd. 1,8 Mrd. Euro im Jahr 2022 stetig angewachsen. Da im Haushalt des Landes traditionell keine Deckungsmittel zur Finanzierung übertragener Haushaltsreste veranschlagt werden, muss jeder in Anspruch genommene Ausgaberest durch Einsparungen an anderer Stelle (möglichst im gleichen Einzelplan) gegenfinanziert werden (§ 45 Abs. 3 LHO). Die hierfür erforderlichen Spielräume werden mit Blick auf schon bestehende oder künftige zusätzliche Haushaltsbelastungen immer enger, zumal im Haushaltsvollzug 2023 und 2024 jeweils noch eine Globale Minderausgabe von 450 Mio. Euro erwirtschaftet werden muss. Ziel ist daher ein Abschmelzen der Haushaltsreste.

Aus diesem Grund kann die Bildung von Ausgaberesten im laufenden Jahr nur noch sehr restriktiv erfolgen. Sie muss sich im Wesentlichen auf bereits gebundene Ausgabemittel und auf Drittmittel beschränken; die Übertragung ungebundener Ausgabereste kann nur in Ausnahmefällen in Betracht kommen.

Nach VV Nr. 6 zu § 45 LHO soll der Übertragung von Ausgaberesten nur zugestimmt werden, wenn in demselben oder einem anderen Einzelplan entsprechende Einsparungen erbracht werden können. Da bereits jetzt absehbar ist, dass in früheren Jahren verfügbare Spielräume in den zentralen Einzelplänen 17 und 18 in der erforderlichen Höhe nicht mehr vorhanden sein werden, bitte ich um Verständnis, dass ich Anträgen auf Übertragung von Ausgaberesten grundsätzlich nur zustimmen kann, wenn im Rahmen der Antragstellung die Bereitschaft erklärt wird, bei Inanspruchnahme eine Einsparung im gleichen Einzelplan sicherzustellen. Spätestens bei der Inanspruchnahme des übertragenen Ausgaberestes ist eine entsprechende Einsparungsstelle zu benennen.

2. Übertragbarkeit von Haushaltsermächtigungen

Voraussetzung für eine Übertragung von Haushaltsermächtigungen ist ihre grundsätzliche Übertragbarkeit. Nach § 19 Abs. 1 der Hessischen Landeshaushaltsordnung (LHO) sind Ausgaben für Investitionen und Ausgaben aus zweckgebundenen Einnahmen übertragbar. Andere Ausgaben und Aufwendungen können im Haushaltsplan für übertragbar erklärt werden, wenn dies der wirtschaftlichen und sparsamen Haushaltsführung dient. Für Aufwendungen und Ausgaben für Förderprogramme ist dies mit § 6 Abs. 5 HG 2023/2024 erfolgt; die Einzelpläne können darüber hinausgehende Übertragbarkeitsvermerke enthalten. Zusätzlich enthält § 45 Abs. 4 LHO eine Ermächtigung meines Hauses, in besonders begründeten Einzelfällen die Übertragbarkeit von Aufwendungen und Ausgaben im Haushaltsvollzug zuzulassen; hierzu verweise ich auf VV Nr. 3 zu § 45 LHO.

3. Höhe der Haushaltsreste

Haushaltsreste können nur insoweit gebildet werden, als die Haushaltsermächtigungen im Haushaltsvollzug nicht in Anspruch genommen worden sind, der Zweck der Haushaltsermächtigung

HESSISCHE STAATSKANZLEI

HESSISCHES MINISTERIUM DES INNERN UND FÜR SPORT

390

Katastrophenschutz in Hessen

Hiermit führe ich die KatS-Dienstvorschriften 400 – Der Sanitätszug – und 600 – Der Betreuungszug – mit Wirkung vom 1. April 2012 ein.

Dieser Erlass tritt mit Ablauf des 31. März 2017 außer Kraft.

Von einem Abdruck des Textes im Staatsanzeiger für das Land Hessen wird wegen des Umfangs abgesehen. Die **KatS DV 400** und **KatS DV 600** sind im Internet auf der Homepage des Hessischen Ministeriums des Innern und für Sport (www.hmdis.hessen.de) abrufbar.

Wiesbaden, 31. März 2012

Hessisches Ministerium
des Innern und für Sport
V 4 – 24 t 10 04 –
– Gült.-Verz. 312 –

StAnz. 19/2012 S. 526

391

Richtlinie zur Nutzung von E-Mail- und Internetdiensten in der Hessischen Landesverwaltung

1 **Allgemeines**

1.1. **Geltungsbereich**

1.1.1. Die Richtlinie gilt verbindlich für alle Beschäftigten der Hessischen Landesverwaltung, die Zugang zu dienstlichen E-Mail- und/oder Internetdiensten haben. Sie regelt die dienstliche und private Nutzung von Internet und E-Mail am Arbeitsplatz. Dies gilt entsprechend für externe Mitarbeiterinnen und Mitarbeiter, sofern ihnen ein Arbeitsplatz zur Verfügung gestellt wird.

