Andreas Krauß
Hard- und Softwareservice GmbH
Grub 91, 94539 Grafling
Tel.: 0800 / 959 72 99
info@pronotar.de

03. April 2019

Vereinbarung zur Auftragsverarbeitung gemäß Artikel 28 DSGVO

Zwischen

_____

Kanzleiname/Notariat

_____

Straße, Hausnummer, PLZ und Ort

- Verantwortlicher (Auftraggeber) -

und der

Andreas Krauß Hard- und Softwareservice GmbH,
Grub 91, 94539 Grafling

- Auftragsverarbeiter (Auftragnehmer) –

Inhaltsverzeichnis

1. Gegenstand und Dauer der Vereinbarung

a) Gegenstand des Auftrags:

- Installation und Wartung der Software ProNotar;
- Schulungen (Vor Ort und Online) über die Software ProNotar bzw. zur Textintegration;
- Bereitstellung bzw. Einspielung von Patches, Sicherheits- und anderen Programmupdates;
- Telefonischer Service und Kundensupport zur Software ProNotar, in Ausnahmefällen auch zu Produkten von Drittanbietern, u.a. Microsoft Word, Virenscanner, Telefonanlagen, Datev, Lexware;
- Analyse und Fehlerbehebung per Fernwartungsservice;
- Unterstützung von Systembetreuern oder Hardwarelieferanten bei der Einrichtung von Clients und Server;
- Erhebung, Erfassung, Speicherung und Anpassung von Kundendaten zum Zwecke der Dokumentation aller angefallenen Arbeiten bei dem Auftraggeber (Mandantenhistorie);
- Durchführung von Datenbankbackups- oder änderungen;
- Durchführung von teilweisen oder vollständigen Datenwiederherstellungen soweit die Datensicherung über ProNotar erfolgt ist,
- Datenmigration;
- in Ausnahmefällen: Hardware-Inbetriebnahme und Wartung, Austausch von Komponenten an Clients und Servern.

Bei Durchführung des Auftrags kann der Auftragnehmer mit personenbezogenen Daten (Vertrags- Kommunikations- oder Personenstammdaten, Mandantenhistorie, IT-Nutzungsdaten) in Berührung kommen.

b) Dauer des Auftrags:

Die Dauer dieses Auftrags (Laufzeit) entspricht der Laufzeit des zwischen Auftraggeber und Auftragnehmer geschlossenen Softwarepflegevertrages, soweit Komfortmodule des Auftragnehmers betroffen sind, gelten bzgl. deren Laufzeit die Angaben in der entsprechenden Ergänzungsvereinbarung.

2. Konkretisierung des Auftragsinhaltes:

Der Umfang ist in dem Softwarepflegevertrag festgelegt. Sofern Komfortmodule beauftragt sind, gilt ebenso der Umfang der Ergänzung zum Softwarepflegevertrag.
Die Art der Daten ergibt sich aus der Leistungserbringung.
Der Kreis der durch den Umgang mit ihren personenbezogenen Daten im Rahmen dieses Auftrags Betroffenen können Kunden und Angestellte aber auch freie Mitarbeiter des Auftraggebers sein.

3. Technische und organisatorische Maßnahmen

a) Der Auftragnehmer hat die erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung dokumentiert (**Anlage 1**) und dem Auftraggeber übergeben. Diese Anlage ist verbindlicher Bestandteil dieser Vereinbarung.

b) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 l c, 32 DSGVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DSGVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme.

c) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Regelungen zur Berichtigung, Löschung und Sperrung von Daten

a) Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder zu sperren, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.

b) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessen werden, Berichtigung, und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Pflichten des Auftragnehmers

Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern er nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt der Auftragsverarbeiter dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DS-GVO).
Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 - 33 DSGVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S.2b, 29, 32 Abs. 4 DSGVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

b) Die Mitarbeiter des Auftragnehmers werden zudem im Hinblick auf die notarielle Verschwiegenheit verpflichtet. Der Auftragnehmer versichert, dass eine solche Regelung in dem jeweiligen Arbeitsvertrag enthalten ist. Auf die gleichlautende Bestätigung in der dem Auftraggeber bereits vorliegenden Verschwiegenheitsverpflichtungserklärung wird Bezug genommen.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S.2c, 32 DSGVO (**siehe Anlage 1**).

d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in

Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt.

f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

6. Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

a) Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer, durch im Einzelfall zu benennende Prüfer, vorher anzumeldende Stichprobenkontrollen über die Einhaltung dieser Vereinbarung durch den Auftragnehmer durchführen zu lassen.

b) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DSGVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

c) Eine eventuelle Kontrolle durch den Auftraggeber ist kostenlos. Im Falle einer missbräuchlicher Nutzung dieses Angebots (anlasslos hohe Frequenz der Kontrolle) behält sich der Auftragnehmer vor, einen Vergütungsanspruch in Rechnung zu stellen.

d) Die Einhaltung der Anforderungen kann auch durch andere Nachweise erbracht werden, wenn der Auftraggeber diese anerkennt (z.B. Berichte von Aufsichtsbehörden, Zertifikate durch externe Organisationen, interne Auditberichte).

e) Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt und verlangt Korrekturmaßnahmen.

f) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragnehmers vertraulich zu behandeln.

g) Der Auftraggeber ist verpflichtet bei der Nutzung des Ticketsystems des Auftragnehmers auf schriftliche Eingabe von personenbezogenen Daten von Mandanten und anderen Dritten, insbesondere Verwendung von Klarnamen, zu verzichten.

7. Mitteilungspflichten des Auftragnehmers

Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32-36 DSGVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei

Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen zur Verfügung zu stellen

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde

Für Unterstützungsleistungen, die nicht im Softwarepflegevertrag oder einer Ergänzungsvereinbarung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen. Diese Leistung ist nach Zeitaufwand zu bewerten. Je angefangener 6 Minuten wird ein Betrag in Höhe von 6,00 € zuzüglich Umsatzsteuer in Rechnung gestellt.

8. Unterauftragsverhältnisse mit Subunternehmern (Art. 28 Abs. 3 Satz 2 lit. d DS-GVO)

a) Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist dem Auftragnehmer nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DS-GVO, welche auf einem der festgelegten Kommunikationswege mit Ausnahme der mündlichen Gestattung erfolgen muss.

b) Die Zustimmung kann nur erteilt werden, wenn der Auftragnehmer dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss der Auftragnehmer dafür Sorge tragen, dass er den Subunternehmer unter besonderer Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DS-GVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Auftraggeber auf Anfrage zur Verfügung zu stellen.

c) Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

d) Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern.

e) Insbesondere muss der Auftraggeber berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

f) Der Vertrag mit dem Subunternehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DS-GVO). Die Weiterleitung von Daten an den Subunternehmer ist erst zulässig, wenn der Subunternehmer die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DS-GVO bezüglich seiner Beschäftigten erfüllt hat.

g) Der Auftragnehmer hat die Einhaltung der Pflichten des/der Subunternehmer(s) regelmäßig angemessen zu überprüfen: Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.

h) Der Auftragnehmer haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch den Auftragnehmer im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

i) Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Subunternehmer, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DS-GVO).

j) Unterauftragsverhältnisse im Sinne dieses Vertrags sind nur solche Leistungen, die einen direkten Zusammenhang mit der Erbringung der Hauptleistung aufweisen. Nebenleistungen, wie beispielsweise Transport, Wartung und Reinigung sowie die Inanspruchnahme von Telekommunikationsdienstleistungen oder Benutzerservice sind nicht erfasst. Die Pflicht des Auftragnehmers, auch in diesen Fällen die Beachtung von Datenschutz und Datensicherheit sicherzustellen, bleibt unberührt.

9. Weisungsbefugnis des Auftraggebers

a) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

b) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften.

Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags

a) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt.

Hiervon ausgenommen sind Sicherheitskopien, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

b) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

c) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Schlussbestimmungen

a) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich darüber zu informieren.

b) Der Auftragnehmer wird alle in diesem Zusammenhang Verantwortlichen unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber liegen.

c) Mündliche Nebenabreden bestehen nicht.

d) Änderungen oder Ergänzungen dieser Vereinbarung bedürfen zu ihrer Wirksamkeit grundsätzlich der Schriftform. Dies gilt auch für die Aufhebung des Schriftform-Erfordernisses.

e) Sollte eine Bestimmung dieser Vereinbarung unwirksam sein oder werden, so wird sie im übrigen Inhalt nicht berührt. Die unwirksame Bestimmung soll einvernehmlich durch eine solche Bestimmung ersetzt werden, welche der ursprünglichen Absicht der Parteien wirtschaftlich so weit wie möglich gleichkommt.

