U

15

Die Präsidentin
des Amtsgerichts Mitte

Dienstanweisung

für die Nutzung der IT-Infrastruktur, des Internets und anderer elektronischer Informations- und Kommunikationsdienste bei dem Amtsgericht Mitte

Stand: 10.08.2022

Inhaltsverzeichnis

U

1 Vorbemerkung

Das Dezernat X (Serviceeinheit IT für die ordentliche Gerichtsbarkeit -) stellt unter Zuhilfenahme des IT-Dienstleistungszentrums Berlin (ITDZ) die IT- Infrastruktur und ausgewählte Dienste (z.B. Intranet, Internet, E-Mail) zur Verfügung. Die Vorgaben dieser Dienstanweisung sind von den Nutzenden entsprechend der auf den Endgeräten bereit gestellten Anwendungen zu beachten.

Das Dezernat X bei dem Präsidenten des Kammergerichts erbringt auf Grundlage der mit der Präsidentin des Amtsgerichts Mitte getroffenen Servicevereinbarung vom 20.06.2013/26.09.2013 IT-Dienstleistungen für das Amtsgericht.

2 Begriffsbestimmungen

Im Sinne dieser Dienstanweisung sind

Dez X beim Präsidenten des Kammergerichts	Dezernat für Informationstechnologie in der ordentlichen Gerichtsbarkeit bei dem Präsidenten des Kammergerichtes
ITDZ	IT-Dienstleistungszentrum Berlin
Zentrale Grundbuchdatenstelle (ZGBS)	Anwendungs- und Anwendungssystembetreuung des gesamten Verfahrens unter solumSTAR
FAT-Client	Arbeitsplatz-PC der Anwendenden; Datenaustauschstation
VPN Client	mobiler Arbeitsplatz Laptop; Zugriffsmöglichkeit über eine direkte, verschlüsselte Datenverbindung zum zentralen Server
SBC	Server Based Computing der ordentlichen Gerichtsbarkeit, in der z. Zt. die meisten Programme und Daten auf zentralen Servern bereitgestellt, ausgeführt und gesichert werden
IT-Betreuung	die geschäftsplanmäßig mit der Wahrnehmung der

	Aufgaben der IT-Angelegenheiten befassten Mitarbeitenden des Amtsgerichtes Mitte
Anwendungssystembetreuer*innen	die örtlich mit der Wahrnehmung der Aufgaben als Anwendungssystembetreuer*in betrauten und geschulten Mitarbeitenden des Amtsgerichtes; Ansprechpartner*in zur ZGBS, zum Dez. X und den anderen Fachverfahren; First-Level-Help-Desk
Anwenderbetreuer*innen	örtliche Mitarbeitende, die bei der Erledigung von Fachaufgaben mit der Informationstechnik unterstützen, Ansprechpartner*in der ZGBS und des Dez. X beim KG
Anwender*in / Nutzer*in	alle Mitarbeitenden im Amtsgericht

3 Ansprechpartner*innen

3.1 IT-Stelle

Störungen und Ausfälle der an den Arbeitsplätzen installierten Geräte sind unverzüglich der IT-Stelle zu melden. Änderungen der Berechtigungen (z.B. Sachgebietswechsel) sind von den Verantwortlichen des jeweiligen Sachgebiets ebenfalls rechtzeitig - vorzugsweise per E-Mail - der IT-Stelle unter der Anschrift IT-Stelle@ag-mitte.berlin.de mitzuteilen.

Die Zuständigkeiten für bestimmte Online-Dienste, die Vergabe von Berechtigungen und bei Problemen mit der IT-Technik ergeben sich aus der im Verzeichnis I:\IT-Zuständigkeiten eingestellten Zusammenfassung.

Bei einer selbstständigen Einrichtung eines häuslichen Arbeitsplatzes durch Beschäftigte erfolgt kein Support, der über die Treiberinstallation nach 9.2.4 hinausgeht. Bei der heimischen Nutzung eines VPN Laptops hat der*die Anwender*in selbst für die Einrichtung eines funktionierenden und störungsfreien Internetanschlusses Sorge zu tragen.

3.2 ANITA

Technische Probleme im Zusammenhang mit der **SBC-Umgebung** sind direkt an die **Annahmestelle für IT-Störungen** bei dem Präsidenten des Kammergerichts **- ANITA - (Tel. 915 - 25 15, E-Mail: anita.kg@it.verwalt-berlin.de)** zu melden.

3.3 Anwenderbetreuer*innen

Bei **fachlichen oder verfahrensspezifischen** Fragen sind zunächst die Anwenderbetreuer*innen für das entsprechende Verfahren bzw. Sachgebiet zu kontaktieren. Diese werden bei Bedarf weitere Bereiche informieren.

