V E R T R A G

A U F T R A G S V E R A R B E I T U N G

M A N D A N T E N P O R T A L

Zwischen

dem **Nutzer** (Vertragspartner des Hauptvertrages)

- nachstehend „**Auftraggeber“** genannt –

und

Bundesnotarkammer
Anton-Wilhelm-Amo-Straße 34
10117 Berlin

- nachstehend „**Auftragnehmerin“** genannt –

- nachstehend gemeinsam „**Parteien“** genannt -

wird Folgendes vereinbart:

§ 1 Gegenstand und Dauer der Vereinbarung

(1) Das Mandantenportal („**die Anwendung**“) ermöglicht potentiellen Mandanten des Auftraggebers, die Kontaktaufnahme über Formulare, die dem Auftraggeber die Mandatsanbahnung erleichtern sollen. Die Anwendung wird im Rahmen der von der Auftragnehmerin entwickelten und von der NotarNet GmbH vertriebenen Software XNP (Modul Mandantenportal) verwendet. Die Parteien haben hierzu eine Vereinbarung in Form von Allgemeinen Geschäftsbedingungen („**Hauptvertrag**“) geschlossen.

(2) Auch wenn der Auftraggeber für die von ihm in die Anwendung eingetragenen personenbezogenen Daten i.S.d. § 4 Nr. 7 Europäischen Datenschutzgrundverordnung („**DS-GVO**“) selbst verantwortlich bleibt, verarbeitet die Auftragnehmerin Informationen und personenbezogene Daten des Auftraggebers sowie dessen potentieller Mandanten im Rahmen des Betriebs sowie der Wartung und Pflege der Anwendung. Die Auftragnehmerin verarbeitet daher personenbezogene Daten für den Auftraggeber im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages.

(3) Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedstaat der Europäischen Union oder in einem Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erbracht. Jede Verlagerung der Dienstleistung oder von Teilarbeiten dazu in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

(4) Die Laufzeit richtet sich nach der Laufzeit des Hauptvertrags.

§ 2 Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

(1) Die personenbezogenen Daten, die einer Verarbeitung durch die Auftragnehmerin unterliegen können, sind sämtliche Daten, die im Rahmen der Nutzung der Anwendung durch den Auftraggeber oder dessen potentielle Mandanten eingegeben werden, sowie ggf. zusätzliche Informationen, die beispielsweise in Störungsmeldungen übermittelt werden. Ein Zugriff auf diese Daten kann für den Betrieb und Verbesserungen des Systems und Mängelbeseitigung sowie für die Wartung und Pflege des Systems nicht ausgeschlossen werden. Die Anwendung ist jedoch so gestaltet, dass im regulären Betrieb ein Zugriff des Auftragnehmers auf diese Daten nicht stattfindet. Die Daten werden durch besondere Maßnahmen (VPD, Database Vault) gesichert in den Systemen der Auftragnehmerin abgelegt.

(2) Im Rahmen der Nutzung der Anwendung werden insbesondere solche personenbezogenen Daten eingegeben, die im Rahmen der Mandatsanbahnung über das Mandantenportal von potentiellen Mandanten in den bereitgestellten Formularen eingegeben und übermittelt werden. Das sind insbesondere:
    - Stammdaten, Namen, Adressen, Kontaktdaten (E-Mail-Adresse, Telefonnummer etc., Geburtsdaten, Beruf, Staatsangehörigkeit, etc.);
    - Daten zu familiären Verhältnissen (Familienstand, Verwandtschaftsverhältnisse, Stammdaten der Familienangehörigen, Angaben zu Beziehungsverhältnissen, etc.)
    - Finanzdaten (Steueridentifikationsnummer, Bankdaten, Vermögenswerte, Nachlassinformationen, etc.)
    - Zugehörigkeit zu einer Religionsgemeinschaft
    - personenbezogene Daten aus laufenden oder anstehenden Behördenverfahren;
    - personenbezogene Daten aus sich anbahnenden oder geschlossenen Verträgen;
    - sonstige personenbezogene Daten, die mit der Anbahnung von Mandatsbeziehungen zwischen Mandant und Notar verbunden sind.