12. Anlagen

a) Anlage 1: Maßnahmen zur Datensicherheit des Auftragnehmers

(Technische und Organisatorische Maßnahmen der im Auftrag verarbeiteten Informationen)

b) Anlage 2: Wortlaut der Verschwiegenheitsvereinbarung i. S. d. § 26a Abs. 3 BNotO zwischen Auftraggeber und Auftragnehmer

_____, den _____
Ort *Datum*

_____
(Unterschrift des Auftraggebers)

Grafling, den 4. Mai 2019

_____
Andreas Krauß
Geschäftsführer der Andreas Krauß Hard- und Softwareservice GmbH

Anlage 1:

Andreas Krauß
Hard- und Softwareservice GmbH
Grub 91, 94539 Grafling

Tel.: 0800 / 959 72 99
info@pronotar.de

Technische und Organisatorische Maßnahmen der im Auftrag verarbeiteten Informationen

1. Zutrittskontrolle (Kein unbefugter Zutritt zu Datenverarbeitungsanlagen)

Es gibt keine einheitliche Betriebsstätte. Jeder Mitarbeiter arbeitet per Homeoffice in eigenen Räumen. Ein Arbeiten in einem fremden WLAN wird untersagt. Hierfür gilt:

- Die beruflich, von der Andreas Krauß GmbH zur Verfügung gestellte, IT-Ausstattung sowie etwaige dienstliche Unterlagen werden von jedem Mitarbeiter in einem abschließbaren Zimmer aufbewahrt.
- Diese IT besteht aus einem Notebook, sowie eine externe Festplatte, die durch eine Vollverschlüsselung abgesichert Ist. Private Datenträger dürfen nicht verwendet werden.
- Diese IT-Ausstattung darf nicht privat genutzt werden, insbesondere sind berufliche E-Mails nicht auf private E-Mail-Postfächer weiterzuleiten.
- Während einer Fernwartung oder während der Arbeit mit personenbezogenen Daten darf nur autorisiertes Personal Einblick auf den Monitor haben.
  Für jeden PC bzw. Laptop den die Mitarbeiter nutzen, sind das Betriebssystem und alle benutzen Programme jeweils mit einem eigenen Kennwort versehen und auch bei kurzzeitigem Verlassen des Arbeitsplatzes gesperrt bzw. kennwortgeschützt. (Richtlinien zu den benutzten Kennwörtern siehe 2)
- Im Homeoffice erfolgt **keine** Datensicherung.

Sämtliche Daten und Unterlagen, die aus gesetzlichen Gründen länger aufbewahrt werden müssen, werden am Firmensitz in Grafling verwahrt.
Aus diesem Grund gelten für den Firmensitz folgende zusätzliche Schutzvorschriften:

- Schriftliche Unterlagen werden in einem abschließbaren Bereich gelagert.
- Privates WLAN und geschäftliches WLAN sind streng voneinander getrennt.
- Die Sicherung aller relevanten Daten erfolgt verschlüsselt und werden am Firmensitz aufbewahrt. Verschlüsselte Sicherungsdatenträger, die zum Schutz vor Diebstahl oder Feuer außerhalb der Firmenräume gelagert werden sollen, werden ausschließlich im Tresor des Notariats Dr. Hans-Frieder Krauß in München verwahrt.

2. Zugangs- und Zugriffskontrolle (Keine unbefugte Systembenutzung)

Um unbefugten Zugriff auf den Laptop/PC zu vermeiden gilt:

- Es werden sämtliche Sicherheitspatches des Betriebssystems und der Anwendungen installiert. Diese Installation erfolgt soweit möglich automatisch.
- Es wird eine Antivirensoftware mit aktuellen Virensignaturen eingesetzt. Dies kann beispielsweise F-Secure sein.
- Nur Programme, die zur Auftragsabarbeitung benötigt werden, dürfen installiert werden.
- Eine private Nutzung des Systems ist untersagt.
- Defekte oder nicht mehr gebrauchte Hardware wird komplett nach vorherig vorgeschriebenen WipeDisk (Software-Datenlöschung durch Überschreibung mit Patterns) an den Firmensitz geschickt. Hier werden dann die Festplatten nach militärischen Standards 7 mal komplett überschrieben; defekte Festplatten werden physikalisch zerstört.

