

## INHALT

### Bekanntmachungen

Gebührensatzung für das Elektronische Urkundenarchiv (UA-GebS)	401
Gebührensatzung für das notarielle Videokommunikationssystem (NotViKo-GebS)	403

### Mitteilungen

Verhaltensregeln der Bundesnotarkammer zu technischen und organisatorischen Maßnahmen der Notarinnen und Notare im Hinblick auf deren elektronische Aufzeichnungen und die zur Führung notarieller Akten und Verzeichnisse verwendeten elektronischen Hilfsmittel	405
Eröffnung der Forschungsstelle für notarielle Rechtsgestaltung (NotaReG)	411
Veranstaltungen des Fachinstituts für Notare	412
Verbraucherpreisindex für Deutschland im April 2022	412

### Aktuelles Forum

<i>Danninger/Walch</i> , Datensicherheit in elektronischen Aufzeichnungen und Hilfsmitteln	413
<i>Meier</i> , Eigentumsübergang und Grundsteuerreform	425

### Aufsatz

<i>Siegel/Berthold</i> , Die elektronische Urkundensammlung und von der Haupturkunde abweichende Unterlagen	429
---	-----

### Rechtsprechung

#### *I. Erbrecht*

Auslegung vertragsgemäßer Verfügungen in einem Erbvertrag <i>OLG München, Beschl. v. 3. 11. 2021 – 31 Wx 110/19</i>	461
--	-----

## *II. Notarrecht*

Ermessensausübung der Justizverwaltung bei Wiederbesetzung einer Notarstelle

*BGH, Beschl. v. 20. 7. 2020 – NotZ(Brfg) 5/19 (mit Anm. Grziwotz)*

465

## **Buchbesprechungen**

Ruhwinkel, Die Erbengemeinschaft (*Röhl*) – Hogenschurz, WEG (*Basty*) – Husemann, Der moderierte Vertrag (*Forschner*) – Weingärtner, Vermeidbare Fehler im Notariat (*Blaeschke*)

476

Herausgegeben im Auftrag der Bundesnotarkammer von  
RA und Notar Manfred Blank, Lüneburg,  
Notar a. D. Prof. Dr. Günter Brambring, Köln,  
Notar Christian Hertel, Weilheim i. OB

6 | 2022

Heft 6, Juni 2022  
Seite 401–480

### BEKANNTMACHUNGEN

## Gebührensatzung für das Elektronische Urkundenarchiv (UA-GebS)

### Vorbemerkung

Auf Grund des § 78j Absatz 1 Satz 2, Absatz 4 Satz 1 der Bundesnotarordnung hat die 125. Generalversammlung der Bundesnotarkammer am 8. April 2022 die Gebührensatzung für das Elektronische Urkundenarchiv wie folgt beschlossen:

### § 1

#### Gebührentatbestand

- (1) Die Bundesnotarkammer als Urkundenarchivbehörde erhebt Gebühren für die Aufnahme von elektronischen Dokumenten in die elektronische Urkundensammlung.
- (2) Die Bundesnotarkammer erhebt Gebühren für die Führung des Verwahrungsverzeichnisses.

### § 2

#### Gebührenhöhe

- (1) Für die Aufnahme eines elektronischen Dokuments in die elektronische Urkundensammlung wird eine Gebühr von 4,50 Euro erhoben. Werden zu einem Amtsgeschäft weitere Dokumente in die elektronische Urkundensammlung eingestellt, entsteht die Gebühr nur einmal.
- (2) Bei Beglaubigungen von Unterschriften, die nicht mit der Fertigung eines Entwurfs in Zusammenhang stehen, beträgt die Gebühr 2,50 Euro.
- (3) Für die Führung des Verwahrungsverzeichnisses wird eine Gebühr von 32 Euro pro eingetragener Verwahrungsmasse erhoben.

### § 3

#### **Gebührensschuldner**

Wer die Gebühren schuldet, richtet sich nach § 78j Absatz 2 der Bundesnotarordnung.

### § 4

#### **Fälligkeit**

(1) Die Gebühr nach § 1 Absatz 1 wird fällig, wenn zu einem Amtsgeschäft ein Dokument in die elektronische Urkundensammlung eingestellt ist.

(2) Die Gebühr nach § 1 Absatz 2 wird mit der ersten Eintragung einer Verwahrungsmasse fällig.

