

Dokumentation technischer und organisatorischer Maßnahmen (Art. 25, 32 DSGVO)

Der Verantwortliche hat folgende Maßnahmen zur Sicherheit der Datenverarbeitung ergriffen:

1. Pseudonymisierung und Verschlüsselung

Jeder EDV-Arbeitsplatz ist mit einem individuellen Passwort geschützt. Diese Passwörter werden regelmäßig geändert und müssen bestimmte Kriterien erfüllen. Elektronische Kommunikation erfolgt ausschließlich über das VPN der Notarnet GmbH. Entwürfe im Erb- und Familienrecht werden nur als verschlüsselte PDF-Dateien versendet. Bei sensiblen Vorgängen wird mit den Mandanten die Möglichkeit einer Ende-zu-Ende-Verschlüsselung erörtert.

2. Gewährleistung der Vertraulichkeit

Der Zutritt zum Urkundenarchiv ist nur mit dem Notariatsschlüssel möglich. Einen solchen haben lediglich erfahrene und vertrauenswürdige Mitarbeiter des Notariats.

Das Urkundenarchiv befindet sich im Keller des Gebäudes und ist das alte Bankarchiv. Nicht nur das Archiv selber, sondern auch der Vorraum sind nur mit den vorgenannten Schlüsseln begehbar.

Der Empfang kontrolliert, ob sich unberechtigte Personen in der Geschäftsstelle aufhalten. Da jeder Mitarbeiter jedes Sachgebiet bearbeitet, hat grundsätzlich jeder sachbearbeitende Mitarbeiter Zugriff auf sämtliche Vorgänge. In keinen Räumlichkeiten, in denen sich Besucher alleine aufhalten, werden Unterlagen mit personenbezogenen Daten verwahrt. Die Türe zwischen Wartezimmer und Telefonzentrale bleibt geschlossen. Das Beurkundungszimmer ist mit einer besonders schalldichten Türe ausgestattet.

In den Urkunden enthaltene Daten werden nur an in der Urkunde genannte Dritte oder an gesetzlich vorgeschriebene Empfänger weitergegeben.

3. Gewährleistung der Integrität

Sofern Firmen nicht als vertrauenswürdig bekannt sind, werden möglichst sämtliche mitgeteilten Daten bei Kontakt mit den Beteiligten verifiziert. Ausschließlich die Hard- und Software betreuenden Firmen, TriNotar Service oHG,

NotarNet GmbH, die Schleupen AG und die Wolters Kluwer Deutschland GmbH haben (eingeschränkten) externen Zugriff auf die EDV.

Die Mitarbeiter des Notariats sind angewiesen, geänderte Beteiligendaten in der EDV abzuändern und nicht etwa eine neue Person anzulegen. Durch Einsicht in das Grundbuch und die Register wird die Richtigkeit der verwendeten Daten überprüft.

4. Gewährleistung der Verfügbarkeit

Der Server befindet sich in einem Raum, zu dem nur die Mitarbeiter Zutritt haben. Dieser Raum ist vor äußeren Einflüssen (insbesondere Hochwasser) geschützt. Der Server wird laufend gekühlt. es existiert zusätzlich eine Notstromversorgung. Neben den in den physisch vorhandenen Urkunden enthaltenen sind keine Daten erkennbar, die auch in einem solchen Fall unbedingt verfügbar sein müssen.

In der Urkundensammlung wird laufend die Luftfeuchtigkeit überprüft. Sie ist gegen Schädlingsbefall, Hochwasser und Einbruch geschützt.

5. Gewährleistung der Belastbarkeit der Systeme und Dienste

Es wird im Abstand von ca. fünf Jahren kontrolliert, ob die Hardware noch zeitgemäß ist. Die Notarsoftware und insbesondere der Virenschutz werden fortlaufend aktualisiert. Ausschließlich Frau Neuhoff-Pongratz und Herr Fleischmann-Zilian sowie die Mitarbeiter der vorgenannten IT-Firmen haben Zugriff auf den Server und kümmern sich um die Aktualisierungen. USB-Sticks werden im Notariat grundsätzlich nicht verwendet und angeschlossen, insbesondere keine USB-Sticks von Dritten. CD's können nur an den Arbeitsplätzen des Notars und von Frau Lehnhardt verwendet werden.

6. Maßnahmen zur zeitnahen Wiederherstellung der Verfügbarkeit der Daten nach Zwischenfällen

Der Datenbestand wird fortlaufend gesichert. Dabei wird der genutzte Datenträger täglich gewechselt. Die notwendigen Maßnahmen bei einem technischen Zwischenfall kennen Frau Neuhoff-Pongratz und Herr Fleischmann-Zilian. Ferner sind die zu ergreifenden Schritte in einem jedem Mitarbeiter bekannten Ordner zusammen mit wichtigen Kontaktdaten hinterlegt. Eine Sicherungskopie wird regelmäßig außerhalb des Büros gelagert; sie ist verschlüsselt. Die wichtigsten Urkunden werden vor der Ablage im Urkundenarchiv eingescannt und zusätzlich elektronisch archiviert. Zusätzlich existiert ein Disaster-

Recovery-Gerät. Hierzu gibt es eine Service-Vereinbarung mit der Schleppen AG, Disaster-Recovery vom 12.03.2018 mit der Vertragsnummer DVNZ 006449.

7. Kontrolle der vorgenannten Maßnahmen

Die EDV ist in Abstimmung von Frau Neuhoff-Pongratz und Herrn Fleischmann-Zilian mit dem Datenschutzbeauftragten GDI im Turnus von etwa zwei Jahren auf notwendige Verbesserungen zu überprüfen. Die Datenschutzbeauftragte überprüft sämtliche Abläufe in der Geschäftsstelle laufend während des Geschäftsbetriebs und berichtet dem Notar anlassbezogen, jedenfalls jedoch halbjährlich.

Eine Verschlüsselung des elektronischen Mandantenkontakts ist aus Sicht des Notars nicht erforderlich, aber künftig wünschenswert. Dies scheitert derzeit jedoch an der Akzeptanz der Mandantschaft.

Wuppertal 6.7.2018
(Ort, Datum)


(Unterschrift des Verantwortlichen)

Kleist
Notar
Bankstraße 23
42103 Wuppertal
Telefon: 0201 25 49 00