4 Sicherheitshinweise

4.1 Allgemeines

Das Dezernat X (Serviceeinheit IT für die ordentliche Gerichtsbarkeit -) ergreift - zum Teil unter Zuhilfenahme des IT-Dienstleistungszentrums Berlin (ITDZ) - Maßnahmen, um die Sicherheit der beim Amtsgericht Mitte eingesetzten Informations-Technologie (IT) zu gewährleisten. Über diese Maßnahmen haben die Anwender*innen die folgenden Regelungen zu beachten, damit die getroffenen Vorkehrungen nicht unterlaufen werden.

4.2 Nutzung der IT-Technik

Jede*r Anwender*in hat sorgsam, insbesondere „gewaltfrei" mit der Informationstechnik umzugehen. An den Geräten dürfen keine privaten Aufkleber angebracht werden.

Eigenmächtige Standortveränderungen von IT-Endgeräten (insbes. PC, Monitor und Drucker) sind zu unterlassen, da die Geräte inventarisiert und bestimmten Nutzer*innen, Räumen oder Netzwerksegmenten zugeordnet sind.

Private IT-Geräte dürfen nicht an das Berliner Landesnetz oder an dienstliche IT-Geräte angeschlossen werden; das gilt auch für Mobiltelefone. Verboten ist auch die Nutzung privater Software auf dienstlichen IT-Geräten.

Jede*r Anwender*in hat Zugriff auf die im Netz eingestellten Anleitungen und Handbücher (Infoportal unter http://justiz.b-intern.de/ag-mitte/arbeits-hilfen/bedienungsanleitungen/). Die Anweisungen in diesen Dokumenten sind unbedingt zu beachten.

4.2.1 Aufstellung und Handhabung der Geräte

Die an den Arbeitsplätzen installierten IT-Geräte dürfen keiner direkten und starken Sonneneinstrahlung ausgesetzt und nicht in unmittelbarer Nähe von Wärmequellen (z.B. Heizgeräten, Heizungen) aufgestellt werden.

Sie sind auf einer stabilen, ebenen Fläche in einem Raum mit ausreichender Belüftung

aufzustellen. Die Umgebungstemperaturen sollten stabil gehalten werden. Abrupte Temperatur- und Luftfeuchtigkeitsschwankungen sind zu vermeiden.

Belüftungsöffnungen dürfen nicht blockiert, abgedeckt oder verklebt werden. Die Ablage von Akten oder anderen Gegenständen auf Drucker und Tastatur ist zu unterlassen.

Der Drucker sollte genügend Freiraum erhalten, so dass alle ausziehbaren Teile der Papierzuführung ohne Umstellen genutzt werden können. Die Lüftungsschlitze des Druckers sollten nicht auf den Arbeitsplatz des Anwendenden gerichtet sein.

Zum Wechsel des Toners, der Belichtungseinheit, bei Fehlern im Druckbild, bei Papierstau oder sonstigen Fehlern, die unerklärlich sind, ist unverzüglich die Hilfe der IT-Stelle in Anspruch zu nehmen. Keinesfalls darf mit Gegenständen im Inneren des Druckers herumhantiert werden. Daraus resultierende Beschädigungen des Druckers können haftungsrechtliche Ansprüche auslösen.

Es ist darauf zu achten, dass keine Gegenstände oder Flüssigkeiten in die Geräte gelangen.

Die Rechnereinheit darf auch nach dem Ausschalten wegen der Möglichkeit der Fernwartung nicht vom Stromnetz getrennt werden (Daher Netzschalter am Gerät und an der Steckdosenleiste nicht ausschalten!).

Es ist verboten, die Gehäuse von Geräten eigenmächtig zu entfernen oder Geräte selbst zu warten (Gefahr eines Stromschlags). Wartungsarbeiten dürfen nur die IT-Stelle oder ein autorisierter Kundendienst vornehmen.

Die Benutzung der EDV-Steckdosen ist für andere technische Geräte untersagt (z.B. Kaffeemaschinen, Wasserkocher, Handy-Aufladekabel).

Die Reinigung der Geräte mit einem trockenen oder leicht befeuchteten Tuch obliegt dem*der jeweiligen Anwender*in. Reinigungsmaterialien werden von der Hausverwaltung (C 2) bei Bedarf ausgegeben.

4.3 Notebook/Tablet-Benutzung

Bei der Benutzung eines dienstlich zur Verfügung gestellten Notebooks/Tablets sind folgende Regeln einzuhalten:

Das Gerät ist pfleglich zu behandeln und nicht direkter Sonneneinstrahlung sowie Feuchtigkeit auszusetzen. Es ist untersagt, das Gerät zu manipulieren oder selbst zu warten. Wartungsarbeiten darf allein die IT-Stelle vornehmen bzw. beauftragen.

