Verhaltensregeln zu technischen und organisatorischen Maßnahmen der Notarinnen und Notare im Hinblick auf elektronische Aufzeichnungen und Hilfsmittel

I. Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a) DS-GVO)

- **Mobile Speichermedien**, die die Geschäftsstelle verlassen (z.B. Notebooks, Tablets und externe Festplatten), müssen nach dem Stand der Technik verschlüsselt sein.
- **Sonstige Speichermedien**, die regulär in der Geschäftsstelle verbleiben (wie insbesondere der Server und Arbeitsplatzrechner), sollen ebenfalls nach dem Stand der Technik verschlüsselt sein.
- Auf die Nutzung eines **WLAN** für Bürotätigkeiten soll verzichtet werden. Sofern die Nutzung erforderlich sein sollte, muss das WLAN nach dem Stand der Technik verschlüsselt sein.
- Die **Website** der Notarstelle muss mindestens über eine Transportverschlüsselung nach dem Stand der Technik verfügen.[1]

II. Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste (Art. 32 Abs. 1 lit. b) DS-GVO)

1. Vertraulichkeit

a) Zutrittskontrolle

- Der Raum, in dem sich der **Server** befindet, soll nicht für den Publikumsverkehr geöffnet sein. Dort, wo dies aufgrund der räumlichen Gegebenheiten nicht anders möglich ist, muss die Notarin bzw. der Notar durch weitere technische und organisatorische Maßnahmen sicherstellen, dass kein unbeaufsichtigter Zugriff auf den Server erfolgen kann.
- **Weitere Geräte**, die personenbezogene Daten verarbeiten, wie z.B. Arbeitsplatzrechner und Multifunktionsdrucker, sollen ebenfalls so aufgestellt sein, dass sie vor unbeaufsichtigtem Zugriff oder Manipulation geschützt sind. Die Geräte können z.B. an nicht öffentlich zugänglichen oder an jederzeit durch Mitarbeitende einsehbaren Stellen platziert werden. Sofern die örtlichen Gegebenheiten dies nicht zulassen, muss der Druckauftrag z.B. durch eine PIN-Eingabe, einen Transponder oder eine Benutzerkarte gestartet und überwacht werden.

---

[1] Vgl. etwa BSI TR-02102-2.

- **Mobile Speichermedien** der Notarstelle müssen bei Nichtgebrauch so aufbewahrt werden, dass sie vor Gelegenheitsdiebstahl geschützt sind (z.B. in einem abschließbaren Schrank).

b) Zugangskontrolle

- Für verschiedene Anwendungen und Dienste (wie die Anmeldung zum Arbeitsplatzrechner, zur Notarsoftware, zur Einsicht in das Grundbuch, das ZVR usw.) müssen für unterschiedliche Zugänge **unterschiedliche Passwörter** verwendet werden. Der Einsatz geeigneter Passwortmanager, die Passwörter nach dem Stand der Technik schützen, sowie einer Zwei-Faktor-Authentisierung bei der Nutzung von Online-Diensten sind empfehlenswert.
- Passwörter dürfen **nicht weitergegeben** werden.
- Die Notarin bzw. der Notar muss auf eine hinreichende Passwortsicherheit durch an aktuellen Standards orientierten **Passwortrichtlinien** achten.[2]
- Passwörter müssen unverzüglich **geändert** werden, wenn der Verdacht besteht, dass jemand unbefugt Kenntnis erlangt hat. Darüber hinaus müssen vom Anbieter voreingestellte Passwörter (die automatisch vergebenen Passwörter bei einer Erstanmeldung) für Software und Hardware geändert werden. Einzelnen Mitarbeitenden individuell zugewiesene Accounts müssen nach deren Ausscheiden unverzüglich insgesamt deaktiviert werden.
- Ist eine **Aufbewahrung** von Passwörtern erforderlich, müssen diese an einem sicheren Ort (z.B. in einem Tresor, abschließbaren Schrank oder Passwortmanager) hinterlegt werden. Keinesfalls darf ein Passwort in unmittelbarer Nähe des Arbeitsplatzrechners (z.B. unter der Tastatur oder in der Schreibtischschublade) notiert sein.
- Passwörter sollen nicht automatisch **gespeichert** werden. Auch im Browser sollen keine Passwörter gespeichert sein, es sei denn, diese werden durch ein Masterpasswort zusätzlich abgesichert.
- Sofern die betreffende Anwendung eine dahingehende Konfiguration erlaubt, sollen häufige fehlgeschlagene Anmeldeversuche zu zeitlichen **Sperrungen** führen.

c) Zugriffskontrolle

- Bei der Delegation von Benutzerrechten und Programmberechtigungen an Mitarbeitende und externe Dienstleister muss sichergestellt werden, dass die Nutzer nur die zur Erledigung ihrer Aufgaben notwendigen **Berechtigungen** erhalten. Hierfür ist

---

[2] Vgl. BSI ORP.4.A8, A22, A23 (Stand Februar 2020).

ein Rechte- und Rollenkonzept empfehlenswert. Die vergebenen Rechte müssen regelmäßig auf ihre Aktualität bezüglich der jeweiligen Tätigkeitsfelder überprüft werden.