1.1.2. Die Richtlinie gilt nicht für das Ressort Hessisches Ministerium der Justiz, für Integration und Europa. Das Ressort wird für seinen Zuständigkeitsbereich eine eigene Regelung erlassen. Die Richtlinie gilt ferner nicht für die Beschäftigten an den Hessischen Hochschulen und sonstigen Forschungseinrichtungen im Aufsichtsbereich des Hessischen Ministeriums für Wissenschaft und Kunst sowie für die Beschäftigten an den Hessischen allgemeinbildenden und berufsbildenden Schulen und den Fachschulen. Sofern dort keine verbindlichen Vorgaben zum Umgang der Beschäftigten mit E-Mail- und Internetdiensten bestehen, sind diese Einrichtungen gehalten, eine entsprechende Regelung zu verabschieden.

Ausgenommen vom Geltungsbereich der Richtlinie sind das Virtuelle Private Netz (VPN) der Polizei sowie das eigene Netz des Landesamtes für Verfassungsschutz („rotes Netz“).

Ebenfalls ausgenommen sind die Tätigkeiten im Zusammenhang mit der operativen Nachrichtenbeschaffung des Landesamtes für Verfassungsschutz Hessen sowie die nicht offene Ermittlungstätigkeit der Polizei.

1.1.3. Bezüglich der E-Mail-Nutzung regelt sie sowohl den internen elektronischen Geschäftsverkehr zwischen Behörden der Landesverwaltung als auch die Korrespondenz nach außen, zum Beispiel mit Bürgerinnen und Bürgern oder anderen Behörden.

1.2. **Organisatorische Grundsätze**

1.2.1. In Dienststellen ist jeweils mindestens ein zentrales E-Mail-Postfach mit einer Adresse entsprechend dem Muster „poststelle@dienststelle.hessen.de“ einzurichten. Darüber hinaus sollen personenbezogene Postfächer und – soweit erforderlich – Postfächer für Organisationseinheiten eingerichtet werden (zum Beispiel für Abteilungen, Referate, Interessenvertretungen, Datenschutzbeauftragte, Suchtbeauftragte).

1.2.2. Die für das Land Hessen festgelegten Namenskonventionen sind zu beachten (vgl. hierzu den Erlass über „Standards der E-Governmentarchitektur in der Hessischen Landesverwaltung“ vom 3. Februar 2005, Anlage 3 „Technische Spezifikation E-Mail“ (StAnz. S. 854 ff). Ausnahmen sind im nachgeordneten Bereich des Hessischen Ministeriums für Wissenschaft und Kunst möglich.

1.2.3. Für die Teilnahme am elektronischen Geschäftsverkehr sind grundsätzlich nur die dienstlich zur Verfügung gestellten technischen Einrichtungen zu nutzen.

1.2.4. Posteingänge sind entsprechend den Regelungen des Erlasses zur Aktenführung in den Dienststellen des Landes Hessen vom 16. Mai 2007 (StAnz. S. 1123) sowie den einschlägigen Geschäftsordnungen in der jeweils gültigen Fassung zu behandeln.

1.2.5. Die Absenderin oder der Absender ist für den Fall eingehender, nicht lesbarer E-Mails (zum Beispiel bei beschädigten Dokumenten, unbekanntem Dateiformat, verschlüsselter Nachricht) hierüber unverzüglich zu informieren.

1.3. **Allgemeine Grundsätze**

1.3.1. E-Mail- und Internetnutzung sollen grundsätzlich nur zu dienstlichen Zwecken erfolgen.

1.3.2. Die private Nutzung ist nur in geringfügigem Umfang zulässig, wenn dienstliche Belange nicht entgegenstehen und die Beschäftigte oder der Beschäftigte die in der Anlage 1 befindliche Einwilligungserklärung zuvor schriftlich abgegeben hat. Für die inner- und außerbehördlichen Interessenvertretungen, die Frauenbeauftragte, die behördliche Datenschutzbeauftragte oder den behördlichen Datenschutzbeauftragten, die Mitglieder der Landesregierung sowie die Staatssekretärinnen und Staatssekretäre gilt die in der Anlage 2 befindliche Einwilligungserklärung. Dienstliche Belange stehen insbesondere entgegen, wenn die Nutzung geeignet ist, den Dienstbetrieb zu beeinträchtigen, den Interessen und dem Ansehen des Landes zu schaden, die Verfügbarkeit der IT-Systeme für dienstliche Zwecke zu beeinträchtigen oder die Nutzung gegen geltendes Recht, insbesondere gegen persönlichkeitsrechtliche, datenschutzrechtliche, urheberrechtliche oder strafrechtliche Bestimmungen verstößt. Die Einhaltung des gestatteten Nutzungsumfangs wird gemäß Ziffer 4 überwacht. Die Gewährung der privaten Nutzung erfolgt freiwillig. Es entsteht kein Rechtsanspruch für die Zukunft. Die Gestattung der Nutzung zu privaten Zwecken kann jederzeit eingeschränkt oder widerrufen werden.