(3) Von der Auftragsverarbeitung sind insbesondere folgende Personenkategorien betroffen:
    - Mandanten und potentielle Mandanten des Auftraggebers,
    - Dritte, die in irgendeiner Weise am betreffenden rechtlichen Sachverhalt beteiligt sind und/oder vom potentiellen Mandanten benannt werden.

§ 3 Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

(1) Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DS-GVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DS-GVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist die Auftragnehmerin verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Auftraggeber gerichtet sind, unverzüglich an diesen weiterzuleiten. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmerin abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

(2) Der Auftraggeber hat vor Beginn der Arbeiten sicherzustellen, dass die Auftragnehmerin personenbezogene Daten nur zur Kenntnis nehmen kann, soweit dies unvermeidlich ist. Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

(3) Der Auftraggeber ist berechtigt, sich wie unter § 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der bei der Auftragnehmerin getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

(4) Der Auftraggeber ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der Auftragnehmerin vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

§ 4 Weisungsberechtigte des Auftraggebers, Weisungsempfänger der Auftragnehmerin

Weisungsberechtigt sind der Auftraggeber selbst sowie gegebenenfalls ein amtlich bestellter Vertreter. Weisungsempfänger sind der IT-Geschäftsführer, der CDO der Auftragnehmerin sowie der Projektleiter der Anwendung. Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind dem Vertragspartner unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen.

§ 5 Pflichten der Auftragnehmerin

(1) Die Auftragnehmerin verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Auftraggebers, sofern sie nicht zu einer anderen Verarbeitung durch das Recht der Europäischen Union oder der Mitgliedstaaten, dem die Auftragnehmerin unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt die Auftragnehmerin 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).

(2) Die Auftragnehmerin verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt, sofern es sich nicht um im Cache zwischengespeicherte oder automatisierte Datensicherungen zum Zweck der Meidung eines Datenverlustes bei der Auftragnehmerin handelt, für deren Behandlung diese Vereinbarung gleichermaßen gilt.

(3) Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DS-GVO durch den Auftraggeber an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat die Auftragnehmerin im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. e und f DS-GVO).

(4) Die Auftragnehmerin wird den Auftraggeber unverzüglich darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DS-GVO). Die Auftragnehmerin ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.

(5) Die Auftragnehmerin wird dem Auftraggeber zuzuordnende personenbezogene Daten unverzüglich nach Erledigung des jeweiligen Auftrags zu löschen. Die Dokumentation der Maßnahme ist zum Zweck der Datenschutzkontrolle drei Jahre aufzubewahren. Im Übrigen hat die Auftragnehmerin personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen der Auftragnehmerin dem nicht entgegenstehen.

(6) Die Auftragnehmerin erklärt sich damit einverstanden, dass der Auftraggeber – grundsätzlich nach Terminvereinbarung – berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Auftraggeber beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DS-GVO). Die Auftragnehmerin sichert zu, dass sie, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

(7) Die Auftragnehmerin verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Auftraggebers die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort. Die Auftragnehmerin ist gesetzlich gemäß §§ 69a iVm 81a BNotO zur Verschwiegenheit verpflichtet.

(8) Die Auftragnehmerin sichert zu, dass die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter die notwendige fachliche Qualifikation und Zuverlässigkeit aufweisen, insbesondere, dass sie sie vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit, wie auch nach Beendigung des Beschäftigungsverhältnisses, in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DS-GVO).

(9) Die Auftragnehmerin überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in ihrem Betrieb und hat einen Datenschutzbeauftragten bestellt. Dieser ist wie folgt erreichbar:

Bundesnotarkammer
Datenschutzbeauftragter
Anton-Wilhelm-Amo-Straße 34
10117 Berlin
Telefon: +49 30 - 38 38 66-0
Telefax: +49 30 - 38 38 66-66
E-Mail: datenschutz@bnotk.de

§ 6 Mitteilungspflichten der Auftragnehmerin bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Die Auftragnehmerin teilt dem Auftraggeber unverzüglich Störungen, Verstöße der Auftragnehmerin oder der bei ihr beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Auftraggebers nach Art. 33 und Art. 34 DS-GVO und ggf. der Datenschutzfolgeabschätzung nach Art. 35 DS-GVO. Die Auftragnehmerin sichert zu, den Auftraggeber erforderlichenfalls bei seinen Pflichten nach Art. 33 und 34 DS-GVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DS-GVO). Meldungen nach Art. 33 oder 34 DS-GVO für den Auftraggeber darf die Auftragnehmerin nur nach vorheriger Weisung gemäß § 4 dieses Vertrages durchführen.