- **Administratorenrechte** dürfen nur ausgewählten Mitarbeitenden zugewiesen werden. Eine Anmeldung mit Administratorrechten soll nur während Softwareinstallationen oder Konfigurationsänderungen am System erfolgen.
- **Dienstleister** dürfen in den Amtsräumen nur unter angemessenen Aufsichtsmaßnahmen Arbeiten an IT-Systemen oder Telekommunikationsanlagen vornehmen.
- Gegenüber Dritten muss sichergestellt sein, dass beim Verlassen des Raums kein unbefugter Zugriff auf den Arbeitsplatzrechner erfolgt. Nach einer dem Bildschirmstandort angemessenen Wartezeit muss eine **automatische Bildschirmsperre** erfolgen. Wenn es in der konkreten Situation angebracht erscheint, soll die Bildschirmsperre auch bei kürzerer Abwesenheit manuell aktiviert werden.
- Der **Bildschirminhalt** muss vor neugierigen Blicken geschützt werden, etwa durch eine entsprechende Bildschirmausrichtung oder durch den Einsatz von Blickschutzfolien. Dies gilt insbesondere für die Bildschirme im Empfangsbereich.
- Sofern in **öffentlich zugänglichen Bereichen** (z.B. Wartebereich, Flur) Netzwerk-Infrastruktur vorhanden ist, soll eine geeignete Authentifizierung nach dem Stand der Technik erfolgen.[3] Wenn dies – wie im Regelfall – nicht umsetzbar ist, soll sich keine Netzwerk-Infrastruktur im Wartebereich befinden. Sofern ein Wireless-Local-Area-Network (WLAN) eingerichtet ist, soll sich ferner der Router oder WLAN Access Point nicht in den öffentlich zugänglichen Bereichen befinden. Sofern dies aufgrund der örtlichen Gegebenheiten nicht anders möglich ist, dürfen die Zugangsdaten zum Netzwerk nicht auf dem Gerät stehen. Ein Einsatz der WPS-Funktion (Wi-Fi Protected Setup) soll nach dem derzeitigen Stand der Technik nicht erfolgen; der Einsatz darf nicht erfolgen, wenn sich das Gerät in einem öffentlich zugänglichen Bereich befindet.
- Nicht benötigte **Netzwerk-Ports** müssen deaktiviert werden.
- Vor der **Entsorgung** eines Datenträgers müssen alle Daten sorgfältig gelöscht sein, z.B. durch mehrfaches Überschreiben oder physische Zerstörung des Datenträgers.

2. Integrität

- Das gesamte Netzwerk muss nach außen durch eine sachgerecht konfigurierte **Firewall** geschützt sein.

---

[3] Derzeit z.B. IEEE 802.1x/RADIUS.