1.3.3. Wird die Einwilligung zur privaten Nutzung von Internet und E-Mail (Anlagen) nicht abgegeben, ist ein privater Gebrauch von Internet und E-Mail ausdrücklich untersagt. Die Einhaltung dessen wird gemäß Ziffer 4 überwacht.

1.3.4. In keinem Fall darf die Nutzung der dienstlichen E-Mail-Adresse zu nennenswerten Betriebsablaufstörungen führen.

2 **E-Mail-Verkehr**

2.1. Grundsätzlich sollen alle Dokumente per E-Mail versandt werden, sofern nicht durch Rechtsvorschrift Schriftform vorgegeben ist. Gemäß § 3 a HessVwVfG kann eine durch Rechtsvorschrift angeordnete Schriftform, soweit rechtlich möglich, durch die elektronische Form ersetzt werden. In diesem Fall ist das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 17. Juli 2009 (BGBl. I S. 2091) in der jeweils geltenden Fassung zu versehen. Im elektronischen Geschäftsverkehr innerhalb der eigenen Dienststelle oder mit anderen Dienststellen der hessischen Landesverwaltung und anderen Behörden ist in der Regel weder der Einsatz der fortgeschrittenen noch der qualifizierten Signatur erforderlich. Es genügt die Angabe der Dienststelle und des Namens der unterzeichnenden Person.

2.2. Um die Veränderbarkeit des elektronischen Dokuments zu erschweren, sollte eine Umwandlung in ein PDF oder vergleichbares Format erfolgen. Von einem zusätzlichen Versand in Papierform ist abzusehen.

2.3. **Vertrauliche Daten/Verschlusssachen**

2.3.1. Die Übertragung von vertraulich zu behandelnden Daten an Empfängerinnen und Empfänger außerhalb des Hessennetzes darf auf elektronischem Weg nur verschlüsselt erfolgen. Personalaktenrelevante Daten und Daten, für die eine ähnliche Missbrauchsgefahr besteht, dürfen auch innerhalb des Hessennetzes nur PKI-verschlüsselt übertragen werden.

2.3.2. Die Bestimmungen der Verschlusssachenanweisung für das Land Hessen (VSA) sind zu beachten.

2.4. In einem elektronischen Dokument (E-Mails sowie beigefügte Dateien) genügt an Stelle der Unterschrift der Vermerk „gez." in Verbindung mit dem Namen der unterzeichnenden Person und der Fixierung des Datums entsprechend dem jeweiligen Bearbeitungsstand. Darüber hinaus müssen ein aussagefähiger Betreff in Bezug auf den Inhalt der E-Mail sowie die Dienststelle, die Organisationseinheit und die Kontaktdaten der Bearbeiterin oder des Bearbeiters enthalten sein. Letztere Angaben sind in der Regel der E-Mail-Signatur zu entnehmen. Der Versand der aktenrelevanten elektronischen Dokumente ist in geeigneter Weise aktenkundig zu machen.

Bei ausnahmsweiser privater E-Mail-Nutzung darf keine dienstliche Signatur verwendet werden.

2.5. Bei geplanter Abwesenheit (zum Beispiel Urlaub, Gleittag, Dienstreise) ist eine Vertretung jeder Beschäftigten und jedes Beschäftigten hinsichtlich der E-Mail-Nutzung sicherzustellen. Sie hat grundsätzlich durch Weiterleitung der E-Mail-Eingänge oder Zugriffsgewährung auf das E-Mail-Postfach zu erfolgen. Sofern es sachdienlich erscheint, kann auch eine bloße Abwesenheitsbenachrichtigung unter Angabe der Erreichbarkeit (Telefon/E-Mail) der Vertreterin oder des Vertreters oder die Verwendung eines Funktionspostfachs genügen. Die Vorgesetzte oder der Vorgesetzte organisiert insbesondere für den Fall der ungeplanten Abwesenheit einer Beschäftigten oder eines Beschäftigten einen Zugriff auf deren oder dessen E-Mail-Postfach, um die Aufrechterhaltung eines ordnungsgemäßen dienstlichen Ablaufs zu gewährleisten.

