Dienstanweisung zum Datenschutz und zur Informationssicherheit beim Einsatz von IT-Geräten bei Justizbehörden des Landes Nordrhein-Westfalen - DA DI -

RV d. JM vom 27. Oktober 2022 (1510-IT.103/ Überarbeitung DA DS)

Zum Schutz der Unversehrtheit, Vertraulichkeit und Verfügbarkeit von Informationen im Allgemeinen sowie zur Gewährleistung eines angemessenen Schutzes personenbezogener Daten im Besonderen wird Folgendes bestimmt:

Abschnitt 1
(Geltungsbereich, Grundsätze, allgemeine Pflichten)

§ 1 Geltungsbereich und Begriffsbestimmungen

(1)
Diese Dienstanweisung gilt für den Umgang mit Informationen einschließlich personenbezogener Daten im Geschäftsbereich des Ministeriums der Justiz, insbesondere für die automatisierte Verarbeitung durch Geräte der Informationstechnik (IT-Geräte). Für die Benutzung privater IT-Geräte gilt diese Dienstanweisung nur, soweit dies ausdrücklich vorgeschrieben ist. Für bestimmte Geschäftsbereiche oder IT-Verfahren können ergänzende landes- oder bezirksweite Regelungen erlassen werden. Diese Dienstanweisung findet keine Anwendung auf Schiedspersonen im Sinne des Gesetzes über das Schiedsamt in den Gemeinden des Landes Nordrhein-Westfalen, für die gesonderte Regelungen gelten.

(2)
IT-Geräte im Sinne dieser Dienstanweisung sind elektronische Geräte zur (teil-)automatisierten Erfassung, Darstellung, Speicherung, Verarbeitung, Übermittlung und Löschung von Informationen, insbesondere PCs, mobile Geräte (Notebooks, Convertibles, Tablets, Smartphones o. ä.) und Speichermedien.

(3)
Personenbezogene Daten sind solche im Sinne des Art. 4 Nr. 1 DSGVO.

(4)
Vertrauliche Informationen im Sinne dieser Dienstanweisung sind solche, bei denen durch eine unbefugte Kenntnisnahme Schutzgüter Dritter oder die Aufgabenerfüllung der Justizbehörden oder sonstiger öffentlicher Stellen beeinträchtigt oder gefährdet würden.

§ 2 Grundsätze

(1)

Im Rahmen des Umgangs mit Informationen ergeben sich (etwa durch unberechtigte Zugriffe auf Informationen oder die Vornahme von Änderungen durch Unbefugte) vielfältige Bedrohungen für die gesetzeskonforme Erfüllung der Aufgaben der Justiz, durch die es zu weitreichenden Beeinträchtigungen für die jeweiligen Beteiligten kommen kann.

Die Gewährleistung der Informationssicherheit mit ihren wesentlichen Schutzzielen der Vertraulichkeit, Integrität und Verfügbarkeit sowie die Gewährleistung eines angemessenen, gesetzeskonformen Datenschutzniveaus sind wesentliche Teile der dienstlichen Aufgabenerfüllung.

(2)
Mitarbeiterinnen und Mitarbeiter sind verpflichtet, die Vertraulichkeit, die Integrität und die Verfügbarkeit von Informationen zu schützen. In Erfüllung dieser Pflicht haben sie im Rahmen ihrer Aufgabenerfüllung in eigener Verantwortung die Einhaltung der Vorschriften über den Datenschutz und die Informationssicherheit unter Berücksichtigung der justizspezifischen Vorschriften (z. B. Prozessordnungen, Verwaltungsverfahrensgesetz, Strafvollzugsgesetz) sowie dieser Dienstanweisung sicherzustellen. Verstöße sind nach Maßgabe örtlicher Vorgaben der Behördenleitung mitzuteilen.

§ 3 Schutz vor unbefugtem Zugriff und unbefugter Änderung

(1)
Mitarbeiterinnen und Mitarbeiter haben dafür Sorge zu tragen, dass dienstliche Informationen Unbefugten gegenüber nicht bekannt werden.

(2)
Mitarbeiterinnen und Mitarbeiter sind verpflichtet, in den ihnen zugewiesenen Diensträumen bei Verlassen Fenster und Türen zu verschließen, sofern nicht ein unbefugter Zutritt im Einzelfall ausgeschlossen ist oder im Einzelfall zwingende dienstliche Gründe entgegenstehen.

(3)
Bei der Benutzung eines IT-Geräts ist der Gefahr einer unbefugten Einsichtnahme durch Dritte durch angemessene Schutzvorkehrungen vorzubeugen.

(4)
Mitarbeiterinnen und Mitarbeiter sind verpflichtet, folgende Maßnahmen zum Schutz vor unbefugtem Zugang zu Informationen auf IT-Systemen zu ergreifen:

a)
Bei der Verwendung von Passwörtern in dienstlichem Zusammenhang ist Folgendes zu beachten:

aa)
- Benutzerkonten sollen durchgängig mit einer Mehr-Faktor-Authentisierung geschützt werden. Passwörter müssen dabei mindestens 8 Zeichen lang sein und drei Zeichenarten enthalten oder 10 Zeichen lang sein und zwei Zeichenarten enthalten.

- Ist eine Mehr-Faktor-Authentisierung nicht möglich, müssen Passwörter wahlweise
* mindestens 8 Zeichen Länge und vier genutzte Zeichenarten (komplexer, geringere Länge des Passworts),
* mindestens 10 Zeichen Länge und drei genutzte Zeichenarten (komplexer, geringere Länge des Passworts) oder
* mindestens 20 Zeichen Länge und zwei genutzte Zeichenarten (weniger komplex, längeres Passwort beziehungsweise Passphrase) enthalten.

Lässt das System nur kürzere Passwörter zu, ist die maximale Stellenanzahl auszunutzen.