- Ferner muss innerhalb des Netzwerks eine geeignete **Netzwerksegmentierung** erfolgen, z.B. mittels Virtual Local Area Network (VLAN). Neben einem etwa vorhandenen Gäste-WLAN (s. sogleich) müssen mindestens solche Geräte, die keinen Serverzugriff erfordern, ein eigenes Netzwerksegment bilden (z.B. mit dem Internet verbundene Alarmanlagen, Frankiermaschinen, Kartenzahlungsgeräte).
- Alle Arbeitsplatzrechner und Server sowie sonstigen zentralen Komponenten, die dem Datenaustausch dienen, müssen über ein **Virenschutzprogramm** verfügen. Das Virenschutzprogramm einschließlich der verwendeten Signaturen muss stets aktuell gehalten werden und so konfiguriert werden, dass es Datenträger und Netze (Notarnetz, Intranet, Internet) sowie Dateien von Dritten, z.B. E-Mail-Anhänge, vor dem Öffnen prüft bzw. überwacht. Je nach Betriebssystem können hierbei die vom Hersteller bereitgestellten Maßnahmen ausreichen.
- Eingegangene **E-Mails** müssen bereits mittels technischer Vorkehrungen auf Spam und Schadsoftware untersucht werden.
- Auf die Nutzung eines **WLAN** für Bürotätigkeiten soll verzichtet werden. Sofern die Nutzung erforderlich sein sollte, muss das WLAN nach dem aktuellen Stand der Technik verschlüsselt sein. Gäste- und private Mitarbeitergeräte dürfen mit diesem WLAN nicht verbunden werden. Sofern für Gäste- und private Mitarbeitergeräte ein WLAN angeboten werden soll, muss ein separates Gäste-WLAN bereitgestellt werden.
- **Private Mitarbeitergeräte** dürfen nicht für die Verarbeitung von personenbezogenen Daten von Mandaten verwendet werden.
- Die Notarin bzw. der Notar darf in der Notarstelle nur Betriebssysteme verwenden, die regelmäßige **Updates** bereitstellen. Sicherheits-Updates (insbesondere für das Virenschutzprogramm, aber auch für Firewall, Router, Betriebssystem, Web-Browser, Notarsoftware, andere Office-Anwendungen etc.) müssen regelmäßig durchgeführt werden. Auch bestimmte Hardware-Komponenten müssen regelmäßig gewartet und aktualisiert werden, wobei hierfür eine individuelle Betrachtung möglicher Schwachstellen erforderlich ist.
- Alle **aus externen Quellen** bezogenen Dokumente müssen vor dem Öffnen auf **Schadsoftware** überprüft werden. In Office-Anwendungen sollten nur überprüfte und digital signierte Makros aktiviert werden, sofern dies technisch möglich ist und insbesondere weitere Systeme und Software (wie die eingesetzte Notarsoftware) ohne Einschränkungen verwendet werden können.
- Die **Mitarbeitenden** müssen im erforderlichen Umfang zu Fragen der IT-Sicherheitund der Sicherheit der Verarbeitung personenbezogener Daten qualifiziert und regelmäßig sensibilisiert werden. Insbesondere muss die Notarin bzw. der Notar die Mitarbeitenden für die Gefahren externer Inhalte, etwa beim unbedachten Öffnen

verdächtiger E-Mail-Anhänge und Links, beim Download von Dateien aus dem Internet und bei der Nutzung fremder Speichermedien (z.B. eines USB-Sticks eines Dritten) sensibilisieren. Im Zweifelsfall müssen sichernde Maßnahmen ergriffen werden, z.B. eine Nachfrage beim Absender der E-Mail, eine Überprüfung des USB-Sticks vor der Nutzung oder dessen alleinige Verwendung an einem speziell gesicherten Arbeitsplatzrechner. Weiter sollen die Mitarbeitenden dazu angehalten werden, nur bekannte bzw. die notwendigsten Websites zu besuchen, da allein der Besuch einer Website bereits zu Infektionen mit Schadcode führen kann.

- Sofern von außerhalb auf das interne Netzwerk zugegriffen wird (z.B. bei einer Auswärtsbesprechung oder -beurkundung oder bei Heimarbeit), muss dies über eine sichere **VPN-Verbindung** geschehen. Dies gilt nicht für den Fall einer Fernwartung (s.u. Ziff. II.3.).

3. Verfügbarkeit

- Die **Hardware** muss regelmäßig gewartet und unter Berücksichtigung des Standes der Technik erneuert werden.
- **Wichtige IT-Komponenten** (Server, Sicherungsmedien, Register- bzw. Notarnetzbox etc.) dürfen keinen wesentlichen Umgebungsrisiken (wie extreme Luftfeuchtigkeit, Staubbelastung, Temperatur etc.) ausgesetzt sein und müssen an eine unterbrechungsfreie Stromversorgung mit Überspannungsschutz angeschlossen sein.
- Die Notarin bzw. der Notar soll besonders wichtige Systemelemente **redundant** vorhalten.
- Daten sollen **nicht lokal** auf dem Arbeitsplatzrechner gespeichert werden, sondern auf Servern und Festplatten, die dem Backup unterliegen. Die Notarin bzw. der Notar muss die Mitarbeitenden auf die Gefahr des unwiederbringlichen Verlusts lokal gespeicherter Daten hinweisen.
- Im Falle einer **Fernwartung** müssen technische und/oder organisatorische Vorkehrungen gegen Missbrauch getroffen werden. Solche Vorkehrungen können z.B. darin bestehen, dass
    - anhand eines Protokolls nachvollziehbar ist, welche Veränderungen vorgenommen wurden und auf welche Daten zugegriffen wurde,
    - der Beginn der Fernwartung durch den Notar oder die betroffenen bzw. zuständigen Mitarbeitenden ausgelöst wird und diese die Fernwartung mitverfolgen und jederzeit abbrechen können,
    - die Zugriffsrechte des Technikers auf ein Minimum beschränkt werden,
    - die Fernwartungsdaten nur verschlüsselt und über eine geschützte Verbindung übertragen werden.