Eine automatisierte Weiterleitung an private E-Mail-Postfächer ist unzulässig.

Im Rahmen der Vertretung oder der Erledigung sonstiger dienstlicher Aufgaben (Systemadministration) muss die Beschäftigte oder der Beschäftigte bei eingehenden privaten E-Mails damit rechnen, dass diese von anderen Beschäftigten zur Kenntnis genommen werden können. E-Mails mit offensichtlich privatem Charakter dürfen im Rahmen der Vertretung oder Systemadministration nicht geöffnet werden. Offenbart sich der private Charakter erst nach dem Öffnen der E-Mail, ist diese unverzüglich zu schließen, daraus erlangte Informationen unterliegen der dienstlichen Verschwiegenheitspflicht.

2.6. Ziffer 2.5. gilt nicht für die Funktionspostfächer der inner- und außerbehördlichen Interessenvertretungen, der Frauenbeauftragten, der behördlichen Datenschutzbeauftragten oder des behördlichen Datenschutzbeauftragten sowie die Postfächer der Mitglieder der Landesregierung und der Staatssekretärinnen und Staatssekretäre.

2.7. Alle eingehenden E-Mails werden ungeachtet ihres Inhalts automatisiert auf Standardkonformität, Viren oder andere Schadprogramme und SPAM-Wahrscheinlichkeit geprüft. In Abhängigkeit des Prüfergebnisses werden die E-Mails entweder nicht angenommen, in „Quarantäne" genommen oder zugestellt. Aus technischen Gründen kann hierbei nicht zwischen dienstlichen und privaten E-Mails unterschieden werden. Im Einzelfall kann dies dazu führen, dass E-Mails falsch klassifiziert und nicht zugestellt werden.

2.8. Ist bei einer eingehenden E-Mail aufgrund der Absenderangabe, der Betreffzeile, der Anlage, einer Meldung des Virenerkennungsprogramms oder sonstiger Umstände der Verdacht eines Virus oder eines anderen Schadprogramms gegeben, sind unverzüglich die IT-Administration und – soweit vorhanden – die IT-Sicherheitsbeauftragte oder der IT-Sicherheitsbeauftragte zu benachrichtigen und die Öffnung der E-Mail und eventueller Anlagen hat zu unterbleiben.

3 **Internetnutzung**

3.1 Die Internetnutzung zu dienstlichen Zwecken ist unter Beachtung des geltenden Rechts, insbesondere der persönlichkeitsrechtlichen, datenschutzrechtlichen, urheberrechtlichen und strafrechtlichen Vorschriften zulässig. Entgeltliche Recherchen erfordern vorab die Zustimmung der Vorgesetzten oder des Vorgesetzten.

3.2 Zu privaten Zwecken ist die Nutzung von Internet-Diensten gemäß Ziffer 1.3.2. in geringfügigem Umfang zulässig. Unzulässig sind jedoch insbesondere das Herunterladen von Programmen und anderen ausführbaren Dateien, die Nutzung von Audio und Video Streams, die Teilnahme an Sozialen Netzwerken (zum Beispiel Foren, Blogs etc.), Netz-, Onlinespielen und Auktionen sowie die Verfolgung gewerblicher Zwecke. Unzulässig ist ferner das Aufrufen oder Herunterladen diskriminierender, beleidigender, verleumderischer, menschenverachtender, verfassungsfeindlicher, gewaltverherrlichender, rassistischer, sexistischer, pornographischer und anderer außerhalb des gesetzlichen Rahmens befindlicher Inhalte.

4 **Protokollierung/Kontrolle/Sanktionen**

4.1. Die Nutzung von E-Mail und Internet wird protokolliert. Eine Trennung in private und dienstliche Nutzung findet hierbei nicht statt. Bei der E-Mail Nutzung entstehen regelmäßig die folgenden Protokolldaten: Absenderin oder Absender, Empfängerin oder Empfänger, Datum und Uhrzeit des Versands und übertragene Datenmenge. Bei der Internetnutzung entstehen in der Regel die folgenden Protokolldaten: Benutzerkennung, Start-IP-Adresse, Ziel-IP-Adresse und aufgerufene URL[1], Datum und Uhrzeit, übertragene Datenmenge. Die Protokolldaten dienen dabei der Sicherstellung eines ordnungsgemäßen Betriebes des Systems, der Kapazitätsplanung sowie der Verfolgung von Verstößen gegen diese Richtlinie, im Übrigen aber nicht der Verhaltens- und Leistungskontrolle der Beschäftigten.