- Passwörter dürfen nur geschützt (schriftlich oder digital) abgelegt werden. Bei der schriftlichen Hinterlegung muss das Passwort mindestens in einem fest verschlossenen Umschlag sicher abgelegt werden. Das Passwort darf nicht auf programmierbaren Funktionstasten abgespeichert werden. Es sollen nur behördlich freigegebene Softwareprodukte zur eigenen Passwortverwaltung eingesetzt werden. Die Speicherung von Passwörtern in einem Webbrowser ist nicht zulässig.

- Bei der Änderung des Passwortes darf das neue Passwort nicht identisch mit den im System gespeicherten letzten zehn zuvor verwendeten sein.

- Für jedes IT-System bzw. jede Anwendung muss ein eigenständiges Passwort verwendet werden (keine Mehrfachverwendung).

- Die Verwendung von Passwort-Generationen ist nicht erlaubt (z. B. Winter+001, Winter+002, Winter+003, etc.).
- Passwörter dürfen nicht leicht zu erraten sein. Informationen aus dem persönlichen oder dienstlichen Umfeld und somit offensichtlichen Inhalten dürfen nicht verwendet werden, bspw. "Support+123", "Personal+007".
- Passwörter müssen geheim gehalten werden und dürfen Dritten nicht zugänglich gemacht werden. Das Passwort muss bei Verdacht der Kompromittierung umgehend geändert werden.

- Die Eingabe des Passwortes hat stets unbeobachtet zu erfolgen.

- Passwörter, welche privat genutzt werden, dürfen nicht innerhalb der Institution für dienstliche Zwecke benutzt werden.

- Passwörter dürfen vorbehaltlich etwaiger bundes- und landesrechtlicher Verpflichtungen nicht weitergegeben werden. Stattdessen ist beispielsweise die Nutzung einer technischen Vertretungsfunktion zu verwenden.

- Bei personenbezogenen Zugängen darf nur die hiermit verknüpfte Person diesen Zugang nutzen oder muss diese Nutzung persönlich überwachen.

bb)
- Administrative Konten zur Bedienung von Servern, Anwendungen und sonstigen IT-Systemen sollen durchgängig mit einer Mehr-Faktor-Authentisierung geschützt werden. Passwörter müssen dabei mindestens 10 Zeichen lang sein und drei Zeichenarten enthalten oder 12 Zeichen lang sein und zwei Zeichenarten enthalten.

- Ist eine Mehr-Faktor-Authentisierung nicht möglich, müssen Passwörter für administrative Konten wahlweise
* mindestens 12 Zeichen Länge und vier genutzte Zeichenarten (komplexer, geringere Länge des Passworts),
* mindestens 14 Zeichen Länge und drei genutzte Zeichenarten (komplexer, geringere Länge des Passworts) oder
* mindestens 25 Zeichen Länge und zwei genutzte Zeichenarten (weniger komplex, längeres Passwort beziehungsweise Passphrase) enthalten.

- Voreingestellte Administrationspasswörter sind unverzüglich nach den vorgegebenen Regelungen zu ändern.

cc)
- Für Systempasswörter von System-, Maschinen- oder ähnlich genutzten Konten zur Kommunikation der Systeme untereinander bzw. automatisierten Systemabfragen u. a. (Systempasswörter) sind sog. "verwaltete Dienstkonten" zu verwenden, die automatisiert einen Wechsel durchführen. Bei fehlender automatischer Änderung muss ein manueller Prozess etabliert werden.

- Systempasswörter im vorgenannten Sinne müssen mindestens 20 Zeichen Länge und vier genutzte Zeichenarten enthalten.

- Das Systempasswort muss nur bei Vorliegen eines Grundes (z.B. Wechsel der Administratoren, Verdacht der Kompromittierung) geändert werden.

- Voreingestellte Standard-Systempasswörter sind unverzüglich nach den vorgegebenen Regelungen zu ändern.

- Soweit technisch möglich, müssen Systempasswörter sicher dokumentiert und verwahrt werden. Eine rein digitale Verwahrung ist dabei nur dann zulässig, wenn diese im Notfall (z.B. an einem anderen Standort) verfügbar ist. Eine Notfallvorsorge

ist umzusetzen. Systempasswörter können z.B. in einem fest verschlossenen Umschlag im Safe der Verwaltungsleitung gelagert werden.

Sämtliche in dienstlichem Zusammenhang vergebenen Passwörter sollen - soweit dies dem Anwender/der Anwenderin möglich ist - spätestens nach 180 Tagen geändert werden.

b)
Physische oder ideelle Sicherheitsmerkmale (z. B. Passwörter, Token, Zugangskarten) sollen getrennt von dem jeweiligen IT-Gerät aufbewahrt werden.

c)
Bei Nichtbenutzung sind IT-Geräte vor einem unbefugten Zugriff durch Dritte zu schützen. Dies geschieht in der Regel durch Abmeldung oder durch einfaches passwortgesichertes Sperren des Bildschirms.

d)
Die Weitergabe und der Transport von IT-Geräten (Notebooks, USB-Sticks, etc.), die vertrauliche Informationen oder personenbezogene Daten beinhalten, sind grundsätzlich untersagt, soweit diese nicht zur Erfüllung von Aufgaben der Rechtsprechung oder zu sonstigen dienstlichen Zwecken erforderlich sind und eine Verschlüsselung erfolgt ist. Ein Transport zur Ermöglichung von mobiler Arbeit im Sinne von § 8 Abs. 1 gilt als zu dienstlichen Zwecken erforderlich.

e)
Ausdrucke mit vertraulichen Informationen oder personenbezogenen Daten sind umgehend aus Druckern, Kopierern oder Faxgeräten zu entfernen.

(5)
Zur Ermöglichung von Updates sind IT-Geräte regelmäßig hochzufahren.

Das Herunterladen und die Installation von Software sind grundsätzlich nur dem Zentralen IT-Dienstleister der Justiz des Landes Nordrhein-Westfalen (ITD) gestattet. Im Einzelfall kann die Behördenleitung abweichende Regelungen treffen. Diese müssen dokumentiert werden.