Das Notebook/Tablet darf bei Nutzung außerhalb des Dienstgebäudes nicht unbeaufsichtigt gelassen werden. Wird der Raum für längere Zeit verlassen, ist das Gerät auszuschalten und wegzuschließen.

Beim Transport ist mit besonderer Sorgfalt darauf zu achten, dass Beschädigungen vermieden werden. Beim Transport mit einem Kraftfahrzeug ist es außerdem gesichert und für Dritte nicht einsehbar aufzubewahren.

Das Notebook/Tablet darf nur mit lizenzierter Software genutzt werden. Die Nutzung des Internets über einen auf dem Gerät lokal installierten Internetbrowser wird aufgrund der Bedrohung durch Viren und Schadsoftware nicht empfohlen. Dieses gilt nicht, wenn das Gerät für das VPN der Berliner Justiz berechtigt ist und das Internet über die dienstliche Desktop-Umgebung benutzt wird.

Nach dem zum Zeitpunkt des Erlasses der Dienstanweisung bekannten technischen Sachstand ist der Zugang zum VPN der Justiz über jede Form einer Netzwerkverbindung unter Aspekten der Datensicherheit gefahrlos, da von dem Gerät eine direkte, verschlüsselte Datenverbindung zu den beim ITDZ betriebenen Systemen aufgebaut wird. Dennoch besteht die Möglichkeit, dass z. B. bei der Nutzung von öffentlichen WLAN-Hotspots aus der Anmeldung des Gerätes am Netzwerk Nutzer*innenprofile erstellt werden können. Es obliegt daher wie bei anderen privaten netzwerkfähigen Geräten dem*der einzelnen Nutzer*in des Notebooks, welche WLAN-Netzwerke als vertrauenswürdig einstuft werden.

Kommunikationsschnittstellen wie Netzwerkanschlüsse, drahtlose Kommunikationsschnittstellen und andere Schnittstellen zum VPN der Berliner Justiz dürfen mit einem mobilen Gerät nur dann genutzt werden, wenn das Gerät dafür berechtigt ist, m.a.W. das Gerät darf nicht eigenmächtig, sondern nur nach entsprechender Instruktion durch einen Mitarbeitenden der IT-Stelle mit den im Dienstgebäude befindlichen Netzwerkanschlüssen verbunden werden. Die Koppelung dieser Geräte mit dem VPN der Berliner Justiz erfolgt in der Regel mit Hilfe einer entsprechenden Docking-Station.

Von dem*der Anwender*in erstellte Dokumente sollen vorrangig in der SBC-Umgebung gespeichert werden, wenn das mobile Gerät den Zugang zu SBC ermöglicht, m. a. W. es soll vorrangig die auch auf dem Arbeitsplatz im Gericht vorhandene IT-Umgebung genutzt werden. Ist dieses nicht möglich, dürfen Dokumente auf dem mobilen Gerät nur temporär gespeichert werden und ist dafür zu sorgen, dass die erstellten Dokumente entweder gelöscht oder in die SBC-Umgebung übernommen werden.

Die IT-Stelle sichert keine von Anwender*innen erzeugten Dokumente. Die IT-Stelle hält lediglich die Installationsdateien für Betriebssystem und Programme bereit.

Bei Rückgabe des Notebooks an die IT-Stelle oder Weitergabe an andere Berechtigte sind alle erzeugten Dokumente und Dateien zu löschen. Soweit diese ausnahmsweise noch benötigt werden (z. B. Profil einer Spracherkennungssoftware), sind sie auf einem externen Speichermedium zu sichern.

4.4 Arbeitsplatzergonomie

4.4.1 Sitzhaltung

Die Anwender*innen sitzen möglichst gerade zum Bildschirm. Sie vermeiden körperliche Zwangshaltungen, indem sie die Arbeitsmittel so anordnen, dass sie ihren Körper nicht verdrehen oder schief halten. Grundsätzlich sollen Tischkante, Tastatur, Arbeitsvorlage und Bildschirmoberfläche senkrecht zur Sehachse der Anwender*innen verlaufen.

Der Stuhl sollte so eingestellt sein, dass Ober- und Unterschenkel einen Winkel von 90 Grad bilden, wenn die Füße flach auf dem Boden stehen.

Mithilfe der Einstellungsmöglichkeiten der elektrisch höhenverstellbaren Tische sollen die Anwender*innen für eine abwechselnde Sitz- und Stehposition während der Bildschirmarbeit Sorge tragen.

4.4.2 Einstellung des Tisches

Die Höhe des Tisches sollte so eingestellt sein, dass die Unterarme parallel aufliegen können und die Oberarme locker herunterhängen. Auch hier sollte ein Winkel von ca. 90 Grad eingehalten werden.