### § 5

#### **Art der Gebührenerhebung**

(1) Ist Gebührenschuldner, wer zur Zahlung der Kosten für die jeweilige notarielle Amtshandlung verpflichtet ist, nimmt der Notar die Gebühren, die für die Aufnahme eines elektronischen Dokuments im Elektronischen Urkundenarchiv entstehen, für die Urkundenarchivbehörde vom Gebührenschuldner entgegen. Die Urkundenarchivbehörde zieht die nach Satz 1 entgegenzunehmenden Gebühren auf der Grundlage einer Sammelrechnung von dem Notar ein. Der Notar erteilt der Urkundenarchivbehörde ein Lastschriftmandat für ein inländisches Bankkonto.

(2) Kann der Notar eine von der Urkundenarchivbehörde abgerechnete und eingezogene Gebühr nicht erlangen, obwohl die Zahlung vom Gebührenschuldner verlangt und mindestens einmal angemahnt wurde, wird diese auf Antrag zurückerstattet. Die Gebühr wird in diesem Fall unmittelbar durch die Urkundenarchivbehörde vom Gebührenschuldner erhoben. Dazu teilt der Notar der Urkundenarchivbehörde den Vor- und Nachnamen sowie die Anschrift des Gebührenschuldners mit.

(3) Im Fall des Absatz 2 erhöht sich die Gebühr um den Betrag von 3 Euro für jeden Gebührenschuldner, gegenüber dem die Urkundenarchivbehörde die Gebühr geltend macht. Die Urkundenarchivbehörde soll gleichzeitig nur einen Gebührenschuldner in Anspruch nehmen. Zahlt der Gebührenschuldner die Gebühr im Fall des Absatz 2 nicht innerhalb von zwei Monaten nach Fälligkeit, erhöht sich die Gebühr um 5 Euro, wenn sie trotz Androhung der Erhöhung nicht innerhalb von zehn Tagen vollständig bezahlt wird.

### § 6

#### **Art der Gebührenerhebung bei Notaren, Staatskasse und Notarkammern**

(1) Ist der Notar selbst Gebührenschuldner, erhebt die Urkundenarchivbehörde die Gebühren bei ihm. Der Notar erteilt der Urkundenarchivbehörde ein Lastschriftmandat für ein inländisches Bankkonto.

(2) Ist die Staatskasse oder die Notarkammer Gebührenschuldner, erhebt die Urkundenarchivbehörde die Gebühren bei diesen. Die Einzelheiten können durch Verwaltungsvereinbarungen geregelt werden.

## § 7

### **Absehen von der Gebührenerhebung**

Die Urkundenarchivbehörde kann von der Erhebung von Gebühren absehen, wenn dies durch besondere Umstände des Einzelfalls geboten erscheint, insbesondere wenn und soweit die Gebührenerhebung eine unzumutbare Härte für den Gebührenschuldner darstellen würde oder wenn der mit der Erhebung der Gebühr verbundene Verwaltungsaufwand außer Verhältnis zur Höhe der zu erhebenden Gebühr stünde.

## § 8

### **Inkrafttreten, Außerkrafttreten**

Diese Satzung tritt am 1. Juli 2022 in Kraft. Gleichzeitig tritt die Gebührensatzung für das Elektronische Urkundenarchiv in der Fassung vom 1. Oktober 2021 (DNotZ 2021, 916) außer Kraft.

Das Bundesministerium der Justiz hat die vorstehende Satzung mit Schreiben vom 12. April 2022 gemäß § 78j Absatz 4 Satz 2 der Bundesnotarordnung genehmigt.

Die vorstehende Satzung wird hiermit ausgefertigt und wird in der Deutschen Notar-Zeitschrift verkündet.

Berlin, den 2. Mai 2022

Der Präsident der Bundesnotarkammer

*Prof. Dr. Jens Bormann*

## **Gebührensatzung für das notarielle Videokommunikationssystem (NotViKo-GebS)**

### **Vorbemerkung**

Auf Grund des § 78q Absatz 1, Absatz 2 Satz 1 der Bundesnotarordnung hat die 125. Generalversammlung der Bundesnotarkammer am 8. April 2022 die Gebührensatzung für das notarielle Videokommunikationssystem wie folgt beschlossen:

## § 1

### **Gebührentatbestand und Gebührenschuldner**

(1) Die Bundesnotarkammer erhebt zur Finanzierung des Videokommunikationssystems nach § 78p Absatz 1 der Bundesnotarordnung Grundgebühren und fallbezogene Gebühren, zu deren Zahlung die Notare verpflichtet sind.