(6)
Mitarbeiterinnen und Mitarbeiter dürfen Sicherheitsmaßnahmen weder deaktivieren noch umgehen oder sonstige technische Veränderungen an den IT-Geräten vornehmen. Nicht als technische Veränderung gelten das Anschließen und Trennen von zulässigen (vgl. § 7 Abs. 6) Peripheriegeräten und der Dockingstation.

§ 4 Schutz vor Verlust und Beeinträchtigung

(1)
Mitarbeiterinnen und Mitarbeiter sind verpflichtet, pfleglich mit IT-Geräten umzugehen. Hierbei sind insbesondere die folgenden Anforderungen einzuhalten:

a)
Ein pfleglicher Umgang mit IT-Geräten ist sicherzustellen, insbesondere sind IT-Geräte vor Schmutz, Flüssigkeiten und Chemikalien zu schützen.

b)
IT-Geräte sind vor Zerstörung oder Beschädigung zu schützen. Hierzu sind insbesondere die behördeninternen Vorgaben des Brandschutzes einzuhalten. Eine Überhitzung, z. B. durch Verdecken der Belüftung eines IT-Geräts oder Einhaltung eines zu geringen Abstands zur Belüftung, ist zu vermeiden.

(2)
IT-Geräte sind außerhalb eines Dienstraums oder des heimischen Arbeitsplatzes zu beaufsichtigen oder durch geeignete Maßnahmen vor einem unbefugten Zugriff zu sichern.

(3)
Zum Schutz vor einem Verlust von digitalen Informationen sind diese grundsätzlich an einem dafür bestimmten Speicherort abzulegen. Um einem größeren Datenverlust während eines Arbeitsvorgangs vorzubeugen, wird empfohlen, regelmäßige Zwischenspeicherungen vorzunehmen. Eine Datenablage im lokalen Speicher des IT-Geräts ist zu vermeiden, soweit dies nicht zu dienstlichen Zwecken übergangsweise erforderlich ist.

§ 5 Datenminimierung

(1)
Die Verarbeitung personenbezogener Daten ist auf das für die Zwecke der Verarbeitung notwendige Maß zu beschränken (Art. 5 DSGVO). Dies umfasst sowohl die Datenmenge, die Dauer der Speicherung als auch die Anzahl der Speicherorte, unabhängig von dem Speichermedium. Im Falle einer notwendigen Verarbeitung von personenbezogenen Daten sind diese zu anonymisieren oder zu pseudonymisieren, sobald dies nach dem Verwendungszweck möglich ist (Art. 25 DSGVO).

(2)
Werden personenbezogene Daten außerhalb eines Fachverfahrens der Justiz oder sonstiger dienstlich bereitgestellter Verfahren verarbeitet, sind Art und Umfang der Verarbeitung der Behördenleitung anzuzeigen.

(3)

Die Speicherung von personenbezogenen Daten außerhalb der dafür bestimmten Speicherorte ist vorbehaltlich der Regelung zur Speicherung dienstlicher Informationen auf privaten IT-Geräten nach § 7 Abs. 2 zu unterlassen.

§ 6 Störungen im IT-Betrieb

(1)
Störungen, Fehler und Änderungen an Hard- und Software sind durch die Mitarbeiterinnen und Mitarbeiter an das Beratungstelefon Informationstechnik (BIT) des ITD zu melden. Die Fehler- und Störungsbehebung darf grundsätzlich nur durch die zuständigen IT-Mitarbeiterinnen und IT-Mitarbeiter erfolgen. Lediglich bei Störungen, deren Ursache offenkundig und ohne Schwierigkeiten selbst zu beseitigen ist, darf die Nutzerin bzw. der Nutzer selbst tätig werden und entfällt eine Meldepflicht. Die Pflichten nach § 13 bleiben hiervon unberührt.

(2)
Bei der Nutzung von E-Mail und Internet ist bei unbekannten Anlagen oder Links vor dem Öffnen auf offensichtliche Hinweise auf Kompromittierung zu achten. Bestehen konkrete Anhaltspunkte, dass eine E-Mail kompromittierte Links oder Anhänge enthält, dürfen die Links oder Anhänge nur geöffnet und die E-Mail selber nur dann weitergeleitet oder verschoben werden, wenn durch Nachfrage bei der Absenderin oder beim Absender oder durch Vermittlung des BIT seitens der IT-Betreuung geklärt werden konnte, ob eine Gefährdung vorliegt. Muss eine möglicherweise kompromittierte E-Mail oder ein entsprechender Link aus zwingenden dienstlichen Gründen geöffnet werden, muss dies in einer gesicherten Betriebsumgebung (z.B. Datenschleuse) erfolgen. Bei konkreten Anhaltspunkten auf Gefährdung eines IT-Geräts durch Virenbefall haben sich die Mitarbeiterinnen und Mitarbeiter von der aktuellen Citrix-Sitzung - sofern möglich - als erstes ordnungsgemäß abzumelden und sodann das Gerät auszuschalten. Tritt der Verdacht eines Virenbefalls außerhalb einer Citrix-Sitzung auf, ist das Gerät sofort auszuschalten. In jedem Fall ist das BIT unverzüglich zu unterrichten.

(3)
Der Verlust von dienstlichen IT-Geräten ist der Behördenleitung unverzüglich anzuzeigen. Sind hiervon vertrauliche Informationen oder personenbezogene Daten betroffen oder kann dies nicht ausgeschlossen werden, ist hierauf ausdrücklich hinzuweisen.

(4)
Defekte oder nicht mehr benötigte IT-Geräte (inklusive Speichermedien) dürfen nicht selbst entsorgt werden, sondern sind der ausgebenden Stelle zurückzugeben.

Abschnitt 2

(Ergänzende Regelungen für Spezifische Geräte, Benutzungssituationen und Kommunikationskanäle)

§ 7 Einsatz privater IT-Geräte

(1)
Der Einsatz privater IT-Geräte zur Verarbeitung vertraulicher dienstlicher Informationen ist vorbehaltlich nachfolgender Ausnahmen untersagt.