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

(1) Die Beauftragung von Subunternehmern zur Verarbeitung von Daten des Auftraggebers ist der Auftragnehmerin nur mit Genehmigung des Auftraggebers gestattet, Art. 28 Abs. 2 DS-GVO, welche auf einem der o. g. Kommunikationswege (§ 4) mit Ausnahme der mündlichen Gestattung

erfolgen muss. Die Zustimmung kann nur erteilt werden, wenn die Auftragnehmerin dem Auftraggeber Namen und Anschrift sowie die vorgesehene Tätigkeit des Subunternehmers mitteilt. Außerdem muss die Auftragnehmerin dafür Sorge tragen, dass sie 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.

(2) Die Auftragnehmerin bemüht sich, die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmerin auch gegenüber Subunternehmern festzulegen. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten der Auftragnehmerin und des Subunternehmers deutlich voneinander abgegrenzt werden. Werden mehrere Subunternehmer eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern.

(3) 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).

(4) 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.

(5) Die Westernacher Solutions GmbH sowie deren Tochtergesellschaft Justin LegalTech GmbH, beide mit Sitz in Columbiadamm 37, 10965 Berlin unterstützen die Auftragnehmerin bei der Entwicklung der Anwendung und bei Verbesserungen, Mängelbeseitigung und Wartung/Pflege. Es kann hierbei nicht ausgeschlossen werden, dass im Rahmen dieser Beauftragung auf personenbezogene Daten zugegriffen werden kann. Die Auftragnehmerin und die Westernacher Solutions GmbH sowie deren Tochtergesellschaft Justin LegalTech GmbH haben eine Vereinbarung zur Auftragsverarbeitung abgeschlossen sowie eine Verpflichtung zur Verschwiegenheit im Sinne des § 26a BNotO. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

(6) Die Anwendung wird auf der Microsoft Azure Cloud betrieben. Der Auftraggeber stimmt bereits jetzt dem Einsatz von Microsoft Ireland Operations Ltd., One Microsoft Place, South County Business Parl, Leopardstown, Dublin 18, D18 P521, Ireland („Microsoft“), zu. Microsoft und die Auftragnehmerin habe eine Vereinbarung zur Auftragsverarbeitung abgeschlossen sowie eine Verpflichtung zur Verschwiegenheit im Sinne des § 26a BNotO. Daten im Zusammenhang mit der Anwendung werden von Microsoft nur innerhalb des Europäischen Wirtschaftsraums verarbeitet. Mit der Beauftragung von Microsoft erklärt sich der Auftraggeber einverstanden.

(7) Die Auftragnehmerin informiert den Auftraggeber 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 innerhalb von zwei (2) Wochen nach Eingang der Information zu erheben (§ 28 Abs. 2 Satz 2 DS-GVO). Erfolgt kein Einspruch innerhalb der Frist, gilt die Zustimmung zur Änderung als gegeben. Legt der Auftraggeber fristgerecht Einspruch ein und ist eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich, wird dem Auftraggeber ein Sonderkündigungsrecht eingeräumt.

§ 8 Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO (Art. 28 Abs. 3 Satz 2 lit. c DS-GVO)

(1) Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DS-GVO, wie Vertraulichkeit, Integrität und

Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

(2) Das in der **Anlage** beschriebene Datenschutzkonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT-Systeme und Verarbeitungsprozesse bei der Auftragnehmerin dar.

(3) Die Auftragnehmerin hat bei gegebenem Anlass, mindestens aber jährlich, eine Überprüfung, Bewertung und Evaluation der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung durchzuführen (Art. 32 Abs. 1 lit. d DS-GVO). Die Maßnahmen bei der Auftragnehmerin können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.