(2) Die Grundgebühr entsteht für einen Kalendermonat, wenn der Notar am fünfzehnten Tag dieses Monats aufgrund der Eintragung in das Notarverzeichnis an das Videokommunikationssystem angeschlossen ist. Notariatsverwalter sind von der Grundgebühr ausgenommen.

(3) Die fallbezogene Gebühr entsteht mit jeder Inanspruchnahme des Videokommunikationssystems durch den Notar für ein Beurkundungsverfahren oder für eine Beglaubigung einer qualifizierten elektronischen Signatur. Eine Inanspruchnahme nach Satz 1 gilt als erfolgt, wenn der Notar eine qualifizierte elektronische Signatur mittels des Videokommunikationssystems erstellt. Erfolgt eine Beglaubigung mehrerer qualifizierter elektronischer Signaturen in einem einzigen Vermerk, entsteht die fallbezogene Gebühr nur einmal.

## § 2

### Gebührenhöhe

(1) Die Grundgebühr beträgt 38 Euro für jeden Anwaltsnotar und 118 Euro für jeden hauptberuflichen Notar pro Monat.

(2) Die fallbezogene Gebühr für die Inanspruchnahme des Videokommunikationssystems beträgt 25 Euro im Falle einer Beurkundung und 8 Euro im Falle einer Beglaubigung, die der Notar mittels des Videokommunikationssystems vornimmt. Der Notar ist verpflichtet, beim Erstellen seiner qualifizierten elektronischen Signatur in dem Videokommunikationssystem anzugeben, ob es sich um eine Beurkundung oder eine Beglaubigung handelt.

## § 3

### Fälligkeit

Die Gebühren werden mit ihrer Entstehung fällig.

## § 4

### Verfahren der Gebührenerhebung

(1) Die Bundesnotarkammer zieht die Gebühren auf der Grundlage einer Sammelrechnung von dem Notar monatlich ein.

(2) Der Notar erteilt der Bundesnotarkammer ein Lastschriftmandat für ein inländisches Bankkonto.

## § 5

### Absehen von der Gebührenerhebung

Die Bundesnotarkammer kann von der Erhebung von Gebühren absehen, wenn dies durch besondere Umstände des Einzelfalls geboten erscheint, insbesondere wenn und soweit die Gebührenerhebung eine unzumutbare Härte für den Gebührenschuldner darstellen würde oder wenn der mit der Erhebung der Gebühr verbundene Verwaltungsaufwand außer Verhältnis zur Höhe der zu erhebenden Gebühr stünde.

## § 6 Inkrafttreten

Diese Satzung tritt am 1. August 2022 in Kraft.

Das Bundesministerium der Justiz hat die vorstehende Satzung mit Schreiben vom 13. April 2022 gemäß § 78q Absatz 2 Satz 2 der Bundesnotarordnung genehmigt.

Die vorstehende Satzung wird hiermit ausgefertigt und wird in der Deutschen Notar-Zeitschrift verkündet.

Berlin, den 2. Mai 2022

Der Präsident der Bundesnotarkammer

*Prof. Dr. Jens Bormann*

## MITTEILUNGEN

### **Verhaltensregeln der Bundesnotarkammer zu technischen und organisatorischen Maßnahmen der Notarinnen und Notare im Hinblick auf deren elektronische Aufzeichnungen und die zur Führung notarieller Akten und Verzeichnisse verwendeten elektronischen Hilfsmittel**

#### **I. Pseudonymisierung und Verschlüsselung (Art. 32 Abs. 1 lit. a DSGVO)**

- *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.<sup>1</sup>

---

1 Vgl. etwa BSI TR-02102-2.

## 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.
- *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.<sup>2</sup>
- 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 un-

---

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

mittelbarer 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 dahin gehende 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 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.<sup>3</sup> 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

---

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

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.
- 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-Sicherheit und 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 Backup-Medien (auch „Offline“), wobei sich ein Backup-Medium 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 Backup-Medien und auch der Datenübertragungsweg sind *verschlüsselt*. Empfehlenswert ist ferner eine Einschränkung der Schreibrechte auf dem Backup-System.

