Innerdienstliche Anordnung des Justizministeriums zum Einsatz von Informationstechnik in der Justiz (Dienstanweisung IT)

vom 23. September 2020, Az.: JUMRII-JUM-1500-12/1/4

INHALTSÜBERSICHT

1.

…

2. Zielgruppe

Diese Anordnung … gilt auch für sonstige Personen mit Zugang zu dienstlich genutzten IT-Endgeräten im Geschäftsbereich des Ministeriums der Justiz und für Europa.

3. Inhaltlicher Geltungsbereich

Die Anordnung enthält Regelungen zur Verwendung von Informationstechnik sowie zum Zugangsschutz, die von *jeder* Person der Zielgruppe unabhängig von ihrer Funktion umzusetzen sind.

„Dienstliche Nutzung“ ist jede Verwendung der Bürokommunikation, die der Aufgabenwahrnehmung für das jeweilige Gericht oder für die jeweilige Justizbehörde dient oder mit dieser in Zusammenhang steht. Alle anderen Verwendungen sind „private Nutzung“.

…

Verstöße gegen diese Regeln können disziplinar- oder arbeitsrechtliche Konsequenzen haben. Bei missbräuchlicher Nutzung des Internets können Haftungsansprüche entstehen.

4.

…

5. Verwendung von Hardware und Software

5.1 Freigegebene Hardware und Software zur dienstlichen Nutzung

5.1.1 Grundsätzliche Regelung

Für die Verarbeitung dienstlicher Daten ist nur von der Justizverwaltung bereitgestellte Hardware zugelassen. Für dienstliche Zwecke eingesetzte Software wird entweder von der Verwaltungsleitung bereitgestellt oder darf nur nach einem vom Justizministerium (IuK-Leitstelle) freigegebenen Verfahren beschafft und installiert werden. Diese Regelung betrifft nicht nur die Erst- und Standardausstattung, sondern auch zusätzliche Hardware- und Software-Ausstattungen.

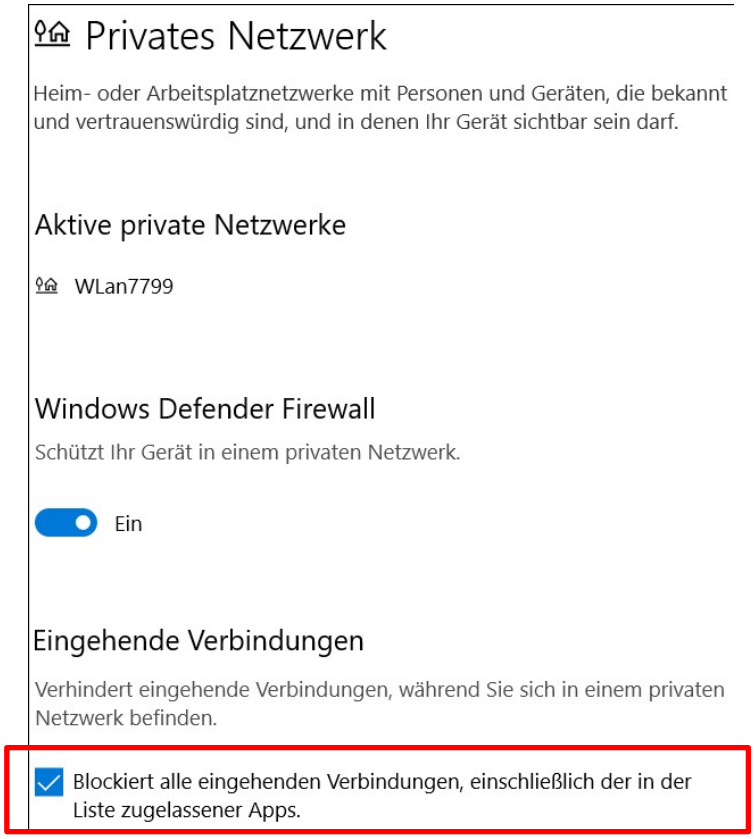
5.1.2 Ausnahmen

Hiervon gibt es folgende Ausnahmen:

a) Personen, die keinen dienstlichen Computer erhalten (etwa Referendare oder ehrenamtliche Richter), dürfen dienstlich bezogene Daten, die ihnen über öffentlich zugängliche Quellen oder über das Akteneinsichtsportal zur Verfügung gestellt werden, abrufen und auf einem *dienstlichen* USB-Stick bearbeiten und speichern. Ferner dürfen sie auf dem dienstlichen USB-Stick Dokumente erstellen, weiterbearbeiten und speichern. Dabei ist die Bearbeitung möglichst offline ohne Verbindung zum Internet durchzuführen. Der dienstliche USB-Stick ist auch für den sicheren Transport zum zuständigen Ansprechpartner vor Ort zu verwenden. Steht für die sichere Bearbeitung, Speicherung oder den sicheren Transport kein dienstlicher USB-Stick zur Verfügung, muss zur Verschlüsselung alternativ auf einem privaten Computer bzw. privaten USB-Stick die Anwendung 7-Zip (Download über https://www.7-zip.de/) mit denselben Vorgaben wie in Nummer 5.6 verwendet werden – auch zur Übertragung von verschlüsselten Anhängen in E-Mails. Die Übertragung ist auch online über das EGVP möglich. Eine *unverschlüsselte* Speicherung oder Bearbeitung auf einem privaten Computer (wiederum möglichst offline) sowie die unverschlüsselte Übertragung solcher Dokumente per normaler E-Mail an die Dienststelle

ist nur dann erlaubt, sofern Namen und alle sonstigen personenbezogene Merkmale hinreichend unkenntlich gemacht oder entfernt wurden. Gespeicherte Aktenauszüge sind nach Beendigung der zur Verarbeitung berechtigenden Zwecksetzungen unwiederbringlich zu löschen (bei USB-Sticks am besten über die Rücksetzungsfunktion). Auch die auf dienstlichen USB-Sticks gespeicherten Inhalte sind vor Rückgabe unwiederbringlich zu löschen.

Der verwendete private Computer muss in jedem Fall mit einem Betriebssystem mit regelmäßigen zeitnahen oder automatisches Updates und mit einer möglichst tagesaktuellen gebräuchlichen Anti-Viren-Software sowie einer Personal Firewall ausgestattet sein (Software, die den Datenverkehr eines PC filtert), die während der Dokumentenbearbeitung eingehende Verbindungen blockt (trotzdem ist das Surfen im Internet uneingeschränkt möglich, weil der Verbindungsaufbau ausgehend erfolgt). Bei Computern mit einem Windows-Betriebssystem ist dazu beispielsweise die mitgelieferte Sicherheitssoftware „Windows-Defender“ entsprechend dem folgenden Screenshot zu konfigurieren.



<u>Hinweis:</u> Auf diese Einstellung gelangt man am schnellsten durch klicken auf Virenscannersymbol in der Taskleiste → Firewall- & Netzwerkschutz → Privates Netzwerk oder alternativ über Windows-Symbol → Einstellungen (Zahnrad) → Update & Sicherheit → Windows-Sicherheit → Firewall- & Netzwerkschutz → Antennensymbol links → Privates Netzwerk.

b) …

c) :::

5.1.3 Weitere Regelungen

Nicht mehr benötigte Hardware wird auf Veranlassung der jeweiligen Verwaltungsleitung abgebaut oder ist ihr zu übergeben (insbesondere mobile Datenträger).

…

5.2 IT-Nutzerinformation zum Umgang mit IT-Arbeitsmitteln – insbesondere Notebooks

5.2.1

…

5.2.2 Sorgfaltspflichten und Schutzmaßnahmen

Dienstlich zur Verfügung gestellte IT-Arbeitsmittel sind sorgfältig zu behandeln und vor Beschädigung und dem unbefugten Zugriff Dritter zu schützen. … Dritte dürfen keine Kenntnis von dienstlichen Angelegenheiten erlangen.

…

5.3

….

5.4

…

5.5

…

5.6 Sichere Datenübermittlung

Für die elektronische Kommunikation der Verfahrensbeteiligten (elektronischer Rechtsverkehr) mit Gerichten und Staatsanwaltschaften bestehen gesetzliche Vorgaben, sodass hierfür in der Regel das elektronische Gerichts- und Verwaltungspostfach (EGVP) oder die De-Mail zu verwenden ist.