(2)
Der Einsatz privater IT-Geräte ist Richterinnen und Richtern sowie Staatsanwältinnen und Staatsanwälten ausnahmsweise im Rahmen der Erledigung von Aufgaben der Rechtspflege zur Verarbeitung dienstlicher personenbezogener Daten in ihrem privaten Bereich unter Beachtung der nachfolgenden Bestimmungen gestattet. Dies gilt nicht, soweit ihnen ein zu diesem Zweck geeignetes dienstliches IT-Gerät auch für die Nutzung in privater Umgebung zur Verfügung gestellt wird und dieses im Einzelfall hinreichend störungsfrei verwendet werden kann.

(3)
Bei dem Einsatz privater IT-Geräte ist zu beachten:

a)
Es dürfen nur personenbezogene Daten aus laufenden Verfahren, mit denen sie dienstlich befasst sind, verarbeitet werden.

b)
Auf einem privaten IT-Gerät gespeicherte Informationen sind umgehend revisionssicher zu löschen, soweit eine weitere Speicherung dort nicht mehr erforderlich ist, spätestens jedoch bei Abschluss des Verfahrens.
Sollen Texte als Vorlage oder Bausteine weiterverwendet werden, so ist deren weitere Speicherung zulässig, sofern sie anonymisiert sind.

c)
Die für dienstliche Zwecke verwendeten vertraulichen Informationen und personenbezogenen Daten sind vor dem Zugriff Dritter auch im privaten Bereich zu schützen. Dies gilt insbesondere, wenn das private IT-Gerät durch weitere Personen genutzt wird. In diesem Fall sind geeignete technische Schutzmaßnahmen zu treffen, etwa durch das Anlegen unterschiedlicher passwortgeschützter Benutzerkonten.

(4)
Bei der Konfiguration des privaten IT-Gerätes ist Folgendes zu beachten:

a)

Das private IT-Gerät ist durch ein Passwort oder biometrisch zu schützen. Sofern ein Passwort verwendet wird, ist § 3 Abs. 4 lit. a) zu beachten.

b)
Es sind die aktuellen Versionen von Betriebssystemen und Programmen zu verwenden. Automatische Updates sind zu aktivieren.

c)
Ein geeignetes Virenschutzprogramm soll installiert und aktuell gehalten werden.

d)
Die Einstellungen zum Datenschutz sind so zu wählen, dass die Weitergabe personenbezogener Daten an den Hersteller der eingesetzten Hard- und Software minimiert ist.

e)
Sofern möglich, sind die Daten ausschließlich auf einem dienstlichen Speichermedium (z. B. hardwareverschlüsselter USB-Stick) und nicht auf dem privaten Gerät zu speichern.

(5)
Die Behördenleitung kann auf schriftlichen Antrag und unter der Voraussetzung eines dienstlichen Bedürfnisses auch sonstigen Anwenderinnen und Anwendern den Einsatz eines privaten IT-Gerätes in ihrem privaten Bereich für die Verarbeitung dienstlicher personenbezogener oder dem Dienstgeheimnis unterfallender Daten widerruflich gestatten. Die Absätze zwei und drei gelten entsprechend.

(6)
Für im Rahmen des Gerichtsvollzieherdienstes genutzte IT-Geräte gelten die Vorgaben für private IT-Geräte. Der Einsatz von ausschließlich zu diesem Zweck verwendeten IT-Geräten ist nicht anzeige- oder gestattungspflichtig.

(7)
In Diensträumen dürfen private Drucker und Monitore nicht genutzt werden. Im Übrigen ist die Nutzung privater Peripheriegeräte erlaubt, sofern diese mittels Kabel angeschlossen werden. Einer Anzeige bedarf es nicht.

§ 8 Mobiles Arbeiten

(1)
Mobiles Arbeiten umfasst jegliche dienstliche Tätigkeit, bei der keine Verbindung zum Landesverwaltungsnetz über ein behördliches LAN hergestellt wird (z. B. in Form von Telearbeit, auf Dienstreisen).

(2)
Drahtlose Schnittstellen von IT-Geräten, wie WLAN oder Bluetooth, sollen nur aktiviert werden, solange sie für die Arbeit benötigt werden.

(3)
Eine mobile Verbindung zum Landesverwaltungsnetz ist ausschließlich mittels VPN-Technik herzustellen. Es ist grundsätzlich ein sicherer Netzzugang zu wählen (kabelgebundenes Netz, verschlüsseltes WLAN, Mobilfunk o.ä.).
Ist die Nutzung einer unsicheren Verbindung (öffentliche "Hot-Spots") unumgänglich, ist sicherzustellen, dass keine schützenswerten Informationen lokal auf dem Gerät ungesichert gespeichert sind.
Für die Löschung von gespeicherten Daten gilt § 7 Abs. 2 lit. b) entsprechend.

(4)
Das IT-Gerät ist zur Sicherstellung eines aktuellen Standes der Updates regelmäßig nach näheren Vorgaben der Behördenleitung über das Landesverwaltungsnetz zu verbinden.

§ 9 Aufenthalt im Ausland

(1)
Die Nutzung und Mitnahme von dienstlichen Geräten und Daten ist bei Aufenthalten in Ländern zulässig, in denen nach dem Schengener Abkommen (https://www.auswaertiges-amt.de/de/newsroom/buergerservice-faq-kontakt/faq/17-schengenstaaten/606502) Grenzkontrollen grundsätzlich nicht erfolgen. Solche Reisen sind der Behördenleitung anzuzeigen. Bei regelmäßigem Aufenthalt in den in Satz 1 genannten Ländern, ist eine einmalige Anzeige hierüber ausreichend.

(2)
Bei Reisen in andere Länder sind Nutzung und Mitnahme von dienstlichen Geräten und Daten grundsätzlich nicht erlaubt. Eine Ausnahmegenehmigung kann in Einzelfällen durch die Behördenleitung erteilt werden.

(3)
Die Anzeige nach Absatz 1 und ggf. der Antrag auf Erteilung einer Ausnahmegenehmigung nach Absatz 2 müssen sechs Wochen vor der Reise oder - bei kurzfristigerer Planung - unverzüglich bei der Behördenleitung vorliegen.