Der Zugriff auf das System erfolgt kennwortgeschützt. Zur Erzeugung des Kennwortes wird am besten ein Passwortgenerator verwendet. Für das zu verwendende Kennwort gilt folgendes:

- mindestens 12 Zeichen
- enthält Sonderzeichen und Zahlen und unterschiedliche Groß- /Kleinschreibung gemäß Arbeitsanweisung an die Mitarbeiter.
- enthält keine existierenden Wörter oder Namen sowie Geburtsdaten
- Dieses Kennwort darf nicht offen schriftlich in der Nähe des Arbeitsplatzes hinterlegt sein.
- Es darf nicht für andere, private Dienste verwendet werden

Es gibt zwei unterschiedliche Arten von personenbezogenen Daten, mit denen ein Mitarbeiter während der Auftragsbearbeitung in Kontakt kommt:

- Personenbezogene Daten aus dem Bereich des Auftraggebers, also z.B. Mandantendaten- und Rechnungen, Urkundenrolle etc. Diese werden im folgenden Notariatsdaten genannt.
- Auftragsdaten, die zur Abwicklung und Abrechnung des Auftrages erhoben werden müssen. Diese sind vor allem Dokumentation über das gemeldete Problem, ergriffene Maßnahmen und dafür verbrauchte Arbeitszeiten. Dieses werden im folgenden Auftragsdaten genannt.

Diese beiden Datenarten werden auf unterschiedliche Weise geschützt.

Für die Notariatsdaten mit personenbezogenen Inhalten gilt:

- Der Zugriff auf die IT des Notariats erfolgt mit dem professionellen Fernwartungstool. Die Verbindung hierbei ist verschlüsselt. Dies kann z.B. „TeamViewer“ sein.
- Notariatsdaten werden nur auf das eigene System geladen, wenn es für die Fehlersuche oder Auftragsabwicklung unerlässlich ist. Diese Daten werden ausschließlich auf der externen Festplatte gespeichert, die einen z.B. mit „VeraCrypt“ erzeugten Datencontainer enthält.
- Ein Speichern auf einem unverschlüsselten Datenträger ist nicht erlaubt. Müssen diese Daten während der Auftragsbearbeitung übertragen werden, so erfolgt dies AES256-verschlüsselt.
- Nach der Auftragsbearbeitung werden diese Daten unverzüglich gelöscht.
- Es erfolgt keine Datensicherung. Kommt es zu einem Datenverlust, so können diese Daten erneut aus dem Notariat heruntergeladen werden.
- Lediglich Daten aus dem Notariat, die keine personenbezogenen Daten enthalten, also z.B. Musterverträge und Vorlagen, Textbausteine ohne Personendaten etc. dürfen auf der lokalen Festplatte gespeichert werden.

Für die Auftragsdaten gilt:

- Die Auftragsdaten werden auf einem zentralen Server gespeichert. Dieser wird in Deutschland gehostet.
- Der Zugriff erfolgt kennwortgeschützt (Kennwort: siehe oben). Nach längerer Inaktivität wird die Verbindung automatisch getrennt.
- Sämtlicher Zugriff auf diesen Server erfolgt Ende-zu-Ende verschlüsselt. Ein Abhören (Man in the Middle) ist dadurch nicht möglich
- Notariatsdaten werden ausschließlich lokal und nicht auf diesem Server gespeichert.

3. Weitergabekontrolle (Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung)

Die Datenübertragung zum Notariat erfolgt ausschließlich mit „TeamViewer“ oder ähnlicher Fernwartungssoftware, also verschlüsselt. Notariatsdaten werden lokal auf einem verschlüsselten Datenträger gespeichert. Werden diese Daten zwischen den Heimarbeitsplätzen weitergereicht, so sind diese Daten mit einer AES256 – Verschlüsselung zu schützen. Das Passwort hierfür wurde durch einen anderen Kanal mitgeteilt, also z.B. fernmündlich. Die Speicherung der Daten wird ausschließlich auf dem dafür vorgesehenen System durchgeführt. Jeglicher administrative Zugriff erfolgt auf Basis der Zugangs- und Zugriffskontrolle.

4. Eingabekontrolle (Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme bearbeitet wurden)

Die Verarbeitung, Nutzung und Speicherung von personenbezogenen Daten ist nur bestimmten, dafür vorgesehenen Personen möglich.

5. Auftragskontrolle

Die Auftragskontrolle wird im Sinne des §11 BDSG/Art. 28 DSGVO durchgeführt. Hierzu ist sichergestellt, dass personenbezogene Daten nur entsprechend den Weisungen des Kunden und zu Abrechnungszwecken verarbeitet werden können. Weisungen können über die unterschiedlichen Kommunikationsmöglichkeiten eingehen, z.B. E-Mail, Eintragung eines Tickets, fernmündlich.