(4) Wesentliche Änderungen muss die Auftragnehmerin mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

§ 9 Verpflichtungen der Auftragnehmerin nach Beendigung des Auftrags (Art. 28 Abs. 3 Satz 2 lit. g DS-GVO)

Nach Abschluss der vertraglichen Arbeiten hat die Auftragnehmerin sämtliche in ihren Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber herauszugeben oder datenschutzgerecht zu löschen bzw. zu vernichten/vernichten zu lassen.

§ 10 Haftung

Es gelten die Regelungen des Hauptvertrags.

§ 11 Schlussbestimmungen

(1) Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Parteien für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

(2) Es gilt das Recht der Bundesrepublik Deutschland. Erfüllungsort und Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit diesem Vertrag ist, soweit der Auftraggeber die Voraussetzungen des § 38 ZPO erfüllt, Berlin.

(3) Sollten einzelne Bestimmungen dieses Vertrags unwirksam sein, berührt dies die Gültigkeit der übrigen Bestimmungen grundsätzlich nicht. Die Parteien werden sich bemühen, anstelle der unwirksamen Bestimmungen eine solche zu finden, die dem Vertragsziel rechtlich und wirtschaftlich am ehesten gerecht wird. Das gleiche gilt entsprechend für den Fall einer Vertragslücke.

Anlage – Technische und organisatorische Maßnahmen

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

1.1. Zutrittskontrolle

Bei der Zutrittskontrolle sind in Verbindung mit dem Mandantenportal die Zutrittskontrolle des Microsoft Azure Cloudrechenzentrum und die Betriebsflächen der Bundesnotarkammer, von denen aus das Mandantenportal administriert wird, zu unterschieden.

Das Schutzniveau der in Deutschland gehosteten Azure-Cloud wurde von der Bundesnotarkammer durch Konditionsverträge abgesichert, auf die sich das Bundesministerium des Innern und Microsoft im Februar 2025 geeinigt haben. Mit den sog. Konditionenverträgen werden die Standardvertragsbedingungen von Microsoft partiell an die Bedürfnisse der öffentlichen Hand in der Bundesrepublik Deutschland bei der Beschaffung von Microsoft-Produkten angepasst.

Die Zutrittskontrollen basieren auf mehreren internationalen Normen und Standards ISO/IEC 27001, ISO/IEC 27018 und SOC 2 Typ II. Zusätzlich wurden folgende Zusatzvereinbarungen geschlossen, die sicherstellen, dass Daten nicht in ein anderes Rechenzentrum verschoben werden, welches nicht DSGVO konform ist und nicht dem vereinbarten hohen Schutzniveau entspricht:

- Zusatzvereinbarung ID M471 – Konzernbeitritt Datenschutznachtrag für Produkte und Services von Microsoft
- Zusatzvereinbarung ID M657 - Enterprise Enrollment Deutsches Datengeheimnis

Folgende Quellen bieten umfangreiche weitere Informationen zu den implementierten Maßnahmen seitens Microsoft:

- https://learn.microsoft.com/de-de/azure/security/fundamentals/physical-security
- https://azure.microsoft.com/de-de/explore/trusted-cloud/
- https://docs.microsoft.com/de-de/azure/compliance/

Die Betriebsflächen der Bundesnotarkammer sind wie folgt gesichert:

- Überwachung und Alarmsicherung der Eingänge zu den Büroflächen zu festgelegten Zeiten
- Überwachung und Alarmsicherung der Eingänge zu den Sicherheitsbereichen
- Separate Sicherheitsbereiche sind durch eine Zutrittskontrolle mit Zwei-Faktor-Authentifizierung (Token + PIN) geschützt.
- Dokumentation von Zutritten in den Sicherheitsbereichen
- Die IT-Räume sind separiert und verschlossen und nur durch Berechtigte zugänglich

1.2. Zugangskontrolle

Die Registrierung und Anmeldung zum Mandantenportal erfolgt über XNP. Die Zugangskontrollen zu XNP sind in der AVV zu XNP geregelt.

Der Zugriff auf die in Microsoft Azure betriebene Infrastruktur ist nur über gesicherte Wege sowie Multi-Faktor-Authentifizierung und von bestimmten IP-Adressen möglich.