(4)
Bei Dienstreisen gilt der Dienstreiseantrag gleichzeitig als Anzeige nach Absatz 1 und ggf. als Antrag auf Erteilung einer Ausnahmegenehmigung nach Absatz 2.

(5)

Ergänzend gelten die Handlungsanweisungen bei Dienstreisen ins Ausland (Anlage 1).

§ 10 Nutzung des Internets und von Kommunikationsdienstleistungen

(1)
Der dienstlich eröffnete Zugang zum Internet darf nur zu dienstlichen oder dienstlich veranlassten Zwecken genutzt werden.

(2)
Der dienstlich eröffnete E-Mail-Zugang darf ausschließlich zu dienstlichen oder dienstlich veranlassten Zwecken genutzt werden.

(3)
Die Nutzung privater E-Mail-Accounts, privater Cloud-Dienste, Messenger-Dienste und Sozialer Medien zum Austausch von vertraulichen Informationen und personenbezogenen Daten zu dienstlichen Zwecken ist untersagt. Dies gilt insbesondere auch für die Umleitung, Weiterleitung oder Speicherung dienstlicher Informationen.

(4)
Sind die elektronisch zu übermittelnden Inhalte im Hinblick auf ihre Vertraulichkeit, Integrität oder Authentizität schutzwürdig (beispielsweise personalaktendatenbezogener Schriftverkehr, Schriftverkehr über niederschwellig sicherheitsrelevante Angelegenheiten unterhalb VS-nfD Einstufung, Zugangsbeschreibungen oder Sicherheitskonzepte einschließlich IT-Anlagen oder IT-Verfahren und deren Passwörter, Schriftverkehr zu laufenden Vergabemaßnahmen) sind gesicherte Übermittlungswege (z.B. gemeinsame Gruppenlaufwerke, EGVP, Verschlüsselung) zu nutzen. Erfolgt die Übersendung in verschlüsselter Form, sind Passwörter auf einem anderen Kommunikationskanal, z. B. telefonisch oder per Post, zu übermitteln. Die Übermittlung von Daten nach Art. 9 DSGVO über Telefax ist grundsätzlich ausgeschlossen. Dies gilt nicht, wenn eine Übermittlung derartiger Daten aus zwingenden dienstlichen Gründen zur Wahrung der Rechte Dritter erforderlich ist und gesicherte Übermittlungswege (gemeinsame Gruppenlaufwerke, EGVP, E-Mail mit Verschlüsselung) nicht verfügbar sind.

(5)
Bei besonders schutzwürdigen Angelegenheiten (beispielsweise Schriftstücke, die besonders vertraulich zu behandeln sind, Disziplinarsachen, Berichte und Erlasse in missbrauchsgefährdet eingestuften Verfahren, Prüfungsaufgaben oder Prüfungsbewertungen im Zusammenhang mit der Ausbildung und Fortbildung) ist eine behördenübergreifende Übermittlung in Justizverwaltungssachen innerhalb des Landes Nordrhein-Westfalen per E-Mail ausschließlich verschlüsselt an die hierfür in der RV des Justizministeriums zum elektronischen Schriftverkehr in

Justizverwaltungssachen (1422 - I. 2) in der jeweils gültigen Fassung bestimmten Poststelle zulässig.

(6)
Der Umgang mit Verschlusssachen richtet sich nach den einschlägigen Vorschriften, insbesondere der Allgemeinen Verwaltungsvorschrift des für Inneres zuständigen Ministeriums des Landes Nordrhein-Westfalen zum materiellen und organisatorischen Schutz von Verschlusssachen (VSA) in der jeweils gültigen Fassung.

(7)
An Empfänger außerhalb der Behörde gerichtete E-Mails sind mit einer Signatur zu versehen, die auf die Datenschutzerklärung der jeweiligen Institution oder aber auf ein spezielles Merkblatt verlinkt ist, mit dem die sich aus der DSGVO ergebenden Hinweispflichten erfüllt werden.
Bei Abwesenheit soll eine automatische Benachrichtigung eingerichtet werden.

(8)
Die Vorschriften zum Schriftverkehr im Übrigen bleiben unberührt.

Abschnitt 3
(Regelungen für die Behördenleitungen)

§ 11 Allgemeine Regelungen

(1)
Die Behördenleitung hat die in der Informationssicherheitsleitlinie der Justiz NRW und ggf. in weiteren für die Behörde verbindlichen Informationssicherheitsleitlinien genannten Sicherheitsziele in ihrem Geschäftsbereich umzusetzen.

(2)
Die Behördenleitung trägt dafür Sorge, dass die Anforderungen dieser Dienstanweisung in ihrem Geschäftsbereich umgesetzt und eingehalten werden. Sofern erforderlich hat sie für die Anforderungen ihres Geschäftsbereichs ergänzende ausführende Bestimmungen (z. B. zur Aufbewahrung von Speichermedien) zu erlassen. Sie hat den/die Informationssicherheitsbeauftragte(n) und den/die Datenschutzbeauftragte(n) in erforderlichem Umfang zu beteiligen.

(3)
Die Behördenleitung kann sich zur Erfüllung ihrer Pflichten aus dieser Dienstanweisung des ITD bedienen, soweit diesem die Verantwortung für den IT-Betrieb übertragen wurde.

§ 12 Informationssicherheitsbeauftragter und Datenschutzbeauftragter

(1)
Die Behördenleitung bestellt für ihren Geschäftsbereich eine(n) behördliche(n) Datenschutzbeauftragte(n) nach den Vorschriften der DSGVO. Eine Bestellung für mehrere Behörden ist zulässig; die Einzelheiten werden einvernehmlich zwischen den jeweiligen Behördenleitungen geregelt, sofern nicht durch die gemeinsame Aufsichtsbehörde Regelungen getroffen worden sind.