[1] zum Beispiel www.hessen.de

4.2. Bis zum Aufbau einer eigenen IT-Infrastruktur mit entsprechenden Sicherheits- und Zugriffsmaßnahmen ist das Hessische Landesamt für Verfassungsschutz von der Pflicht zur Protokollierung befreit. Solange eine Protokollierung hier nicht erfolgt, ist die private Nutzung von E-Mail und Internet durch die Beschäftigten des Hessischen Landesamts für Verfassungsschutz untersagt.

4.3. Je nach IT-Architektur der einzelnen Dienststelle erfolgt die Protokollierung der Internetnutzung durch die HZD, durch die Dienststelle selbst oder durch eine von ihr beauftragte dritte Person. Soweit gesetzlich nicht eine längere Speicherung vorgeschrieben ist, werden die durch Nutzung des Internets entstandenen Protokolle und Protokolldaten spätestens nach Ablauf von sechs Monaten wieder gelöscht. Die Protokollierung der E-Mail- Nutzung erfolgt zentral durch die HZD. Die durch die Nutzung von E-Mail entstandenen Protokolldaten ihrer Beschäftigten werden den Dienststellen von der HZD regelmäßig zur Verfügung gestellt. Die Dienststellen führen sodann die Stichprobenkontrollen unter Beachtung der in Ziffer 4.3.1. geregelten Vorgaben in eigener Verantwortung durch. Die Protokolle und Protokolldaten, die durch die Nutzung von E-Mail entstanden sind, werden spätestens nach drei Monaten gelöscht. Wenn eine längere Aufbewahrung gesetzlich vorgeschrieben ist, können die Protokolle und Protokolldaten bis zur Erfüllung der gesetzlichen Vorschriften aufbewahrt werden. Nach Ablauf der Aufbewahrungsdauer sind diese zu löschen. Auf Anfrage einer Beschäftigten oder eines Beschäftigten sind die einzelnen Dienststellen verpflichtet, eine Verfahrensbeschreibung vorzulegen, die über die technischen Verfahrensabläufe bei der Protokollierung Auskunft gibt.

4.3.1. Eine Kontrolle der nach Ziffer 4.1. angefallenen Protokolldaten erfolgt stichprobenartig. Die Auswertung der Internetnutzung erfolgt in einem ersten Schritt ohne Personenbezug. Die Stichprobenkontrolle ist in regelmäßigen Abständen, in einem repräsentativen Umfang und nach dem Zufallsprinzip durchzuführen. Empfohlen wird, eine solche Stichprobe vierteljährlich (90 Tage) an einem zufällig ausgewählten Tag in einem zufällig ausgewählten Zeitraum durchzuführen und als Basis alle Beschäftigten einer Dienststelle zu berücksichtigen. Je nach den individuellen Gegebenheiten der Dienststelle ist die Durchführung anderer Kontrollverfahren möglich, sofern den in Satz 3 skizzierten Prinzipien ausreichend Rechnung getragen wird. Eine entsprechende Regelung erfolgt in Abstimmung mit der örtlichen Personalvertretung. Die Kontrolle der Protokolle erfolgt durch eine von der Dienststelle beauftragte Beschäftigte oder einen von der Dienststelle beauftragten Beschäftigten. Im Falle der E-Mail-Nutzung erfolgt die Kontrolle in Anwesenheit einer Vertreterin oder eines Vertreters der Personalvertretung sowie der Datenschutzbeauftragten oder des Datenschutzbeauftragten der Dienststelle. Die Beauftragung der Beschäftigten oder des Beschäftigten ist aktenkundig zu machen.

Die Funktionspostfächer der inner- und außerbehördlichen Interessenvertretungen, der Frauenbeauftragten, der behördlichen Datenschutzbeauftragten oder des behördlichen Datenschutzbeauftragten sowie die Postfächer der Mitglieder der Landesregierung und der Staatssekretärinnen und Staatssekretäre sind von der Stichprobenkontrolle ausgenommen.