Sofern außerhalb des Anwendungsbereichs der gesetzlichen Regelungen zum elektronischen Rechtsverkehr *sensible* Daten mit anderen Stellen ausgetauscht werden müssen, stehen auch andere sichere Übertragungskanäle zur Verfügung, die zu nutzen sind:

- …,
- Übertragung als verschlüsselter Anhang in einer E-Mail (auch für den Empfang). Für die Verschlüsselung ist die Anwendung 7-Zip mit AES 256 Bit zu verwenden (Verschlüsselung: Dateien oder Verzeichnisse markieren > rechte Maustaste > 7-Zip > Zu einem Archiv hinzufügen > Passwort eingeben. Genauere Anleitungen sind im Wissensportal unter „Wissensdatenbank → Allgemein (Wikiseite) → IT-Sicherheit“ hinterlegt). Das Passwort muss hinreichend sicher sein (vgl. Nummer 6 „Zugangssicherheit (Passwörter)“) und auf einem separaten Kanal (etwa Telefon, SMS) ausgetauscht werden.
- Postversand der Daten mittels dienstlichem USB-Stick oder eines optischen Datenträgers unter separater Mitteilung des Verschlüsselungs-Passwortes auf anderem Kanal. …
- …

Verschlusssachen sollten nur in unabdingbaren Ausnahmefällen elektronisch gespeichert und ausgetauscht werden. Die Übertragung von Verschlusssachen ab Stufe VS-Vertraulich ist nicht gestattet. Verschlusssachen, deren Einstufung über VS-NfD hinausgeht, sind von der elektronischen Aktenführung ausgenommen.

5.7

…

6. Zugangssicherheit (Passwörter)

…

Die Sicherheit eines Passwortes wächst exponentiell mit seiner Länge und dem verwendeten Zeichenvorrat, so dass generell eine Passwortlänge von 10 oder noch besser 12 Stellen empfohlen wird. Mit Verwendung der Software ‚Kee-Pass 2' … ist es trotzdem möglich, die verschiedenen Passwörter (etwa für die Fachverfahren) mit Hilfe nur eines einzigen ausreichend langen und sicheren Master-Passwortes zu verwalten. …

Auch ohne Verwendung von KeePass 2 kann man lange Passwörter erzeugen, die man sich trotzdem gut merken kann. Dies gelingt, indem man sich einen Satz (möglichst mit eingebauten Zahlen) merkt und
- von jedem Wort aus diesem Satz jeweils den Anfangsbuchstaben wählt,
- Zahlen vollständig übernimmt
- und schließlich geeignete Zeichen durch Sonderzeichen ersetzt.

Beispiel: Der Satz <**M**ein **U**rlaub **i**n **2017 w**ar **s**o **s**chön**, w**eil **d**ie **T**emperatur **n**icht **s**o **h**och **w**ar> führt zunächst zu <MUi2017wss,wdTnshw> und schließlich zum Passwort <MU!2017w$$,wdTnshw>, das eine Länge von 18 Stellen aufweist. Eine zusätzliche Technik zum Erzeugen solcher Sätze ist, in einem Lieblingsbuch eine Stelle mit einem längeren Satz mittels einem Post-it zu markieren. Zum Wechseln solcher generierten Passwörter bietet es sich an, an einer Zwischenstelle einen Zähler einzubauen und bei jedem Wechsel zu verändern.

…

Die Eingabe von Passwörtern muss unbeobachtet erfolgen.

Jedes Passwort darf nur einer einzigen Person bekannt sein. Passwörter dürfen daher nicht weitergegeben werden … .

.

Passwörter dürfen nicht aufgeschrieben und auch *nicht unverschlüsselt* elektronisch gespeichert werden. Zur sicheren elektronischen Handhabung von Passwörtern kann die Software „KeePass 2“ verwendet werden.

…

7.

7.1

…

Für die *private* Nutzung sozialer Medien mit *privaten* Rechnern ist der ‚Leitfaden private Nutzung sozialer Medien' zu beachten (im Justiz-Intranet abgelegt unter Justizministerium > Vorschriften und Dienstanweisungen > EDV / Internet).

7.2

…

7.2.1

…

7.2.2

…

7.2.3

…

8. Dokumenteninformationen

Die nachfolgenden Dokumenteninformationen beruhen auf den Vorgaben der Richtlinie ISMS-Dokumentenarchitektur BW in Umsetzung von Nummer 5.2.1.1 VwV Informationssicherheit.

Version	1.0
Verteilerkreis:	Alle Gerichte und Justizbehörden in Baden-Württemberg sowie weitere Personen nach Genehmigung durch das Ministerium der Justiz und für Europa
Ersteller:	Dr. Matthias Schirle (Informationssicherheitsbeauftragter des Ministeriums der Justiz und für Europa)
Freigegeben am:	22.09.2020
Freigegeben durch:	Ministerialdirektor Steinbacher