(2)
Die Bestellung, die Aufgaben und die Zuständigkeiten einer/eines Informationssicherheitsbeauftragten richten sich nach den Vorgaben der Informationssicherheitsleitlinie der Justiz des Landes NRW.
Bestellt die Behördenleitung keine(n) Informationssicherheitsbeauftragte(n), so richtet sich die Wahrnehmung dieser Aufgabe nach der Leitlinie für Informationssicherheit in der Justiz des Landes NRW in ihrer jeweils gültigen Fassung und nach den hierzu ggf. von den Mittelbehörden für ihren Geschäftsbereich bzw. der Zentralstelle für Informationssicherheit im Justizvollzug getroffenen Regelungen.

(3)
Die/der behördliche Datenschutzbeauftragte und die/der Informationssicherheitsbeauftragte sollen auf der Grundlage ihrer beruflichen Qualifikation, insbesondere ihres Fachwissens auf dem Gebiet des Datenschutzrechts bzw. der Informationssicherheit bestellt werden. Sie dürfen außerhalb des Regelungsbereichs von Abs. 2 Satz 2 nicht zugleich mit der Behördenleitung, der Geschäftsleitung oder der leitenden Verwaltungstätigkeit im IT-Bereich betraut sein. Der/die Datenschutzbeauftrage soll nicht zugleich mit den Aufgaben des/der Informationssicherheitsbeauftragten betraut werden.

(4)
Für die/den behördliche(n) Datenschutzbeauftragte(n) ist eine Vertreterin oder ein Vertreter zu bestimmen. Dies gilt auch für die/den Informationssicherungsbeauftragte(n), soweit eine solche/ein solcher bestellt wird.

§ 13 Sicherheitsvorfälle und Umgang mit Verstößen

(1)
Ein Sicherheitsvorfall ist ein Ereignis, bei dem die Verfügbarkeit, Integrität oder Vertraulichkeit von Informationen bzw. personenbezogenen Daten beeinträchtigt ist. Ein solches Ereignis kann z. B. durch eine Schadsoftware, einen Hackerangriff, einen Einbruch, einen Diebstahl, einen Verlust oder Ausfall von IT-Geräten oder auch menschliches Versagen verursacht werden.

(2)
Die Behördenleitung stellt sicher, dass der/die Informationssicherheitsbeauftrage bzw. die Zentralstelle für Informationssicherheit im Justizvollzug über jeden

Sicherheitsvorfall in Kenntnis gesetzt wird. Sofern ein/eine Informationssicherheitsbeauftrage(r) nicht bestellt wurde, ist die jeweilige Mittelbehörde bzw. die Zentralstelle für Informationssicherheit im Justizvollzug über jeden Sicherheitsvorfall in Kenntnis zu setzen.
Die Meldepflichten bei Sicherheitsvorfällen richten sich im Übrigen nach den einschlägigen organisatorischen Vorgaben, die den jeweiligen Funktionsträgern gesondert bekannt gemacht werden.

(3)
Sind Belange des Datenschutzes betroffen, ist die/der behördliche Datenschutzbeauftragte hinzuziehen (Art. 38, 39 DSGVO).

§ 14 Zutritt

(1)
Die Behördenleitung muss geeignete Vorkehrungen treffen, um Räumlichkeiten ihrem Schutzbedarf entsprechend vor unbefugtem Zutritt zu schützen.

(2)
Der Zugang zu Räumlichkeiten, in denen vertrauliche Informationen oder personenbezogene Daten verarbeitet werden, ist nur soweit erforderlich zu gestatten. Regelmäßig eingesetztes justizfremdes Personal, insbesondere Reinigungspersonal, ist bei Antritt des Dienstes in einer Justizliegenschaft über seine Verschwiegenheitspflicht sowie darüber zu belehren, dass jegliche Manipulation an IT-Geräten, Papierakten und sonstigen dienstlichen Gegenständen sowie deren Mitnahme ebenso wie die gezielte Kenntnisnahme von dienstlichen Informationen untersagt sind. Auf eventuelle straf- und arbeitsrechtliche Konsequenzen ist hinzuweisen. Diese Belehrung ist zu dokumentieren. Anderen justizfremden Personen ist der Zutritt zu den in Satz 1 genannten Räumlichkeiten nur unter Aufsicht einer justizinternen Person zu gestatten. Sofern eine Begleitung organisatorisch nicht sichergestellt werden kann, jedoch die Aufgabenerledigung durch die justizfremde Person nicht aufgeschoben werden kann, ist ausnahmsweise ein unbeaufsichtigter Zugang gestattet, wenn zuvor eine Belehrung im Sinne von Satz 2 stattgefunden hat. In diesem Fall ist zu dokumentieren, in welchem Zeitraum die justizfremde Person sich in welchem Bereich aufgehalten hat.

(3)
Der/dem Datenschutzbeauftragten, der/dem Informationssicherheitsbeauftragten und der IT-Betreuung ist Zutritt zu allen Räumen zu gewähren, in denen IT-Geräte aufgestellt sind, soweit dies im Rahmen ihrer Aufgaben erforderlich ist. Die Regelung des § 65 Abs. 4 des Landespersonalvertretungsgesetzes NRW ist zu beachten.

§ 15 Rechte- und Rollenmanagement

Die Behördenleitung trägt dafür Sorge, dass Mitarbeiterinnen und Mitarbeitern nur über diejenigen Rechte und faktischen Zugangs- oder Zugriffsmöglichkeiten verfügen, die zu ihrer Aufgabenerfüllung erforderlich sind. Zu diesem Zweck regelt, dokumentiert und überwacht sie im Rahmen ihrer Zuständigkeit die Rechte- und Rollenvergabe.

Die Entziehung von Rechten und Zugangs- oder Zugriffsmöglichkeiten, die nicht mehr benötigt werden, ist durch die jeweilige Behördenleitung unverzüglich zu veranlassen und ggf. auf Weisung der Behördenleitung durch den ITD durchzuführen. Stellt eine Mitarbeiterin oder ein Mitarbeiter fest, dass sie/er über Zugriffsrechte verfügt, die sie/er im Rahmen ihrer/seiner dienstlichen Tätigkeit nicht mehr benötigt, teilt sie/er dies unverzüglich der Behördenleitung mit.