4.4.3 Sehabstand

Der Sehabstand zum Monitor sollte je nach Bildschirmgröße zwischen 60 und 100 cm betragen. Die oberste lesbare Zeile des Monitors sollte sich maximal in Augenhöhe befinden.

4.4.4 Beleuchtung, Raumklima und Lärm

Die Arbeitsplätze müssen gemäß den ergonomischen Vorschriften ausreichend beleuchtet sein. Blendeinwirkungen sind zu vermeiden.

Zum gesundheitlichen Wohlbefinden ist für gute Luftqualität und gutes Raumklima zu sorgen. Der*die Anwender*in hat die Büroräume ausreichend zu lüften.

Es ist darauf zu achten, dass der Schallpegel den Arbeitsaufgaben entsprechend niedrig zu halten ist.

4.5 Passwortschutz

Die Benutzer*innenkennung und das Passwort regeln die technische Zugangskontrolle

zum IT-Netz und zu anderen Diensten. Damit verbunden ist die Festlegung der einzelnen Zugriffsrechte auf Verzeichnisse, Dateien oder Online-Dienste (vgl. hierzu unten Nr. 5).

Das Passwort ist individuell nach Maßgabe der jeweiligen Anforderungen des Systems zu wählen.

Eine Weitergabe der Benutzer*innenkennung und des Passwortes ist strikt untersagt.

Es wird ausdrücklich darauf hingewiesen, dass aus den Protokolldateien (vgl. unten Nr. 7) die Identität der Nutzer*innen hervorgeht. Im Falle einer Weitergabe des Passwortes wird jegliche Aktivität - auch unzulässige Nutzung durch Dritte - dem*der eigentlich berechtigten Anwender*in zugeschrieben.

Soweit eine Tätigkeit an einem anderen IT-Arbeitsplatz als gewöhnlich erforderlich ist (z.B. bei Vertretungseinsätzen), erfolgt die Anmeldung immer mit der eigenen Benutzer*innenkennung (walking-user Prinzip).

4.6 Räumliche Zugangskontrolle

Es ist sicherzustellen, dass unberechtigten Personen der Zugang zu den Diensträumen verwehrt bleibt. In Räumen mit Publikumsverkehr ist - unter Berücksichtigung der ergonomischen Anforderungen - der Bildschirm so aufzustellen, dass eine Sicht auf die schutzbedürftigen Daten durch Dritte nicht möglich ist.

Beim Verlassen des Raumes ist die passwortgeschützte Bildschirmsperre (mit den Tasten „Strg + Alt + Entf“ und der Auswahl der Option „Sperren“, bzw. mit den Tasten „⊞ + L“) zu aktivieren. Die Verpflichtung zum Abschließen der Zimmertür bleibt unberührt.

4.7 Datenübertragung in das IT-Netz

Die Übertragung von Daten in das IT-Netz ist mittels elektronischer Post (E-Mail, vgl. unten Nr. 6) möglich und auf das dienstlich unbedingt erforderliche Maß zu beschränken. Eine Übertragung von ausführbaren Programmdateien (z.B. *.dotx, *.bat, *.com, *.exe, *.scr, *.vbs, *.vba, oder *.wsh) ist unzulässig.

Außerhalb des Berliner Landesnetzes erzeugte Dokumente (vgl. Ziff. 9.4) dürfen für eine Weiterverarbeitung im Anhang einer E-Mail oder besser noch direkt im Text einer E-Mail an die dienstliche E-Mail-Adresse versandt oder über den eTeamwork-Server übertragen werden.

Der direkte Datenübertrag von externen Speichermedien (z.B. Disketten, CD-ROM, USB-Speichersticks) ist grundsätzlich untersagt. Eine im Einzelfall notwendige Datenübertragung erfolgt über eTeamwork mit Hilfe eines beim ITDZ betriebenen BSCW Servers oder mit dem im Gericht aufgestellten Transfer-PCs. Die auf dem eTeamwork-Server gespeicherten Dateien sind unverzüglich nach Abschluss des Datentransfers zu löschen.

Neben den Mitarbeiter*innen der IT-Stelle können weitere Mitarbeiter*innen für eine direkte Nutzung von eTeamwork zugelassen werden. Entsprechende Einrichtungswünsche sind an die IT-Stelle zu richten. Der Transfer-PC steht allen Mitarbeitenden zur Verfügung.

Es ist verboten, Daten oder Programme sowie gespeicherte oder zu speichernde Informationen - gleich welchen Inhalts und welchen Dokumentationsstandes - zu einem anderen als dem dienstlich vorgesehenen Zweck zu vervielfältigen, persönlich zu verwenden oder anderen als den hierzu befugten Personen zugänglich zu machen. Sofern Unbefugte IT-Geräte benutzen oder dies versuchen, ist unverzüglich die IT-Stelle zu informieren.

