

Die weiterhin gültigen Arbeitshinweise und Anlagen der GA PPr Stab Nr. 1/2005 sind im IntraPol auf der Startseite der Zentralen Vorschriftenstelle unter dem Stichwort "Arbeitshinweise" zu finden.

Veröffentlichung im IntraPol

Geschäftsanweisung ZSE III Nr.1 / 2016

zur Nutzung von

Informations- und Kommunikationstechnik

in der Polizei Berlin

Diese Geschäftsanweisung gilt für die gesamte Polizeibehörde.

Inhaltsverzeichnis

1	Regelungsinhalt	3
2	Grundsätze	3
3	Folgen bei Verstößen.....	3
4	IuK-Arbeitsplätze.....	4
4.1	Multifunktionaler Arbeitsplatz (MAP)	4
4.2	IuK Endgeräte außerhalb des MAP	4
4.3	Mobile Geräte/ MDM.....	4
5	Regelungen zu den Identifikationsmitteln	4
6	Schutz vor Schadprogrammen.....	5
7	Fernwartung und –administration.....	5
9	Datenablage – Speicherplatz – Löschung von Daten	5
10	Verschlüsselung der Datenübertragung (Kryptographie)/Signatur.....	6
11	Umgang mit Verschlusssachen.....	6
11.1	Im polizeilichen Datennetz (MAP)	6
11.2	In anderen Datennetzen	6
12	Informationssicherheit.....	6
13	Protokollierung und Überwachung des Datenverkehrs.....	6
14	Schlussbestimmungen.....	7

1 Regelungsinhalt

Diese Geschäftsanweisung (GA) beschreibt und regelt die Rahmenbedingungen des dienstlichen Einsatzes von Informations- und Kommunikationstechnik (IuK) in der Polizei Berlin.

2 Grundsätze

- (1) Die Nutzung von polizeilichen Datennetzen ist grundsätzlich nur zu dienstlichen Zwecken und ausschließlich mit dienstlich zur Verfügung gestellten Geräten zulässig. Als dienstlich ist jeder Zweck anzusehen, der unter Berücksichtigung des Inhaltes und des Adressatenkreises mit der dienstlichen Tätigkeit im Zusammenhang steht.
- (2) Alle Anwenderinnen und Anwender mit MAP-Netzanbindung verfügen grundsätzlich über einen Intranet-/Internetzugang und einen persönlichen E-Mail Account. Die private Nutzung des dienstlich zur Verfügung gestellten E-Mail Accounts ist untersagt.
- (3) Jede Nutzung des polizeilichen Datennetzes und des Internets, die gegen geltendes Recht verstößt oder den Interessen der Polizei Berlin oder deren Ansehen in der Öffentlichkeit schaden könnte, ist unzulässig. Die private Nutzung des Internets ist grundsätzlich untersagt.¹
- (4) Bei der Beschaffung, Weiterverarbeitung und Weitergabe der zugänglichen Informationen sind Urheber- und Lizenzrechte zu beachten.
- (5) Die Nutzung privater IT-Geräte (ausgenommen sind Fälle der Telefonie²) für dienstliche Zwecke ist untersagt. Die Nutzung dienstlicher IT-Geräte (dienstlich sind alle Geräte, die die Polizei beschafft) für private Zwecke ist untersagt.
- (6) Ein Zutritt bzw. Zugang zu bestimmten (sicherheitsrelevanten) IT-Bereichen/IT-Systemen (z. B. Rechenzentrum) bzw. der Zugriff auf dienstliche Daten ist ausschließlich den hierzu Befugten zu ermöglichen.

3 Folgen bei Verstößen

- (1) Verstöße gegen diese Geschäftsanweisung können arbeits-, disziplinar- und/oder strafrechtliche Konsequenzen haben.

¹ Link: [Dienstvereinbarung Internet SenInn Sport - HPR](#)

² Link: [SenInn III A 22 v. 4.11.1997 Erlass über Einrichtung und Benutzung von Telekommunikations-einrichtungen für Polizei und Feuerwehr: Nr. 6.6](#)

(2) Bei begründeten Verdachtsmomenten auf Verstöße können Zugriffsrechte entzogen bzw. Accounts zur Beweissicherung gesperrt und ausgewertet werden. Die Datenschutzbeauftragte / der Datenschutzbeauftragte ist zu beteiligen.

4 luK-Arbeitsplätze

luK-Arbeitsplätze können sowohl stationär als auch ortsunabhängig mit mobilen Endgeräten eingerichtet werden

4.1 Multifunktionaler Arbeitsplatz (MAP)

Das MAP-Konzept sieht vor, dass jede Dienstkraft der Polizei Berlin von jedem Gerät, welches in das MAP-Netz integriert ist, auf Daten zugreifen kann. Unterstützt wird dies durch die Möglichkeit, per E-Mail zu kommunizieren. Dabei ist der MAP so konzipiert, dass auf sichere Art und Weise auf Daten und Anwendungen in einer vernetzten Umgebung zugegriffen werden kann.

4.2 luK Endgeräte außerhalb des MAP

Bei anderen Netzen oder luK-Endgeräten trifft die Infrastruktur-/Verfahrensverantwortliche / der Infrastruktur-/Verfahrensverantwortliche in Abstimmung mit der zuständigen luK-Koordinierungsstelle (luK-KooSt) die Entscheidung über die Freigabe von Diensten.

4.3 Mobile Geräte/ MDM

(1) Der Einsatz mobiler dienstlicher Endgeräte mit und ohne Zugriff auf das polizeiliche Datennetz birgt besondere Gefahren (z.B. Verlust, unberechtigter Zugriff, etc.) und unterliegt deshalb aus Gründen der IT-Sicherheit besonderen Restriktionen.