Der Dienstantritt und das Ausscheiden von Mitarbeiterinnen oder Mitarbeitern sind durch einen standardisierten Prozess zu regeln und zu dokumentieren.

§ 16 Sensibilisierung

Die Behördenleitung hat dafür zu sorgen, dass die Mitarbeiterinnen und Mitarbeiter durch regelmäßige Maßnahmen für die Anforderungen des Datenschutzes und der Informationssicherheit sensibilisiert werden. Dies gilt insbesondere bei der Ausgabe mobiler Geräte oder anlässlich der Anzeige privater Geräte nach § 7.

§ 17 IT-Geräte

(1)
Die Behördenleitung hat dafür Sorge zu tragen, dass den Mitarbeiterinnen und Mitarbeitern eine sachgerechte Ausstattung mit IT-Geräten für ihre Diensterfüllung zur Verfügung steht. Erforderlichenfalls hat sie den Bedarf der zuständigen Stelle rechtzeitig anzuzeigen. Die Aus- und Rückgabe sind zu dokumentieren. Die Ausgabe von Speichermedien soll nur erfolgen, wenn ein dienstliches Bedürfnis für den Transport von Daten vorliegt. Das Vorhandensein ausgegebener Speichermedien bei dem/der Empfänger/in ist in regelmäßigen Abständen stichprobenartig zu überprüfen. Dies gilt nicht für an Dritte zum dauerhaften Verbleib ausgegebene Speichermedien.

(2)
Es sollen behördlicherseits nur durch die zentrale IT-Beschaffungsstelle als validiert gekennzeichnete IT-Geräte und entsprechendes IT-Zubehör erworben und eingesetzt werden. Werden andere IT-Geräte oder anderes IT-Zubehör eingesetzt oder IT-Geräte außerhalb des Landesverwaltungsnetzes betrieben, ist jede Behördenleitung insofern selbst für die Einhaltung der Vorgaben des Bundesamtes für Sicherheit in der Informationstechnik (BSI) verantwortlich.

(3)

Mobile IT-Geräte, auf denen vertrauliche digitale Informationen oder personenbezogene Daten gespeichert werden, sind durch geeignete Verschlüsselungstechniken zu schützen. Bei der Verwendung von USB-Sticks ist eine Hardwareverschlüsselung zu bevorzugen.

(4)
Die Behördenleitung hat jährlich bei den Mitarbeiterinnen und Mitarbeitern abzufragen, ob und welche bislang noch nicht gemeldeten privaten IT-Geräte dienstlich genutzt bzw. welche gemeldeten privaten IT-Geräte nicht mehr genutzt werden. Nicht Gegenstand der Abfrage sind Smartphones, die lediglich dazu genutzt werden, dienstliche Anrufe auch außerhalb des Büros entgegennehmen zu können.

(5)
Soweit gesetzliche oder sonstige Rechtsvorschriften eine Löschung von personenbezogenen oder sensiblen Daten vorsehen, ist diese nach Ablauf der jeweiligen Fristen vorzunehmen und zu dokumentieren. Die rechtzeitige Löschung ist durch ein geeignetes Löschkonzept sicherzustellen.

(6)
Ist eine erforderliche Löschung von Daten nicht auf andere geeignete Weise zu erreichen, sind die Speichermedien durch physische Zerstörung zu vernichten.
Die Vernichtung von Ausdrucken mit personenbezogenen oder sensiblen Daten hat durch physische Zerstörung so zu erfolgen, dass eine Rekonstruktion ausgeschlossen ist.

(7)
Speichermedien, die an den Hersteller oder Lieferanten endgültig zurückgegeben oder an Dritte verkauft werden sollen oder die nicht mehr verwendbar sind, sind so zu löschen, dass eine Wiederherstellung ausgeschlossen ist. Ist dies technisch nicht möglich, ist eine Weitergabe der Speichermedien nicht zulässig, es sei denn, dass bei einer Herausgabe an den Hersteller oder Lieferanten mit diesem eine Vereinbarung getroffen wird, die einen sicheren Transport zum Hersteller oder zum Lieferanten und eine sofortige, revisionssichere Löschung der Daten bei diesem gewährleistet. Die Vereinbarung ist aktenkundig zu machen.

(8)
Zur Archivierung verwendete Speichermedien mit vertraulichen Informationen oder personenbezogenen Daten sind zu verschlüsseln oder in Tresoren aufzubewahren. Die Aufbewahrungsdauer richtet sich nach den zugrunde liegenden Aufgaben und den dafür geltenden Vorschriften. Die verwendeten Speichermedien sind eindeutig zu kennzeichnen und es ist ein Verzeichnis zu führen. Passwörter sind getrennt vom archivierten Medium sicher zu verwahren und vor dem Zugriff Dritter zu schützen.

(9)

Soweit es für die technische Systembetreuung erforderlich ist, sind Passwörter sicher zu hinterlegen und vor dem Zugriff Unbefugter zu schützen. Die Hinterlegung, der Austausch und jeder Zugriff sind zu dokumentieren.

§ 18 Einsatz von Programmen

(1)
Auf dienstlichen IT-Geräten dürfen nur freigegebene und validierte Softwareprodukte eingesetzt werden.

(2)
Über sämtliche auf dienstlichen IT-Geräten eingesetzte Programme ist ein Verzeichnis (Softwarekataster) bei der Behördenleitung zu führen, soweit nicht ein solches zentral für mehrere Dienststellen geführt wird. Das Verzeichnis hat mindestens folgende Angaben zu enthalten:

- Bezeichnung des IT-Geräts, auf dem das Programm eingesetzt ist,
- Inventarnummer
- Name der Software
- Versionsnummer/Release-Stand
- Lizenznummer
- bei Mehrfachlizenzen: Anzahl der eingesetzten Programme
- Art der Software (Betriebssystem, Compiler, Datenschutz- und Datensicherungssoftware, Textverarbeitungssoftware, Tabellenkalkulationssoftware usw.)
- Pflegevereinbarungen
- Angaben zum Installationsdatenträger
- Hardwarezusätze
- Kopierschutz.