4.8 Verhalten bei Virenbefall

Sollte es trotz der getroffenen technischen und in dieser Dienstanweisung enthaltenen organisatorischen Vorbeugemaßnahmen zu einem Virenbefall kommen, ist Folgendes zu beachten:

a) Ruhe bewahren!

   Auf keinen Fall die auf dem Bildschirm ausgegebenen Aufforderungen beachten, da dadurch oftmals ein größerer Schaden angerichtet werden kann.

b) Benachrichtigung!

   Vom Virenbefall ist unverzüglich die IT-Stelle sowie die Geschäftsleitung bzw. die Gruppenleitung zu benachrichtigen, und es sind die weiteren Anordnungen abzuwarten.

Auch beim mobilen Arbeiten und am häuslichen Arbeitsplatz gelten die Regelungen des Arbeitsschutzes, des Gesundheitsschutzes und der Arbeitssicherheit. Die Dienststellen überwachen jedoch nicht deren Einhaltung beim Arbeiten außerhalb der Dienstgebäude bzw. der zugewiesenen Arbeitsplätze des Dienstherrn.

Die Dienststellen schulen Beschäftigte, denen das mobile Arbeiten gestattet ist oder werden soll, im Rahmen der allgemeinen Unterweisung über die Belange des Arbeits- und Gesundheitsschutzes sowie der Arbeitssicherheit auch zu den besonderen Anforderungen des Arbeitens am häuslichen Arbeitsplatz bzw. des mobilen Arbeitens.

Diese Schulung umfasst insbesondere die notwendigen Sicherheitsmaßregeln bei mobi-

ler Nutzung. Soweit für die Sicherung bei mobiler Nutzung weitere Ausstattung (z.B. Kabelschlösser) notwendig sind, wird diese in angemessenem Umfang durch die Dienststelle gestellt.

5 Dateiablage

5.1 Allgemeines

Die nachstehenden Regelungen gelten nur, soweit Dateien außerhalb eines für die Vorgangsbearbeitung eingesetzten Fachverfahrens gespeichert werden.

Die Einhaltung dieser Regeln ist für einen reibungslosen Geschäftsbetrieb zwingend erforderlich. Sie gewährleisten, dass die Dateien von den jeweiligen Sachbearbeiter*innen ohne Schwierigkeiten im IT-Netz gefunden werden.

5.2 Home-Verzeichnis

Jedem*jeder Anwender*in wurde im Netz ein Home-Verzeichnis (Laufwerk H:) zugeordnet, auf das außer ihm*ihr kein Dritter Zugriff hat. Dateien oder Entwürfe, die nicht von Dritten gelesen werden sollen, sind in diesem Verzeichnis abzulegen.

5.3 Gemeinsame Verzeichnisse

Sobald eine Weiterbearbeitung von Dateien durch Dritte erfolgen soll, sind diese in den entsprechend eingerichteten Gruppenverzeichnissen der Sachgebiete abzulegen. Diese Verzeichnisse sind in den Zugriffsrechten auf die berechtigten Anwender*innen beschränkt.

5.4 Vorlagen-Verzeichnisse

Die Vorlagenverzeichnisse enthalten einheitliche Vorlagen für die verschiedenen Sachgebiete. Änderungs- und Anpassungswünsche, Korrekturen und Anregungen sind über die jeweilige Gruppenleitung an die IT-Stelle zu richten.

Selbst erstellte "Vorlagen" aus dem eigenen Home-Verzeichnis oder aus Gruppenverzeichnissen sind nicht für Ausgangsschreiben zu verwenden, da diese im Fall von Veränderungen nicht aktualisiert werden. Das Erscheinungsbild von ausgehenden Schreiben soll einheitlich sein.

6 Online-Dienste

6.1 Allgemeines

Mit der bereitgestellten IT-Infrastruktur ist generell die Nutzung des Intranets der Berliner Verwaltung und des Internets möglich.

Für die Nutzung des Internets und anderer elektronische Informations- und Kommunikationsdienste (E-Mail) gilt die Internet-Dienstvereinbarung vom 21.02.2002, die zwischen der Senatsverwaltung für Inneres und dem Hauptpersonalrat abgeschlossen wurde (abrufbar unter http://www.berlin.de/hpr/dienstvereinbarungen/dv8.html). Sie regelt auch für die Gerichte die Nutzung von Internet und E-Mail. Die Dienstvereinbarung zwischen dem Hauptrichterrat und der Senatsverwaltung für Justiz vom 20.10.2010 behandelt denselben Themenbereich für das richterliche Personal des Landes Berlin.