4.3.2. Ergibt sich aus der Durchführung der Stichproben oder aus anderen Gründen, die über die Dienststellenleiterin oder den Dienststellenleiter vorgebracht werden müssen, der konkrete Verdacht einer missbräuchlichen oder unerlaubten Nutzung von E-Mail und/oder Internet (zum Beispiel bei Verstoß gegen diese Richtlinie), können alle vorhandenen Protokolle zur personenbezogenen Auswertung verwendet werden und die Anonymität kann auch im Falle der Internetnutzung aufgehoben werden. Insbesondere ist es dann zulässig, den Personenbezug zwischen IP-Adresse und der Beschäftigten oder dem Beschäftigten herzustellen. Die Personalvertretung und die Datenschutzbeauftragte oder der Datenschutzbeauftragte der Dienststelle sind vom Verdacht zu informieren und nehmen an der Datenauswertung teil. Die Auswertungen sind zu dokumentieren und grundsätzlich der Beschäftigten oder dem Beschäftigten durch die Dienstvorgesetzte oder den Dienstvorgesetzten unverzüglich mitzuteilen. Der Beschäftigten oder dem Beschäftigten wird die Möglichkeit gegeben, zu den protokollierten Kontrollergebnissen Stellung zu nehmen. Wird dadurch der Verdacht einer missbräuchlichen oder unerlaubten Nutzung entkräftet, so endet das Überprüfungsverfahren. Ansonsten ist das Kontrollprotokoll über die jeweiligen Vorgesetzten der für das Personal verantwortlichen Stelle zuzuleiten. Lässt die Auswertung des Kontrollprotokolls offensichtlich erkennen, dass Straftaten begangen worden sind, wird das Protokoll der für das Personal verantwortlichen Stelle direkt übermittelt. In jedem Fall ist die Personalvertretung über den Ausgang der Auswertung zu unterrichten.

4.4 Verstöße gegen diese Richtlinie können neben dem Entzug der privaten Nutzungsrechte disziplinar- oder arbeits- sowie strafrechtliche Folgen haben.

5 **Schlussbestimmungen**

5.1. Mit dieser Richtlinie treten bestehende Regelungen im Geltungsbereich der Richtlinie außer Kraft.

5.2. Die Richtlinie tritt am Tag der Veröffentlichung in Kraft. Soweit die zur Umsetzung der Richtlinie erforderlichen organisatorischen bzw. technischen Voraussetzungen nicht gegeben sind, sind diese bis spätestens sechs Monate nach Inkrafttreten der Richtlinie zu schaffen.

Wiesbaden, 30. Januar 2012

Hessisches Ministerium
des Innern und für Sport
Z 11
– Gült.-Verz. 30 –

StAnz. 19/2012 S. 526

Anlage 1 zur Richtlinie zur Nutzung von E-Mail- und Internetdiensten in der Hessischen Landesverwaltung

Kenntnisnahme- und Einwilligungserklärung

Die Richtline zur Nutzung von E-Mail und Internet in der Hessischen Landesverwaltung habe ich zur Kenntnis genommen und werde die dort gemachten Vorgaben beachten.

_____ _____

Ort, Datum Unterschrift

Ich möchte die von meiner Dienststelle zur Verfügung gestellten Internet- und E-Mail-Dienste in geringfügigem Umfang auch für private Zwecke nutzen.

Ich willige ein, dass mein privater E-Mail- und Internetverkehr in demselben Maße wie mein dienstlicher E-Mail- und Internetverkehr automatisch protokolliert wird. Ich bin damit einverstanden, dass diese Protokolldaten wie in der Richtlinie unter Punkt 4 beschrieben temporär gespeichert werden und stichprobenartig überprüft werden können. Bei einem konkreten Verdacht einer missbräuchlichen Nutzung können alle vorhandenen Protokolle zur personenbezogenen Auswertung verwendet werden und die Anonymität kann auch im Falle der Internetnutzung aufgehoben werden.

Ich gestatte ferner, dass meine privaten E-Mails bei möglicher Verseuchung mit Viren oder anderen Schadprogrammen sowie an mich adressierte unerwünschte oder unverlangt zugehende E-Mails – sog. Spam-Mails – automatisiert herausgefiltert und ggf. nicht zugestellt werden. Mir ist bekannt, dass dabei auch privat erwünschte E-Mails irrtümlich durch den Spamfilter ausgesondert werden können.

Sollten im Fall meiner Abwesenheit vom Arbeitsplatz an mich adressierte E-Mails an meine Vertretung weitergeleitet werden oder sie Zugriff auf mein Postfach nehmen, so billige ich das. Meine Vorgesetzte oder mein Vorgesetzter organisiert insbesondere für den Fall der ungeplanten Abwesenheit einen Zugriff auf mein E-Mail-Konto, wenn dies für einen ordnungsgemäßen betrieblichen Ablauf nötig sein sollte. Mir ist bewusst, dass dabei auch private E-Mails anderen Personen zur Kenntnis gelangen können.

Mir ist bekannt, dass die Gestattung der Privatnutzung jederzeit eingeschränkt oder widerrufen werden kann. Auch ich kann diese Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen. Ab dem Zeitpunkt des Widerrufs darf ich den Internetzugang und den E-Mail-Dienst dann nicht mehr für private Zwecke nutzen.

Diese Erklärung ersetzt alle bisherigen Einwilligungserklärungen, die zur Nutzung von E-Mail- und/oder Internetdiensten abgegeben worden sind.

Die Einwilligungserklärung wird in meine Personalakte aufgenommen.