Der Zugang zu Datenverarbeitungskomponenten (PC, Server, Netzkomponenten) erfolgt durch Berechtigungsvergabe und Authentifizierung in allen Systemen. Die Zugangsregelungen umfassen folgende Maßnahmen:

- Identifikation und Authentifizierung
  - mit Hardwaretoken
  - mit Benutzername und Passwort
  - auf Basis von Zertifikaten
- Vergabe von Benutzernamen und Passwort
- Zuordnung von Benutzerprofilen und -rechten
- Einsatz von VPN-Technologie zum sicheren Fernzugriff
- Automatische Bildschirmsperre
- Verschlüsselung von Datenträgern
- Regelmäßige Implementierung von Sicherheits-Updates

Zusätzlich werden die Anwendungen über eine Multi-Faktor-Authentifizierung geschützt. Die Passwortwahl ist in konkreten Arbeitsanweisungen für die Bundesnotarkammer Mitarbeiter geregelt. Die Weitergabe von persönlichen Zugangsdaten oder -mitteln ist untersagt.

1.3. Zugriffskontrolle

Die Zugriffskontrolle auf das Mandantenportal erfolgt auf Basis eines rollenbasierten Benutzerkonzeptes.

Der Zugriff auf die Azure -Cloud erfolgt nur im Rahmen der Kontrolle von dedizierten IT-Administratoren der Bundesnotarkammer.

Generell stellt die Bundesnotarkammer mit ihren Berechtigungskonzepten in den IT-Systemen sicher, dass keine unbefugten Zugriffe auf Systeme und Daten erfolgen.

In dem Rahmen der Zugriffskontrolle sind folgende Maßnahmen umgesetzt:

- Vergabe von Benutzernamen und Passwort
- Einsatz eines rollenbasierten Benutzer-Berechtigungskonzepts
- Zugriffsberechtigung erfolgt immer nach dem Prinzip der restriktiven Rechtevergabe
- Administratoren sind qualifiziert und auf Zuverlässigkeit geprüft

- Protokollierung von Zugriffen
- Zertifikatsbasierte Zugriffsberechtigung (Zwei-Faktor-Authentifizierung)
- Sichere Aufbewahrung und fachgerechte Entsorgung von Datenträgern

1.4. Trennungskontrolle

Die Trennung von verschiedenen datenverarbeitenden Systemen wird grundsätzlich eingeplant und umgesetzt. Es erfolgt eine getrennte Verarbeitung von Daten, die zu unterschiedlichen Zwecken erhoben wurden.

Es kommen folgende Maßnahmen zum Einsatz:

- Physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern
- Zur Sicherstellung des Produktivbetriebs sind Test- und Entwicklungssysteme vollständig von den Produktivsystemen getrennt.
- Vergabe von Benutzerrechten auf Basis eines Berechtigungskonzepts

Im Mandantenportals ist eine effektive Mandantentrennung implementiert. Programmatisch ist diese durch die Verwendung eines Mehrschlüssel-Systems umgesetzt.

Die Mandantendaten werden final in einer Datenbank abgespeichert, welche sich nicht in der Azure-Cloud befindet, sondern in einem lokalen, hochsicheren Rechenzentrum der Bundesnotarkammer.

1.5. Maßnahmen zur Verschlüsselung der Daten

Ziel der Maßnahmen zur Verschlüsselung von personenbezogenen Daten ist, die Inhalte von Datenbanken vor unerlaubter Einsicht und Veränderung zu schützen.

Es werden folgende Verschlüsselungstechniken eingesetzt:

- Verschlüsselter Transport
- Festplattenverschlüsselung
- Einsatz von VPN-Technologie zum sicheren Fernzugriff

Die jeweilige Verschlüsslung entspricht jeweils dem Stand der Technik.

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

2.1. Weitergabekontrolle

Die Datenübertragung sensibler Daten zwischen der Bundesnotarkammer und den Beteiligten erfolgt verschlüsselt.

Weitere Maßnahmen:

- Verschlüsselter Transport
- Verschlüsselung von Datenträgern
- Einsatz von Firewalls und Intrusion Detection Systemen
- Einsatz von Anti-Viren-Software

Des weiteren führt Microsoft Aufzeichnungen über ein- und ausgehenden Medien, die Kundendaten oder Professional Services-Daten erhalten, einschließlich der Art der Medien, des zugelassenen Absenders/Empfängers, des Datums und der Uhrzeit, der Anzahl der Medien und der darin enthaltenen Arten von solche Daten.