7 Elektronischer Rechtsverkehr

7.1 Empfang

Der elektronische Empfang verfahrensbezogener Dokumente und Anträge erfolgt ausschließlich über Postfächer des Elektronischen Gerichts- und Verwaltungspostfachs - EGVP – mit Hilfe der Eingangslistenapplikation (ELA). Näheres regelt die Dienstanweisung für die Behandlung elektronischer Eingänge (veröffentlicht in der Vorschriftendatenbank unter http://justiz.b-intern.de/ag-mitte/organisation/dienstliche-regelungen/dienstanweisung-ag-mitte-ela-01-01-2018.pdf).

7.2 Versand aus forumSTAR

Das elektronische Versenden und Weiterleiten von Dokumenten erfolgt über die Fachanwendung forumSTAR. Hierbei sind die Dokumente regelmäßig mit einer qualifizierten elektronischen Signatur mittels Signaturkarte zu versehen. Durch Einstecken der Karte in den SC-Kartenslot der Tastatur und Eingabe der persönlichen PIN wird der qualifizierte Versand ausgelöst.

7.3 Versand über das elektronische Gerichts- und Verwaltungspostfach (EGVP)

In Verwaltungsangelegenheiten erfolgt die Kommunikation mit anderen Gerichten und Behörden in den gesetzlich vorgeschriebenen Fällen in elektronischer Form. Der Ver-

sand erfolgt über die Fachanwendung Vibilia durch autorisierte Personen. Eine zusätzliche Signatur der Dokumente ist aufgrund des vertrauenswürdigen Postfaches nicht erforderlich.

7.4 Signaturkarten

Bei der Signaturkarte handelt es sich um eine Chipkarte, die den privaten Schlüssel eines digitalen Zertifikats enthält. Eine qualifizierte elektronische Signatur (qeS) hat die gleiche Rechtswirkung wie eine handschriftliche Unterschrift. Die Identität der Person, die das Dokument signiert hat, ist damit zweifelsfrei nachweisbar.

Die Signaturkarte ist durch den*die Anwender*in persönlich online zu beantragen. Alle dafür notwendigen Informationen werden durch den*die Gruppenleiter*in des Sachgebiets zur Verfügung gestellt.

Nach Erhalt der Signaturkarte ist ein*e Mitarbeiter*in der IT-Stelle zu informieren, damit dieser*diese die Aktivierung der Karte vornehmen kann.

Die zur Signaturkarte gehörige PIN und PUK ist geheim zu halten. Die Karte ist diebstahlsicher und vor Fremdzugriff geschützt aufzubewahren. Die Nutzung der Karte ist personengebunden und ausschließlich zu dienstlichen Zwecken zulässig.

Beim Ausscheiden aus dem Dienst ist die Karte der Dienststelle zu übergeben. Bei Verlust, Beschädigung oder unbefugter Benutzung ist die Dienststelle unverzüglich in Kenntnis zu setzen.

8 Fachverfahren

Zur dienstlichen Nutzung stehen Fachanwendungen und Online-Abfragen zur Verfügung. Die Einrichtung und Verwaltung der Zugangsberechtigungen obliegt der IT-Stelle. Hierzu zählen insbesondere:

- **beck-online** und **juris** (juristische Recherche)
- **AuReg-Online** (Registerabfragen beim Registergericht Amtsgericht Charlottenburg) bzw. Portal www.handelsregister.de
- **Olmera** (Zugriff auf Einwohnermeldedaten.) Bei Abfragen ist in jedem Fall das Aktenzeichen des Bezugsverfahrens anzugeben.
- **ZTR** (Zentrales Testamentsregister)
- **Vollstreckungsportal** (Einsicht in Schuldner- und Vermögensverzeichnisse)
- **ProFiskal** (Rechnungswesen)
- **AULAK** (Aktenverwaltung und Schriftguterstellung, nur noch für die Sachgebiete Betreuung und Nachlass)
- **SolumSTAR** (Grundbuchangelegenheiten)

- **forumSTAR** (Aktenverwaltung und Schriftguterstellung)

9 Mobiles Arbeiten

9.1 Ausstattung

Die Ausstattung erfolgt in Abstimmung mit den Gremien. Der Empfang der Geräte ist zu quittieren. Sie sind sorgfältig zu behandeln. Die Einrichtung, Wartung und ggf. Reparatur der Geräte bzw. die entsprechende Beauftragung obliegt der IT-Stelle des Amtsgerichts.