#### **IV. Kontrolle der vorgenannten Maßnahmen (Art. 32 Abs. 1 lit. d DSGVO)**

- 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* sollen 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.

#### **Eröffnung der Forschungsstelle für notarielle Rechtsgestaltung (NotaReG)**

Am 4. 6. 2022 wurde die Forschungsstelle für notarielle Rechtsgestaltung (NotaReG) an der Universität Heidelberg feierlich eröffnet. Die Forschungsstelle initiiert und betreut Forschungsprojekte aus den Schwerpunktbereichen notarieller Tätigkeit und des notariellen Verfahrens sowie zur Geschichte des Notariats und betreut universitäre Veranstaltungen und Lehrveranstaltungen zu diesen Themen. Besonderes Gewicht wird dabei Bezügen zum europäischen und internationalen Recht und zur Notariatspraxis in den südwestdeutschen Grenzgebieten sowie in den Nachbarstaaten der Länder Baden-Württemberg und Rheinland-Pfalz gegeben. Die Forschungsstelle kooperiert dabei mit der Deutschen Notarrechtlichen Vereinigung (NotRV), der Notarkammer Baden-Württemberg und der Notarkammer Pfalz.

## Veranstaltungen des Fachinstituts für Notare

### 1. Intensivkurs Kostenrecht (Tagungsnummer: Präsenz 034725 / Online 034726)

*Zeit/Ort:* 1. – 2. 7. 2022, Heusenstamm, DAI-Ausbildungszentrum  
*Referent:* Notar Dr. Thomas Diehn, Hamburg  
*Kostenbeitrag:* 435,- € / 310,- € ermäßigt für Notarassessoren und für Mitarbeiter

### 2. Notarielle Fachprüfung – Systematisches Klausurentraining (Tagungsnummer: Präsenz 034769 / Online 034770)

*Zeit/Ort:* 15. 7. 2022, Heusenstamm, DAI-Ausbildungszentrum  
*Referent:* Notar Dr. Sebastian Berkefeld, Bad Brückenau  
*Kostenbeitrag:* 325,- €

### 3. 20. Jahresarbeitsstagung des Notariats (Tagungsnummer: Präsenz 033341 / Online 034813)

*Zeit/Ort:* 8. – 10. 9. 2022, Berlin, Maritim proArte Hotel Berlin  
*Leitung:* Notar Dr. Norbert Frenz, Kempen  
*Referenten:* verschiedene  
*Kostenbeitrag:* 775,- € / 725,- € für Mitglieder der Notarkammern Berlin und Brandenburg / 675,- € ermäßigt für Notarassessoren

**Anmeldung:** Deutsches Anwaltsinstitut e.V. – Fachinstitut für Notare –, Gerard-Mortier-Platz 3, 44793 Bochum, E-Mail [notare@anwaltsinstitut.de](mailto:notare@anwaltsinstitut.de), Tel. 0234/9706418, Fax 0234/703507

Die Online-Vorträge LIVE und die Kurse bzw. Vorträge im Selbststudium sind nur über einen persönlichen DAI-Account der Teilnehmerin bzw. des Teilnehmers buchbar. Der Account kann unter dem Link [www.anwaltsinstitut.de/registrierung.html](http://www.anwaltsinstitut.de/registrierung.html) erstellt werden.

**Weitere Informationen:** Homepage [www.anwaltsinstitut.de](http://www.anwaltsinstitut.de)

## Verbraucherpreisindex für Deutschland im April 2022

Nach Mitteilung des Statistischen Bundesamtes ist der Verbraucherpreisindex für Deutschland auf Basis 2015 = 100 im April 2022 gegenüber April 2021 um 7,4 % (116,2) gestiegen. Im Vergleich zum März 2022 erhöhte sich der Index um 0,8 %.

Die vollständige Pressemitteilung des Statistischen Bundesamtes Nr. 196 vom 11. 5. 2022 ist veröffentlicht unter: [www.destatis.de/DE/Presse/Pressemitteilungen/2022/05/PD22\\_196\\_611.html](http://www.destatis.de/DE/Presse/Pressemitteilungen/2022/05/PD22_196_611.html).