2.2. Eingabekontrolle

Zum Schutz vor Angriffen durch schädliche Benutzereingaben, wie z.B. Code-Injections, wurde die Eingabeschnittstelle des Mandantenportals durch effektive Mechanismen abgesichert, insbesondere durch die Verwendung von Entity Framework und EF Core.

Bei der Bundesnotarkammer sind sämtliche Protokollierungseinrichtungen und Protokollinformationen vor Manipulation und unbefugtem Zugriff geschützt.

So sind folgende Maßnahmen umgesetzt:

- Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts
- Protokollierung der Eingabe, Änderung und Löschung von Daten

In Verbindung mit dem Mandantenportal werden Aktivitäten von IT-Admins und Benutzern protokolliert. Die Verwendung von mobilen Datenträgern ist untersagt.

Im Mandantenportal kommt eine KI basierte Suche zum Einsatz. Es wird hierbei ein KI-Modell in einer eigenen Instanz genutzt, welche nicht mit dem Internet verbunden ist. Durch zusätzliche Vereinbarungen mit Microsoft wird zusätzlich verhindert, dass Mitarbeiter von Microsoft die Chats einsehen oder weiterverwenden dürfen.

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

3.1. Verfügbarkeitskontrolle

Die Bundesnotarkammer verfügt über Maßnahmen, um einen ordnungsgemäßen und sicheren Betrieb der IT-Systeme sicherzustellen.

Diese umfassen u. a. die fortlaufende Überwachung der Kapazitäten und Ressourcen, um einerseits die Verfügbarkeit der erforderlichen Systemleistung sicherzustellen und andererseits für die Überwachung der Integrität und Zuverlässigkeit der Systeme zu sorgen. Zu den überwachten Parametern gehören:

- Status und Speicherauslastung der Festplatten und weiterer Speichersysteme
- Speicher- und CPU-Auslastung der Server
- Status und Erreichbarkeit aller Server und virtuellen Maschinen
- Auslastung der Netzwerksegmente, Firewalls, Router und Switches
- Verfügbarkeit der Applikationsserver und der bereitgestellten Dienste
- Verfügbarkeit der Kommunikationsserver
- Status der Backups
- Unterbrechungsfreie Stromversorgung
- Klimaanlage in Serverräumen
- Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen
- Feuer- und Rauchmeldeanlagen
- Feuerlöschanlage in Serverräumen
- Alarmmeldung bei unberechtigten Zutritten zu Sicherheitsbereichen
- Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort

Die Azure-Cloud wird von der Bundesnotarkammer bezüglich der Verfügbarkeit und Ressourcenauslastung aktiv überwacht. Weitere Informationen zur Kontrolle der werden von Microsoft dargelegt unter: https://learn.microsoft.com/de-de/azure/security/fundamentals/infrastructure-availability

3.2. Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO)

Im Rahmen der Informationssicherheit wird die vorgesehene Verfügbarkeit von Systemen eigens bewertet und dokumentiert. Aus den Anforderungen werden die technischen und organisatorischen Vorgaben, wie beispielsweise redundante Systeme sowie Anbindungen oder entsprechende Planungen, abgeleitet.

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO)

4.1 Datenschutz-Management

Die Bundesnotarkammer hat verantwortliche Personen für den Datenschutz und die Informationssicherheit berufen.

Alle Mitarbeiter sind nach dem Verpflichtungsgesetz besonders verpflichtet und auf das Datengeheimnis und die Einhaltung von Betriebs- und Geschäftsgeheimnissen besonders hingewiesen und sind gemäß DS-GVO, Artikel 29 und 32 (4), angewiesen, personenbezogene Daten nur auf Anweisung zu verarbeiten.

Datenschutzvorfälle werden dokumentiert, behandelt und den Auftraggebern und ggf. den relevanten Behörden gemeldet.