9.2 Umfang der Nutzung

Die Geräte dürfen nur für dienstliche Zwecke genutzt werden. Dienstliche Angelegenheiten umfassen auch Angelegenheiten der Gerichtsverwaltung, die Tätigkeit als Güterichterin/Güterichter, Schulungstätigkeiten sowie ehrenamtliche Tätigkeiten im Zusammenhang mit richterlicher Tätigkeit (z.B. im Präsidium, in Mitwirkungsgremien, als Datenschutz- oder Schwerbehindertenbeauftragte*r oder im Richterwahlausschuss). Das Speichern von nicht für die dienstliche Nutzung bestimmten Daten auf dem Laptop ist unzulässig.

Der Anschluss privater Ein- und Ausgabegeräte (z.B. Tastaturen, Mäuse, Monitor, Drucker) ist zulässig, soweit die Geräte über entsprechende Anschlüsse verfügen. Der Dienstherr bzw. die Dienststelle übernehmen die Installation entsprechender Treiber, soweit der Aufwand hierfür angemessen ist und kein Risiko für die Funktionalität der dienstlichen IT insgesamt entsteht; ein Anspruch, die Funktionsfähigkeit privater Geräte bzw. deren Kompatibilität mit dienstlichen Geräten zu gewährleisten, besteht nicht.

9.3 Kosten des mobilen Arbeitens

Die durch das mobile Arbeiten anfallende Kosten, einschließlich Verbrauchskosten, z.B. für Strom oder Telekommunikation, sind von den Mitarbeitenden selbst zu tragen.

Hiervon unberührt bleibt der durch Ortstermine und Anhörungstermine bestehende Anspruch auf Auslagenersatz.

10 Sicherheitsmaßnahmen

10.1 Sicherheitsrelevante Ereignisse

Alle bei der Nutzung der Dienste auftretenden sicherheitsrelevanten Ereignisse, wie

z.B. unerklärliches Systemverhalten, Verlust oder Veränderung von Daten und Programmen, Verdacht auf Missbrauch der Benutzer*innenkennung, des Passwortes usw., sind durch den*die Anwender*in unverzüglich der IT-Stelle anzuzeigen. Aufklärungsversuche durch den*die Anwender*in sind erst nach Absprache mit den dort Zuständigen zulässig.

10.2 Vorbehalte

Bei der Beschaffung, Weiterverarbeitung und Weitergabe der über die Dienste zugänglichen Informationen sind Urheber- und Lizenzrechte zu beachten. Zweifelsfälle sind unverzüglich mit der Gerichtsleitung zu klären.

10.3 Kostenpflichtige Angebote

Der Zugriff auf kostenpflichtige Angebote ist nur nach Zustimmung mit der Gerichtsleitung zulässig. Mit Zustimmung des Dezernats X beim Präsidenten des Kammergerichts angebotene Informationen (z.B. Juris und beck-online) bleiben hiervon unberührt.

10.4 Datenverarbeitung außerhalb des Berliner Landesnetzes

Werden dienstliche Daten außerhalb des Berliner Landesnetzes verarbeitet, wie beispielsweise beim Entwurf einer Entscheidung am häuslichen Arbeitsplatz, so ist die Verwendung personenbezogener Daten zu vermeiden; namentliches Rubrum und Geschäftszeichen sollen nur am dienstlichen Arbeitsplatz bearbeitet werden.

Sollte die Versendung von vertraulichen Informationen im Anhang einer E-Mail ausnahmsweise notwendig sein, ist die Datei zu verschlüsseln. Die Erstellung einer verschlüsselten Datei ist mit der Anwendung 7-ZIP möglich, welche auch in der SBC-Umgebung installiert und nutzbar ist. Eine Anleitung für den Umgang mit 7-ZIP kann im Intranet unter http://justiz.b-intern.de/ag-mitte/arbeitshilfen/bedienungsanleitungen/artikel.810068.php#7zip abgerufen werden. Das bei der Verschlüsselung verwendete Passwort darf keinesfalls als Klartext mit der E-Mail versandt werden!

Die Verarbeitung dienstlicher Daten setzt eine gesicherte Systemumgebung voraus; das System darf nicht öffentlich zugänglich sein und muss nach dem aktuellen Stand der Technik vor unerwünschten Netzwerkzugriffen geschützt (Firewall) sowie im Falle eines Drahtlosnetzwerkes mit einer dem aktuellen Stand der Technik entsprechenden Verschlüsselung geschützt sein.

Der häusliche Rechner muss bei einer Verarbeitung dienstlicher Daten über aktuelle Si-

cherheitsupdates für das Betriebssystem verfügen und mit einem sich regelmäßigen aktualisierendem Virenschutzprogramm versehen sein. Bei Rechnern mit dem Betriebssystem MS Windows ist nur noch das Betriebssystem Windows 10 oder höher zu verwenden.