_____ _____

Ort, Datum Unterschrift

Anlage 2 zur Richtlinie zur Nutzung von E-Mail- und Internetdiensten in der Hessischen Landesverwaltung

Kenntnisnahme- und Einwilligungserklärung

Für die inner- und außerbehördlichen Interessenvertretungen, die Frauenbeauftragte, die behördliche Datenschutzbeauftrage oder den behördlichen Datenschutzbeauftragten sowie die Mitglieder der Landesregierung und die Staatssekretärinnen und Staatssekretäre

Die Richtline zur Nutzung von E-Mail und Internet in der Hessischen Landesverwaltung habe ich zur Kenntnis genommen und werde die dort gemachten Vorgaben beachten.

_____ _____

Ort, Datum Unterschrift

Ich möchte die von meiner Dienststelle zur Verfügung gestellten Internet- und E-Mail-Dienste in geringfügigem Umfang auch für private Zwecke nutzen.

I. Für die inner- und außerbehördlichen Interessenvertretungen, die Frauenbeauftragte, die behördliche Datenschutzbeauftragte oder den behördlichen Datenschutzbeauftragten

Ich willige ein, dass mein privater E-Mail- und Internetverkehr in demselben Maße wie mein dienstlicher E-Mail- und Internetverkehr automatisch protokolliert wird. Ich bin damit einverstanden, dass diese Protokolldaten wie in der Richtlinie unter Punkt 4 beschrieben temporär gespeichert und stichprobenartig überprüft werden.

Die Überprüfung unterbleibt bei einem Funktionspostfach, das ich als Mitglied der inner- und außerbehördlichen Interessenvertretung, als Frauenbeauftragte oder als behördliche Datenschutzbeauftragte oder behördlicher Datenschutzbeauftragter verwende.

Bei einem konkreten Verdacht einer missbräuchlichen Nutzung können alle vorhandenen Protokolle zur personenbezogenen Auswertung verwendet werden und die Anonymität kann auch im Falle der Internetnutzung aufgehoben werden.

Ich gestatte ferner, dass meine privaten E-Mails bei möglicher Verseuchung mit Viren oder anderen Schadprogrammen sowie an mich adressierte unerwünschte oder unverlangt zugehende E-Mails – sog. Spam-Mails – automatisiert herausgefiltert und ggf. nicht zugestellt werden. Mir ist bekannt, dass dabei auch privat erwünschte E-Mails irrtümlich durch den Spamfilter ausgesondert werden können.

Sollten im Fall meiner Abwesenheit vom Arbeitsplatz an mich adressierte E-Mails an meine Vertretung weitergeleitet werden oder sie Zugriff auf mein persönliches Postfach nehmen, so billige ich das. Meine Vorgesetzte oder mein Vorgesetzter organisiert insbesondere für den Fall der ungeplanten Abwesenheit einen Zugriff auf mein persönliches E-Mail-Konto, wenn dies für einen ordnungsgemäßen betrieblichen Ablauf nötig sein sollte. Mir ist bewusst, dass dabei auch private E-Mails anderen Personen zur Kenntnis gelangen können.

Der Zugriff meiner Vorgesetzten oder meines Vorgesetzten ist für ein Funktionspostfach, das ich als Mitglied der inner- und außerbehördlichen Interessenvertretung, als Frauenbeauftragte oder als behördliche Datenschutzbeauftragte oder behördlicher Datenschutzbeauftragter verwende, untersagt.

Mir ist bekannt, dass die Gestattung der Privatnutzung jederzeit eingeschränkt oder widerrufen werden kann. Auch ich kann diese Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen. Ab dem Zeitpunkt des Widerrufs darf ich den Internetzugang und den E-Mail-Dienst dann nicht mehr für private Zwecke nutzen.

Diese Erklärung ersetzt alle bisherigen Einwilligungserklärungen, die zur Nutzung von E-Mail- und/oder Internetdiensten abgegeben worden sind.

Die Einwilligungserklärung wird in meine Personalakte aufgenommen.

_____ _____

Ort, Datum Unterschrift

II. Für die Mitglieder der Landesregierung sowie die Staatssekretärinnen und Staatssekretäre

Ich willige ein, dass mein privater E-Mail- und Internetverkehr in demselben Maße wie mein dienstlicher E-Mail- und Internetverkehr automatisch protokolliert wird. Ich bin damit einverstanden, dass diese Protokolldaten wie in der Richtlinie unter Punkt 4 beschrieben temporär gespeichert werden. Die Internetnutzung kann stichprobenartig überprüft werden.

Bei einem konkreten Verdacht einer missbräuchlichen Nutzung können alle vorhandenen Protokolle zur personenbezogenen Auswertung verwendet werden und die Anonymität kann auch im Falle der Internetnutzung aufgehoben werden.