In den von uns verantworteten Projekten ist Datenschutz und Informationssicherheit Bestandteil aller Phasen unserer angewandten Projektmethodik. Der Grundsatz der Datenminimierung gehört zu den wesentlichen Richtungsentscheidungen in der Entwicklung der Produkte der Bundesnotarkammer.

4.2. Sicherheits- und Risikomanagement

Die Bundesnotarkammer ist in den Rahmen eines Informationssicherheitsmanagements eingebettet. Dieses beinhaltet unter anderem schriftlich dokumentierte Richtlinien, Prozesse und Handbücher zum IT-/ Rechenzentrumsbetrieb. Die eingesetzten Sicherheitsverfahren werden laufend überprüft.

Die Bundesnotarkammer pflegt und verbessert ein Risikomanagement, das sowohl die operativen Risiken und jene in Projekten berücksichtigt. Darüber hinaus existiert ein IT-Sicherheitsrisikomanagement, welches sich mit den prozessualen, dienstleistungs- und standortbezogenen Risiken beschäftigt.

4.3. Audits und Sicherheitstests

Teile der Bundesnotarkammer unterliegen regelmäßigen Konformitätsbewertungen durch externe Überwachungsstellen. Darüber hinaus finden regelmäßige Penetrations- und Schwachstellenscans statt.

4.4. Störungsmanagement

Störungsereignisse werden von der Bundesnotarkammer nach standardmäßigen und toolgestützten Prozessen bearbeitet, um möglichst zeitnah einen störungsfreien Betrieb zu gewährleisten. Störungsbedingte Sicherheitsvorfälle werden von der Bundesnotarkammer

zeitnah überwacht, analysiert und behoben.

4.5. Datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO)

Bei der Entwicklung von Verarbeitungsvorgängen des Mandantenportals werden geeignete technische Maßnahmen implementiert, um die geplanten Verarbeitungsvorgänge datenschutzkonform zu gestalten. Des Weiteren werden beispielsweise durch entsprechende Voreinstellungen, bei denen die Software nur die nötigsten Daten sammelt, Maßnahmen getroffen, um die Anforderung Privacy by Default einzuhalten.

Generell wird bei Anwendungen der Bundesnotarkammer dafür gesorgt, dass datenschutzfreundliche Voreinstellungen („Privacy-by-Design and Privacy-by-Default“) einer unrechtmäßigen Verarbeitung oder den Missbrauch von Daten präventiv entgegengewirkt wird. Über angemessene technische Voreinstellungen soll sichergestellt werden, dass grundsätzlich nur die personenbezogenen Daten erhoben und verarbeitet werden, die für den konkreten Zweck auch tatsächlich erforderlich sind („Need-to-Know“-Prinzip).

Um eine möglichst risikoarme Verarbeitung personenbezogener Daten zu erreichen, werden u. a. folgende Schutzmaßnahmen umgesetzt:

- Umfang der personenbezogenen Daten minimieren
- Frühestmögliche Pseudonymisierung, Anonymisierung, Löschung oder Verschlüsselung der Daten
- Schaffung von Transparenz in Bezug auf die Funktionen und die Verarbeitung der Daten
- Beschränkung der Zugriffsmöglichkeiten auf Daten
- Voreinstellung vorhandener Konfigurationsmöglichkeiten auf die datenschutzfreundlichsten Werte

4.6. Auftragskontrolle

Die Bundesnotarkammer verarbeitet personenbezogene Daten des Auftraggebers ausschließlich im vertraglich festgelegten Rahmen sowie auf Weisung des Auftraggebers.

Hierbei setzt die Bundesnotarkammer auch die in Anlage 2 aufgeführten Unterauftragsverarbeiter ein. Im Falle eines Auftragsverarbeitungsverhältnisses hat die Bundesnotarkammer mit dem jeweiligen Vertragspartner einen Auftragsverarbeitungsvertrag abgeschlossen, der zwingend den gem. Art. 28 Abs. 3 DSGVO erforderlichen Regelungsgehalt aufweist. Unterauftragnehmer der Bundesnotarkammer erhalten nur Zugriff auf die Systeme des Auftraggebers, sofern der Auftraggeber vorab diesen Zugriff selbst gewährt bzw. durch die Bundesnotarkammer gewähren lässt. Sie werden regelmäßig zur Vorlage aktueller Prüfnachweise bezüglich ihrer vertraglichen Pflichten aufgefordert und im Fall der Verarbeitung von Mandantendaten von der Auftragnehmerin zusätzlich zur Verschwiegenheit

verpflichtet, § 43e Abs. 3 BRAO / § 26a Abs. 3 BNotO.