Die bestehenden dienstlichen Regelungen über den Einsatz von Kommunikationstechnik, über die Verwendung dienstlicher IT-Systeme und die Fachanwendungen gelten jeweils auch, soweit diese im Rahmen des mobilen Arbeitens genutzt werden. Der Anschluss privater externer Speichermedien (z.B. Festplatten, Speicherkarten) oder von privaten Geräten, in die solche Speichermedien verbaut sind (z.B. Smartphones, Kameras) ist verboten.

Das Datenschutzrecht einschließlich der Regelungen zum Sozialdatenschutz gilt auch für mobiles Arbeiten.

Die Beschäftigten sind verpflichtet, bei der mobilen Arbeit auf die erhöhten Gefahren, insbesondere für die Vertraulichkeit personenbezogener Informationen, besonders zu achten und diese so zu schützen, dass Dritte keine Einsicht und keinen Zugriff nehmen können. Dies schließt Familienangehörige der Beschäftigten ein.

Soweit zum mobilen Arbeiten oder zur Verwendung hierfür ausgegebener Geräte personen- oder gerätebezogene Kennungen, Passwörter, PINs oder vergleichbare Berechtigungsnachweise erteilt werden, dürfen diese nicht an Dritte weitergegeben werden. Hiermit gesicherte Geräte dürfen auch im häuslichen Bereich nur unbeaufsichtigt gelassen werden, wenn durch Abmelden, Sperren o.ä. gewährleistet ist, dass ein Zugriff nur mit dem Berechtigungsnachweis erfolgen kann. Beim Transport dürfen Geräte nicht unbeaufsichtigt gelassen werden, insbesondere nicht in Fahrzeugen zurückgelassen werden.

Soweit mobile Geräte einen VPN-Zugang zur SBC-Umgebung ermöglichen, müssen Beschäftigte das Gerät mindestens einmal pro Monat über mehrere Stunden an ihrem Arbeitsplatz im Gericht betreiben, damit über das Landesnetz Sicherheitsupdates und Aktualisierungen aufgespielt werden können.

11 Protokollierung

Für die Speicherung des Datenverkehrs zwischen dem lokalen Netz, den Online-Diensten und Kommunikationsdiensten (E-Mail) gilt die Internet-Dienstvereinbarung vom 21.02.2002, die zwischen der Senatsverwaltung für Inneres und dem Hauptpersonalrat abgeschlossen wurde (abrufbar unter http://www.berlin.de/hpr/dienstvereinbarungen/dv8.html). Sie regelt auch für die Gerichte die Nutzung von Internet und E-Mail. Die Dienstvereinbarung zwischen dem Hauptrichterrat und der Senatsverwaltung für Justiz vom 20.10.2010 behandelt denselben Themenbereich für das richterliche Personal des Landes Berlin.

Die beim mobilen Arbeiten durch den elektronischen Datenaustausch anfallenden Verbindungsdaten werden nicht für eine Zeiterfassung oder zu Leistungs- und Verhaltenskontrollen genutzt. Die Verbindungsdaten sowie die Nutzung oder Nichtnutzung der Angebote zum mobilen Arbeiten haben insbesondere keinen Einfluss auf dienstliche Beurteilungen.

12 Besondere Belange Beschäftigter mit Schwerbehinderung

Die besonderen Belange Beschäftigter mit Schwerbehinderung werden berücksichtigt. Bei der Einrichtung eines der Behinderung entsprechenden häuslichen Arbeitsplatzes für Beschäftigte mit Schwerbehinderung leistet die Dienststelle bei Bedarf Unterstützung bei der Beantragung von Kostenzuschüssen bei externen Kostenträgern (z. B. Integrationsamt).

13 Sanktionen

Vorsätzliche und grob fahrlässige Verstöße gegen die Regelungen zur Nutzung der IT-Infrastruktur können den sofortigen Ausschluss der Dienstkraft von der Nutzung der IT-Systeme zur Folge haben sowie ggf. weitere dienst- und strafrechtliche Konsequenzen nach sich ziehen.

Die Haftung der Beschäftigten gegenüber dem Dienstherrn für Beschädigungen bzw. Abhandenkommen von Geräten für das mobile Arbeiten ist auf Vorsatz und grobe Fahrlässigkeit beschränkt. Eine Haftung für unabwendbare oder auf höherer Gewalt beruhende Ereignisse besteht nicht.

14 Inkrafttreten, Außerkrafttreten

Diese Dienstanweisung tritt am 15.08.2022 in Kraft.

Sie tritt mit Ablauf des 14.08.2027 außer Kraft.

Berlin, den 10.08.2022
i. V.
Dr. Buck

Die Präsidentin des Amtsgerichts Mitte

S:\Verwaltung\1-Verfassung und Verwaltung\15 - Elektronische Datenverarbeitung\15 - Generalakte\2022-08-10-ITDienstanweisung-final-(gegendert).docx