(2) Der Einsatz von mobilen dienstlichen Endgeräten wird, anlehnend an die Dienstvereinbarung³ zwischen der Senatsverwaltung für Inneres und Sport und dem Hauptpersonalrat der Berliner Verwaltung, gesondert geregelt.

5 Regelungen zu den Identifikationsmitteln

Die Nutzung der luK-Endgeräte hat mit den zugewiesenen Zugangsdaten zu erfolgen.

³ Link: [Rahmendienstvereinbarung mobile Endgeräte SenInn Sport - HPR](#)

6 Schutz vor Schadprogrammen

Ein aktueller Virenschutz ist einzurichten.

7 Fernwartung und –administration

Alle IuK-Endgeräte können von Administratoren aus der Ferne gewartet und administriert werden.

8 Ausgelagerte Netze und Domänen

Neben der Domäne MAP dürfen ausgelagerte Netze und Domänen nur in besonders begründeten Einzelfällen, unter Zustimmung von ZSE III, eingerichtet werden.

9 Datenablage – Speicherplatz – Löschung von Daten

(1) Für einen wirtschaftlichen Umgang mit Speicherplatz legen die Organisationseinheiten, in Absprache mit der Abteilung IuK, Regelungen zur Dateiablage, -archivierung und zur Verhinderung der Ablage von doppelten Dateien fest. In Folge dessen werden die Dateiablagen (Fileserver) regelmäßig auf das Vorhandensein großer sowie doppelter Dateien gescannt. Diese können, nach Ankündigung beim Dateibesitzer, durch Administratoren gelöscht werden.

(2) Im dienstlichen Zusammenhang erstellte Daten sind dienstliche Daten, die daher nicht im Ordner „Eigene Dateien“ abgelegt werden dürfen.

(3) Der Ordner „Eigene Dateien“ besitzt eine Möglichkeit zur individuellen Dateiablage⁴ jeden Nutzers bis zum Erreichen der Speichergrenze.

(4) Ausschließlich auf Servern gespeicherte Daten werden automatisiert gesichert. Das Speichern auf lokalen Festplatten sollte deshalb vermieden werden.

⁴ z . B. Urlaubs-/Beihilfeanträge, Fortbildungstermine

10 Verschlüsselung der Datenübertragung (Kryptographie)/ Signatur⁵

Das Verschlüsseln von E-Mails ist immer dann geboten, wenn personenbezogene Daten enthalten sind und/oder eine VS-NfD-Einstufung des Inhalts vorliegt und die Empfängeranschrift der E-Mail außerhalb der Polizeien des Bundes und der Länder liegt oder keine individuelle Leitungsver Schlüsselung⁶ eingerichtet ist.

11 Umgang mit Verschlusssachen

Bei der Beurteilung, ob schutzbedürftige Daten zur Übertragung vorliegen, ist ein strenger Maßstab anzulegen.

11.1 Im polizeilichen Datennetz (MAP)

Die Verarbeitung, der Versand und die Speicherung von als Verschlusssachen (VS) eingestuften Dateien ist nur bis zum Geheimhaltungsgrad „VS - Nur für den Dienstgebrauch“ zulässig.

11.2 In anderen Datennetzen

Die Verschlusssachenanweisung (VSA) und die Informationssicherheitsleitlinie sind zu beachten und bleiben von dieser Geschäftsanweisung unberührt.

12 Informationssicherheit

Die Regelungen⁷ zur Informationssicherheit in der Polizei Berlin gelten in der jeweils gültigen Fassung entsprechend.

13 Protokollierung und Überwachung des Datenverkehrs

(1) Grundsätzlich unterliegt jeder Datenverkehr einer automatischen Protokollierung.

(2) Für die Nutzung des Internets gelten die Regelungen der Dienstvereinbarung Internet⁸ zwischen der Senatsverwaltung für Inneres und Sport und dem Hauptpersonalrat der Berliner Verwaltung. Danach dürfen personenbezogene Protokollierungen nur nach Maßgabe der §§ 3 bis 5 der Internet DV gespeichert und genutzt werden.

⁵ Rundschreiben SenInnSport ZS Nr. 7/2014 Allgemeine Zugangseröffnung der Berliner Verwaltung für elektronische Dokumente zum 1. Juli 2014

⁶ Link: [Tabelle Leitungsver Schlüsselung](#)

⁷ Link: Intrapol [Regelungen der Informationssicherheit](#)

⁸ Link: [Dienstvereinbarung Internet](#)

Eine automatische verdachtsunabhängige personenbezogene Protokollierung ist ausgeschlossen, es sei denn, dass Tatsachen bekannt werden, die den Verdacht einer Dienst- bzw. Arbeitspflichtverletzung rechtfertigen.

(3) Die Nutzung der Protokolldaten unterliegt der engen Zweckbindung des § 11 Abs. 5 Berliner Datenschutzgesetz. Eine Verwendung zur Leistungskontrolle ist unzulässig.

14 Schlussbestimmungen

(1) Diese Geschäftsanweisung tritt am 19. August 2016 in Kraft. Sie tritt am 18. August 2021 außer Kraft und ist allen Dienstkräften jährlich gegen Unterschriftsleistung bekannt zu geben.

(2) Die Geschäftsanweisung PPr Stab Nr. 1/2005 zur Nutzung von Informationstechnik im Rahmen des multifunktionalen Arbeitsplatzes (MAP) der Polizei Berlin (IT-Einsatz im MAP) tritt mit sofortiger Wirkung außer Kraft. Sie ist aus den Sammlungen zu entfernen und zu vernichten.

Kandt