§ 30a Daten- und Informationssicherheit im Geschäftsbetrieb

(1) Der Gerichtsvollzieher regelt den Geschäftsbetrieb unter Beachtung der Bestimmungen der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) sowie der einschlägigen bundes- und landesrechtlichen Regelungen zum Schutz personenbezogener Daten und trifft geeignete technische und organisatorische Maßnahmen, um sicherzustellen und nachweisen zu können, dass die Verarbeitung personenbezogener Daten im Einklang mit diesenVorschriften erfolgt.

(2) [1]Das Geschäftszimmer ist so einzurichten, dass bei Publikumsverkehr personenbezogene Daten Dritter nicht offengelegt werden. [2]Akten, Register, Kassenbücher und sonstige dienstliche Unterlagen sowie für dienstliche Zwecke genutzte IT-Systeme und Datenträger dürfen ausschließlich in Räumen, die den Anforderungen des § 30 Absatz 3 entsprechen, aufbewahrt und betrieben werden. [3]Entsprechendes gilt für Unterlagen, die nach Landesrecht für die Geschäftsprüfung vorzuhalten sind. [4]Der Gerichtsvollzieher hat dafür Sorge zu tragen, dass zu Zwecken der Dienstaufsicht der Zugang zu dem Geschäftszimmer und dem Sprechzimmer sowie ein Zugriff auf sämtliche dienstlichen Unterlagen, die vom Gerichtsvollzieher genutzte Fachanwendung, Archivräume, Briefkästen, IT-Systeme und Datenträger sowie eingerichtete elektronische Postfächer gewährleistet ist.

(3) [1]Die Vertraulichkeit, Integrität und Verfügbarkeit der verarbeiteten Daten ist durch geeignete technische und organisatorische Maßnahmen sicherzustellen. [2]Die verwendeten IT-Anlagen sowie die darauf verwendeten Softwareprogramme, die Telekommunikationseinrichtungen und Datenträger sind insbesondere

1. gegen den physischen Zugriff Dritter sowie gegen physische Gefährdungen zu schützen;

2. gegen unbefugte digitale Zugriffe und Gefährdungen zu schützen, u.a. durch
   a) eine Firewall und eine Antivirensoftware, die regelmäßig zu aktualisieren sind, und
   b) die Verwendung von Kennwörtern oder Codes, die den Anforderungen von Absatz 5 entsprechen;

3. zum Schutz ihrer Integrität arbeitstäglich durch eine zu dokumentierende Anfertigung von Sicherungskopien der dienstlichen Daten so zu sichern, dass eine vollständige Wiederherstellung der Daten zum Sicherungszeitpunkt möglich ist; eine angefertigte Sicherungskopie darf erst dann überschrieben oder gelöscht werden, wenn eine neue Sicherungskopie gefertigt und in ihrer Eignung zur vollständigen Wiederherstellung verifiziert worden ist.

[3]Die für die Datensicherung nach Satz 2 Nummer 3 genutzten Sicherungsdatenträger sind eindeutig zu kennzeichnen, vor unberechtigtem Zugriff und zufälliger Zerstörung zu schützen und sollen vom IT-System räumlich getrennt aufbewahrt werden. [4]Die verwendeten Programme und die programmierte Kurzbezeichnung der Register und Kassenbücher dürfen nicht verändert werden; ausgenommen sind Veränderungen durch Software-Updates. [5]Bei Wartungs- oder Reparaturarbeiten an IT-Systemen wählt der Gerichtsvollzieher erforderliche Dienstleistungsunternehmen sorgfältig aus und trifft erforderlichenfalls Vereinbarungen über Auftragsverarbeitungen nach Artikel 28 der Datenschutz-Grundverordnung.

(4) [1]Die elektronische Kommunikation hat, soweit darin personenbezogene oder solche Daten verarbeitet werden, die unter die amtliche Verschwiegenheitspflicht fallen, in verschlüsselter Form zu erfolgen, soweit sie nicht innerhalb der geschlossenen Kommunikationsnetze des Landes oder des Bundes erfolgt. [2]Richtet der Gerichtsvollzieher elektronische Postfächer selbst ein, verfährt er mit den Zugangsdaten nach Absatz 5.

(5) [1]Kennwörter, Codes und andere Zugangsdaten zu den Einrichtungen und Geräten nach Absatz 2 bis 4 dürfen nicht identisch und müssen ausreichend lang und komplex sein. [2]Anlassbezogen, insbesondere bei dem Verdacht auf Kompromittierung des Zugangs, ist eine Änderung von Kennwörtern, Codes und anderen Zugangsdaten vorzunehmen. [3]Sie sind zum Zwecke der Dienstaufsicht in einem vom Gerichtsvollzieher versiegelten Umschlag bei der Dienstbehörde zu hinterlegen. [4]Im Falle der Änderung der Zugangsdaten

sind die geänderten Daten in gleicher Weise zu hinterlegen. [5]Der zuvor hinterlegte versiegelte Umschlag wird zurückgegeben. [6]Die Übergabe nach Satz 1 bis 4 ist durch die Dienstbehörde jeweils in einem schriftlich oder elektronisch geführten Register zu protokollieren.

(6) [1]Kommt es zu einer Verletzung des Schutzes personenbezogener Daten, hat der Gerichtsvollzieher unverzüglich seinen unmittelbaren Dienstvorgesetzten und den Datenschutzbeauftragten seiner Dienstbehörde zu benachrichtigen. [2]Der nach Landesrecht Verantwortliche im Sinne des Artikels 4 Nummer 7 der Datenschutz-Grundverordnung hat die Artikel 33 und 34 der Datenschutz-Grundverordnung zu beachten.