Ich gestatte ferner, dass meine privaten E-Mails bei möglicher Verseuchung mit Viren oder anderen Schadprogrammen sowie an mich adressierte unerwünschte oder unverlangt zugehende E-Mails – sog. Spam-Mails – automatisiert herausgefiltert und ggf. nicht zugestellt werden. Mir ist bekannt, dass dabei auch privat erwünschte E-Mails irrtümlich durch den Spamfilter ausgesondert werden können.

Mir ist bekannt, dass die Gestattung der Privatnutzung jederzeit eingeschränkt oder widerrufen werden kann. Auch ich kann diese Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen. Ab dem Zeitpunkt des Widerrufs darf ich den Internetzugang und den E-Mail-Dienst dann nicht mehr für private Zwecke nutzen.

Diese Erklärung ersetzt alle bisherigen Einwilligungserklärungen, die zur Nutzung von E-Mail- und/oder Internetdiensten abgegeben worden sind.

Die Einwilligungserklärung wird in meine Personalakte aufgenommen.

_____ _____

Ort, Datum Unterschrift

392

Sachschadensersatz-Richtlinien (SErs-RL)

Bezug: Meine Rundschreiben vom 31. Juli 2006 (StAnz. S. 1914) und 26. Oktober 2006 (StAnz. S. 2623)

Aufgrund des § 233 des Hessischen Beamtengesetzes (HBG) werden zur Konkretisierung der Fürsorgepflicht nach § 45 des Beamtenstatusgesetzes folgende Richtlinien als Rechtsgrundlage für die Erstattung von Sachschäden außerhalb der Unfallfürsorge nach dem Hessischen Beamtenversorgungsgesetz erlassen.

Ist neben dem Sachschaden gleichzeitig ein Körperschaden (Dienstunfall) entstanden, so richtet sich die Erstattung des Sachschadens nach § 32 des Hessischen Beamtenversorgungsgesetzes (HBeamtVG) und der hierzu ergangenen Verwaltungsvorschrift in der jeweils gültigen Fassung.

1. **Definition und Anwendungsbereich**

   Sind bei einem auf äußerer Einwirkung beruhenden plötzlichen, örtlich und zeitlich bestimmbaren Ereignis, das in Ausübung oder infolge des Dienstes eingetreten ist, Kleidungsstücke oder sonstige Gegenstände beschädigt oder zerstört worden oder abhanden gekommen, so soll dafür in angemessenem Umfang Ersatz geleistet werden.

   Sind durch die erste Hilfeleistung nach dem Unfall besondere Kosten entstanden, so ist der Beamtin oder dem Beamten der nachweisbar notwendige Aufwand zu ersetzen. § 31 Abs. 1 Satz 2 und Abs. 2 bis 4 HBeamtVG gilt entsprechend.

1.1 Die SErs-RL finden auch Anwendung, wenn eine Beamtin oder ein Beamter anlässlich der Wahrnehmung von Rechten oder der Erfüllung von Pflichten nach dem Personalvertretungsrecht einen Sachschaden erleidet. Gleiches gilt für die Vertrauensleute der schwerbehinderten Menschen.

1.2 Im Einvernehmen mit dem Hessischen Ministerium der Finanzen bin ich einverstanden, dass die SErs-RL sinngemäß auch auf die Arbeitnehmerinnen und Arbeitnehmer, Praktikantinnen und Praktikanten sowie Auszubildenden des Landes anzuwenden sind.

2. **Ersatzpflicht**

   Ersatz wird geleistet für beschädigte oder zerstörte oder abhanden gekommene Gegenstände des täglichen Bedarfs (Kleidungsstücke, sonstige Gegenstände und Fahrzeuge), die dienstlich benötigt oder gewöhnlich mitgeführt werden, und sich im Besitz der Beamtin oder des Beamten befinden. Es ist unerheblich, ob die Gegenstände Eigentum der Beamtin oder des Beamten sind.

   Ersatz ist auch zu leisten, wenn der Beamtin oder dem Beamten selbst nur deshalb kein Schaden entstanden ist, weil die Haftungsfreistellung unter Ehegatten nach § 1359 Bürgerliches Gesetzbuch (BGB) oder zwischen Eltern und Kindern nach § 1664 BGB greift.

2.1 Ersatz ist nur zu leisten, soweit die Beamtin oder der Beamte den Schaden nicht auf andere Weise, zum Beispiel durch den Schadensersatzanspruch gegen Dritte oder durch die eigene Versicherung ersetzt erhalten kann. Der Ersatzanspruch gegen Dritte ist vorrangig geltend zu machen.