Die Bundesnotarkammer arbeitet nur mit (Unter-)Auftragnehmern zusammen, die die Sicherheit der personenbezogenen Daten garantieren können. Dies bemisst sich nach den von dem jeweiligen Unterauftragnehmer getroffenen technischen und organisatorischen Maßnahmen.

Bei der Bundesnotarkammer erfolgt die Auftragsverarbeitung im Sinne von Art. 28 DS-GVO nicht ohne entsprechende Weisung des Auftraggebers, z.B. durch einen gesetzlichen Auftrag, durch eine eindeutige Vertragsgestaltung, etc.

Folgende Maßnahmen sichern die Auftragskontrolle:

- Alle Aktivitäten der Bundesnotarkammer werden durch Auftrag/Weisung des Auftraggebers initiiert
- Dokumentation von Auftrag/Weisung durch den Auftraggeber
- Laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten
- Regelmäßige Beauftragung von Sicherheitsaudits

4.7 Azure und Azure OpenAI Services (u.a. ChatGPT)

Die Nutzung von ChatGPT erfolgt als Teil des Services von Microsoft Azure. Das Mandantenportal verfügt über eine eigene Azure OpenAI-Instanz, die u.a. das ChatGPT-Modell beinhaltet, welche nicht der öffentlich verfügbaren Ressource von OpenAI entspricht. Mit dem Dienstleister wurden sämtliche verfügbaren zusätzlichen Abkommen und datenschutzfreundlichen Einstellungsmöglichkeiten getroffen, um unter anderem auch die Kenntnisnahme und den Missbrauch der verarbeiteten Daten zu verhindern. Da Service mit modifiziertem Content Filter genutzt wird und die sog. Missbrauchsüberwachung von Microsoft deaktiviert wurde, speichert Microsoft hierfür keine Anfragen und Ergebnisse. Die betroffenen Daten werden außerdem ausdrücklich nicht zum Anlernen der Microsoft KI verwendet. Zur bestmöglichen Vorbeugung gegen mögliche Halluzinationen wurden die entsprechenden Einstellungen hinsichtlich der Kreativität optimiert.

Folgende Quellen bieten weitere Informationen zu den implementierten Maßnahmen bezüglich Microsoft als (Unter-)Auftragsverarbeiter und Azure OpenAI:

- https://learn.microsoft.com/de-de/legal/cognitive-services/openai/data-privacy
- https://learn.microsoft.com/de-de/legal/cognitive-services/openai/limited-access
- AVV Microsoft: https://www.microsoft.com/licensing/docs/view/Microsoft-Products-and-Services-Data-Protection-Addendum-DPA

Anlage 2 – Liste der bestehenden Unterauftragsverarbeitung

(Unternehmens-) Name und Anschrift	Beschreibung der Leistung	Verarbeitung von Man-dantendaten	Ort der Leistungs-erbringung
Microsoft Irland Operations Limited, One Microsoft Place. South Country Business Park, Leopadstown, Dublin 18, Irland	Der Dienstleister stellt die Cloud-Lösung „Microsoft Azure“ bereit, auf der die vertragsgegenständliche SaaS-Lösungen gehostet wird. Dies beinhaltet auch den Betrieb der OpenAI ChatGPT Instanz.	Ja	Deutschland /EU
Justin LegalTech GmbH und Westernacher Solutions GmbH, beide Columbiadamm 37 10965 Berlin	Stellt modifizierbare Software, die die Basis des Mandantenportal s darstellt zur Verfügung und stellen hierfür Wartung, Support und Weiterentwicklungen zur Verfügung	Ja	Deutschland /EU
Rockenstein AG Schleehofstraße 16, 97209 Veitshöchheim	Betrieb des Rechenzentrums	Ja	Deutschland /EU

Anlage 3 Weisungsempfänger:

Ramona Schmidt, mandantenportal@bnotk.de