§ 19 Datensicherung

Die Behördenleitung hat den ITD bei der Sicherung der verarbeiteten Informationen auf Grund des jeweils einschlägigen Datensicherungskonzepts zu unterstützen.

§ 20 Wartung und Reparatur

(1)
Die Wartung oder Reparatur eines IT-Gerätes durch justizfremdes Wartungspersonal im Dienstgebäude darf nur in Abstimmung mit der für das IT-Gerät zuständigen IT-Mitarbeiterinnen und -Mitarbeiter und in Anwesenheit einer geeigneten Aufsichtsperson erfolgen.

(2)

Justizfremdes Wartungspersonal bedarf für den Zugriff auf vertrauliche Informationen und personenbezogene Daten einer ausdrücklichen Genehmigung durch die Behördenleitung oder einer von ihr beauftragten Stelle. Die Genehmigung darf nur erteilt werden, wenn dies für die Wartung oder Reparatur technisch unabweisbar notwendig ist. Die Genehmigung ist schriftlich zu erteilen, wobei erforderlichenfalls ergänzende Weisungen zu technischen oder organisatorischen Maßnahmen und etwaige Unterauftragsverhältnisse festzulegen sind. Sie ist unter Nennung des Namens des die Reparatur oder Wartung Durchführenden zu dokumentieren; die Dokumentation ist drei Jahre ab dem Ende des Jahres der Erstellung aufzubewahren. Im Übrigen richtet sich die Aufbewahrungsdauer nach den allgemeinen Vorschriften.

(3)
Kommt eine Reparatur des IT-Gerätes im Dienstgebäude nicht in Betracht, müssen sämtliche hierauf gespeicherte vertrauliche Informationen und personenbezogene Daten vollständig gesichert und danach der Datenträger des IT-Gerätes revisionssicher gelöscht werden. Anderenfalls ist der Datenträger auszubauen.

§ 21 Notfall

(1)
Ein Notfall liegt vor, wenn durch einen Verlust der Verfügbarkeit von Teilen oder der Gesamtheit des IT-Systems ein Zustand eintritt, bei dem ohne eine besondere Notfallbewältigungsorganisation innerhalb einer angemessenen Zeit die Wiederherstellung der Verfügbarkeit nicht möglich ist und sich daraus ein sehr hoher Schaden ergibt oder ein solcher einzutreten droht.

(2)
Die Behördenleitung hat unter Berücksichtigung der Vorgaben des Notfallmanagementsystems der Justiz ein Notfallhandbuch zu erstellen, in dem die Maßnahmen anzuführen sind, die bei Eintritt eines Notfalls getroffen werden müssen. § 13 Abs. 1 und 2 bleiben unberührt.

(3)
Das Notfallhandbuch ist allen Beteiligten entsprechend ihrer dienstlichen Betroffenheit zur Kenntnis zu geben und soll sowohl elektronisch als auch im schriftlichen Ausdruck vorhanden sein.

(4)
Die Behördenleitung ist für die Aktualität des Notfallhandbuches verantwortlich.

§ 22 Prüfungspflicht

(1)

Die behördeninterne Kontrolle der Einhaltung dieser Dienstanweisung, sonstiger zum Datenschutz und zur Informationssicherheit bestehender Vorschriften und Anweisungen sowie die Kontrolle von Art und Umfang der getroffenen Maßnahmen obliegt der Behördenleitung. Die von ihr mit diesen Aufgaben betrauten Mitarbeiterinnen und Mitarbeiter sind berechtigt, bei den einzelnen Anwenderinnen und Anwendern nach entsprechender Ankündigung Kontrollen vorzunehmen, und verpflichtet, die Beseitigung festgestellter Mängel zu überwachen. Über die Ergebnisse der Kontrollen ist bei besonders schwerwiegenden Mängeln ein Aktenvermerk zu fertigen, der dem/der Datenschutzbeauftragten und/oder dem/der Informationssicherheitsbeauftragen zuzuleiten ist. Die Regelung des § 65 Abs. 4 des Landespersonalvertretungsgesetzes NRW ist zu beachten.

(2)
Für die nach Absatz 1 wahrzunehmenden Aufgaben stellt die Behördenleitung einen mit dem/der Datenschutzbeauftragten und dem/der Informationssicherheitsbeauftragten abgestimmten Kontrollplan auf. In diesem Kontrollplan ist unter Berücksichtigung der für die einzelne Behörde geltenden Regelungen festzulegen, welche Kontrollen bei welchen Stellen durchgeführt werden sollen. Die Kontrollen sollen mindestens jährlich stattfinden. Der Kontrollplan soll dem anliegenden Muster-Kontrollplan (Anlage 2) entsprechen. Er muss mindestens die dort aufgeführten Aufgaben betrachten.
Die Kontrollbefugnis des/der Datenschutzbeauftragten bleibt unberührt.

(3)
Über Mängel, deren Beseitigung nicht im Einflussbereich der Behördenleitung liegt und die auch nicht vom ITD beseitigt werden können (z. B. Programmfehler), ist der vorgesetzten Dienstbehörde zu berichten.

(4)
Die vorgesetzte Dienstbehörde prüft im Rahmen der regelmäßigen Geschäftsprüfungen das Vorliegen einer verbindlichen behördeneigenen Dienstanweisung und eines Kontrollplans und sowie das Ergebnis der Prüfung des Kontrollplans.

Abschnitt 4
(Aufhebung von Vorschriften, Überprüfung und Inkrafttreten)

§ 23 Aufhebung von Vorschriften, Überprüfung und Inkrafttreten

(1)
Die Rundverfügung vom 25. März 2002 (1510 - I D. 15) wird aufgehoben.

(2)

Diese Dienstanweisung wird regelmäßig, spätestens alle drei Jahre, auf ihre Aktualität hin überprüft.

(3)
Die Dienstanweisung tritt zum 01. November 2022 in Kraft.