6. Verfügbarkeitskontrolle (Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust)

Die Verfügbarkeitskontrolle wird anhand einer Netzwerküberwachung sichergestellt. Notariatsdaten werden nicht gesichert. Daten, die aus gesetzlichen/steuerlichen Gründen gespeichert werden müssen, werden ausschließlich am Firmensitz gesichert. Zum Schutz vor Zerstörung oder Verlust erfolgt im Notariat Dr. Hans- Frieder Krauß in München die Unterbringung eines aktuelles Backups.

Anlage 2:

Andreas Krauß
Hard- und Softwareservice GmbH
Grub 91, 94539 Grafling

Tel.: 0800 / 959 72 99
info@pronotar.de

Verschwiegenheitsvereinbarung i. S. d. § 26a Abs. 3 BNotO

Die **Andreas Krauß Hard- und Softwareservice GmbH**, in 94539 Grafling *- nachstehend „Dienstleister" genannt –*

und ***der Notar/die Notarin*** _____**,** in _____ *- nachstehend „Notar" genannt -*

treffen folgende Verschwiegenheitsvereinbarung hinsichtlich der in dem vorgenannten Notariat unter der Bezeichnung „**Pro-Notar**" eingesetzten notarspezifischen Fachanwendungen:

Der Notar hat den Dienstleister mit der Erbringung von Dienstleistungen im Sinne des § 26a BNotO beauftragt (die ***Dienstleistungen***). In diesem Zusammenhang wird der Notar dem Dienstleister, soweit dies zur Inanspruchnahme der Dienstleistungen erforderlich ist, den Zugang zu Tatsachen eröffnen, auf die sich die Verpflichtung des Notars zur Verschwiegenheit nach § 18 BNotO bezieht.

1. Der Dienstleister ist zur Verschwiegenheit über alle Tatsachen verpflichtet, die dem Notar bei Ausübung seines Amtes bekannt geworden sind und zu denen der Notar ihm den Zugang eröffnet hat. Dies gilt nicht für Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Er ist ferner verpflichtet, sich nur insoweit Kenntnis von fremden Geheimnissen zu verschaffen, als dies zur Vertragserfüllung erforderlich ist.
2. Der Dienstleister ist verpflichtet, von ihm beschäftigte Personen, die er zur Vertragserfüllung heranzieht, in schriftlicher Form zur Verschwiegenheit zu verpflichten. Der Dienstleister versichert, dass eine solche Regelung in dem jeweiligen Arbeitsvertrag enthalten ist.
3. Der Dienstleister ist befugt, weitere Personen zur Vertragserfüllung heranzuziehen. In diesem Fall ist der Dienstleister verpflichtet, auch diese Personen in schriftlicher Form zur Verschwiegenheit zu verpflichten.
4. Auf die strafrechtlichen Folgen der Verletzung dieser Pflichten wurde hingewiesen, insbesondere auf §§ 203 und 204 Strafgesetzbuch. Dem Dienstleister ist bekannt, dass diese Strafvorschrift auch für ihn und seine Mitarbeiter gilt.
5. Die Vorschriften über den Schutz personenbezogener Daten bleiben hiervon unberührt.
6. Grundsätzlich speichert der Dienstleister keine Notariatsdaten. Wenn in Ausnahmefällen sich Daten bei dem Dienstleister befinden, werden diese sofort nach Beendigung der Arbeiten unverzüglich an den Notar zurückgegeben oder physikalisch gelöscht.
7. Der Dienstleister nimmt in der Regel die Arbeiten in dem Notariat über eine Fernwartung vor. Deren Aktivierung wird generell seitens der Notariate vorgenommen. In der Regel erfolgt die Fernwartung über das Programm „TeamViewer" oder ähnlicher Fernwartungssoftware. Die Fernwartung kann während einer Servicetätigkeit jederzeit durch das Notariat abgebrochen werden. Die Notare oder ihre Mitarbeiter haben die Möglichkeit, die Wartungsarbeiten über die Onlineverbindung von ihren Bildschirmen aus zu verfolgen.

_____, den _____
Ort *Datum*

_____
(Unterschrift Notar/in bzw. Notariatsverwalter/in)

Grafling, den 4. Mai 2019

_____
Andreas Krauß
Geschäftsführer der Andreas Krauß Hard- und Softwareservice GmbH