- Verkettungen und gegenseitige **Abhängigkeiten von Systemkomponenten** sollen möglichst vermieden werden. So sollen Systeme z.B. nicht davon abhängen, ob ein bestimmter Arbeitsplatzrechner in Betrieb ist oder nicht.

4. Belastbarkeit

- Die Notarin bzw. der Notar soll im Zusammenwirken mit einer **IT-Fachkraft** prüfen, wie sich die Belastbarkeit der Systeme erhöhen lässt. Zu einer höheren Belastbarkeit beitragen kann z.B. eine Abgrenzung kritischer Komponenten, ein Einfügen zusätzlicher Redundanzen (wie eines sog. RAID-Systems) oder ein Ausbau von Speicherkapazitäten.
- Zur regelmäßigen Erneuerung von **Hardware-Komponenten** s. Ziff. 3; auch weitere der in Ziff. 3 genannten Verhaltensregeln (wie eine Minimierung von lokal gespeicherten Daten) tragen zu einer besseren Belastbarkeit der Systeme bei.

III. Rasche Wiederherstellung der Verfügbarkeit der Daten und des Zugangs zu ihnen bei einem Zwischenfall (Art. 32 Abs. 1 lit. c) DS-GVO)

- Die Notarin bzw. der Notar muss ein **Notfallkonzept** für Zwischenfälle erstellen. Dieses soll insbesondere eine Festlegung enthalten, wer bei einem Zwischenfall damit beauftragt wird, wiederherstellende Maßnahmen einzuleiten. Sofern dies ein externer IT-Dienstleister ist, sollen auch die Mitarbeitenden ihren Ansprechpartner und die Kontaktdaten kennen.
- Die Notarin bzw. der Notar muss ein **Backup-Konzept** erstellen und umsetzen. Dieses soll sich an folgenden Maßgaben orientieren:
    - Die **Zuständigkeit** für das Backup (samt Stellvertretung bei Urlaub, Krankheit etc.) ist klar geregelt.
    - Das Backup umfasst **sämtliche Daten**.
    - Das Backup folgt der sog. **3-2-1-Regel**, d.h. es erfolgen drei Datenspeicherungen auf mindestens zwei verschiedenen Backupmedien (auch „Offline“), wobei sich ein Backupmedium an einem externen, hinreichend abgesicherten Standort befindet (z.B. Tresor, anderer Brandabschnitt), um vor Einbrüchen, Brand, Wasserschäden und ähnlichen Gefahren geschützt zu sein. Das Backup wird regelmäßig auf Vollständigkeit, Korrektheit und Wiederherstellbarkeit **geprüft**.
    - Die Backupmedien und auch der Datenübertragungsweg sind **verschlüsselt**. Empfehlenswert ist ferner eine Einschränkung der Schreibrechte auf dem Backupsystem.

IV. Kontrolle der vorgenannten Maßnahmen (Art. 32 Abs. 1 lit. d) DS-GVO)

- Die vorliegenden Verhaltensregeln müssen **turnusmäßig** auf ihre Einhaltung überprüft werden. Dabei ist eine enge Zusammenarbeit mit dem Administrator bzw. IT-Dienstleister und der/dem Datenschutzbeauftragten empfehlenswert.
- Des Weiteren sollen in einem **physischen Rundgang** durch die Notarstelle sämtliche Elemente überprüft werden.
- Für einen besseren **Überblick** soll zudem ein Netzwerkplan und eine Dokumentation der IT-Infrastruktur der Notarstelle vorgehalten werden.

V. Voraussetzungen für Abweichungen von den Verhaltensregeln

- Die vorstehenden Verhaltensregeln spiegeln bewährte und angemessene Verfahren für eine Vielzahl typischer Verarbeitungstätigkeiten wider, wobei drei Regelungsebenen zu unterscheiden sind:
    - Verbindliche Regelungen ohne Abweichungsmöglichkeit („muss“/„darf nicht/nur, wenn“)
    - Verbindliche Regelungen mit Abweichungsmöglichkeit („soll“/„soll nicht“)
    - Unverbindliche Empfehlungen („empfehlenswert“, Beispiele)
- Ein Abweichen von einer Soll-Vorschrift kommt grundsätzlich nur in Betracht, wenn die Abweichung durch nachvollziehbare, sachliche Gründe – auch unter Berücksichtigung der Schutzinteressen der Betroffenen – gerechtfertigt ist und der vom Gesetz bezweckte Datenschutz zudem in gleichem Maße wie bei Einhaltung des Wortlauts der betreffenden Verhaltensregel gewährleistet ist.