

VERTRAG
AUFTRAGSVERARBEITUNG XNP

Zwischen

dem Notar

- nachstehend **Auftraggeber** genannt –

und

Bundesnotarkammer K.d.ö.R.

Mohrenstr. 34

10117 Berlin

- nachstehend **Auftragnehmerin** genannt –

- nachstehend gemeinsam **Parteien** genannt -

wird Folgendes vereinbart:

§ 1 Gegenstand und Dauer der Vereinbarung

- (1) Die Bundesnotarkammer hat das Programm XNP entwickelt, das über das NotarNetz erreichbar ist, und bietet hierfür mehrere Module an. XNP wird über die NotarNet GmbH bestellt. Für die Nutzung von XNP haben die Parteien einen Vertrag mit Nutzungsbedingungen für XNP („**Hauptvertrag**“) geschlossen.
- (2) Auch wenn der Auftraggeber für die von ihm eingetragenen personenbezogenen Daten i.S.d. § 4 Nr. 7 Europäischen Datenschutzgrundverordnung („**DS-GVO**“) selbst verantwortlich bleibt, kann eine Einsicht in Informationen oder eine Kenntnisnahme von personenbezogenen Daten im Rahmen von Wartung und Pflege der Systeme nicht ausgeschlossen werden. Die Auftragnehmerin verarbeitet daher gegebenenfalls 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

Die personenbezogenen Daten, die einer Verarbeitung durch die Auftragnehmerin unterliegen können, sind Daten, die im Rahmen der Nutzung gemäß des Hauptvertrags durch den Auftraggeber eingegeben oder vom System erzeugt werden (**Anlage 1**). Ein Zugriff auf diese Daten kann für 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 der Auftragnehmerin auf diese Daten nicht stattfindet. Die Daten werden gesichert in den Systemen der Auftragnehmerin abgelegt.

§ 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 ist der Geschäftsführer der Auftragnehmerin. 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) Die Auftragnehmerin sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Sie sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.
- (4) 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).
- (5) Die Auftragnehmerin hat Aufzeichnungen über ihre Datenverarbeitungstätigkeiten im Zusammenhang mit dem Hauptvertrag bzw. der betreffenden Leistungsbeschreibung zu führen und wird sie der Aufsichtsbehörde zur Verfügung stellen, wenn diese dies verlangt.
- (6) 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.
- (7) Die Auftragnehmerin hat 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.
- (8) Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf die Auftragnehmerin nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.
- (9) 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.

- (10) Die Auftragnehmerin bestätigt, dass ihr die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind. Sie verpflichtet sich, auch für diesen Auftrag relevante Geheimnisschutzregeln zu beachten, die dem Auftraggeber obliegen.
- (11) 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.
- (12) 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).
- (13) Die Auftragnehmerin überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in ihrem Betrieb und hat eine Datenschutzbeauftragte bestellt. Diese ist wie folgt erreichbar:

Datenschutzbeauftragte der Bundesnotarkammer
Mohrenstraße 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 gem. Ziff. 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) Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.
- (3) Die Auftragnehmerin hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmerin auch gegenüber Subunternehmern gelten. 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. 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.
- (4) 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).
- (5) 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. Die Auftragnehmerin haftet gegenüber dem Auftraggeber dafür, dass der Subunternehmer den Datenschutzpflichten nachkommt, die ihm durch die Auftragnehmerin im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.
- (6) Zurzeit sind keine Auftragsverarbeiter für die Auftragnehmerin tätig. Die Auftragnehmerin informiert den Auftraggeber 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 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 eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, 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 2** 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). Das Ergebnis samt vollständigem Auditbericht ist dem Auftraggeber auf Anfrage mitzuteilen. Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmerin und Auftraggeber abzustimmen. Soweit die bei der Auftragnehmerin getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht

genügen, benachrichtigt er den Auftraggeber unverzüglich. 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 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 1

Im Rahmen der Nutzung von XNP werden insbesondere solche personenbezogenen Daten eingegeben/übernommen, die zur Nutzung von XNP, zur Dokumentenkennzeichnung der in die angebundenen Module hochgeladenen Dokumente und deren Bearbeitung und Signatur erforderlich sind.

Das sind unter anderem

- Daten im Anmeldetoken der Anwendung (Vorname, Nachname, ggf. Amtstitel, Amtspersonen-ID, Name, AT-ID, OrganisationsID),
- Titel, Name, Vorname, Amtstitel, Amtssitz des Signierenden
- Dateiname, Dokumententitel, Dokumentenzeichen, Dokumentbeschreibung, Dokumentendatum, Validierungsvorgaben von Beglaubigungsvermerken, Vertreterbestellungsurkunden und deren Inhalt
- Nutzerspezifische Anwendungseinstellungen (z. B. Spaltenauswahl von Übersichten, automatisches Abmelden, Verzeichnispfad)
- Daten zur Bearbeitung von Vorgängen (z.B. Amtstätigkeit, Bearbeiter, Zeitpunkt, Vorgangssperren).

Anlage 2

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

1.1. Zutrittskontrolle

Das Rechenzentrum der BNotK besitzt folgende Zutrittskontrollen:

- ▶ Umzäunung des Geländes
- ▶ Automatisches Zutrittskontrollsystem mit Personenvereinzlungsanlage
- ▶ Absicherung des Zutrittskontrollsystems mit Zwei-Faktor-Authentifizierung (Karte und PIN)
- ▶ Protokollierung der Zutritte
- ▶ Alarm- und Einbruchmeldeanlage
- ▶ Videoüberwachung
- ▶ Tragepflicht von Berechtigungsausweisen
- ▶ Sorgfältige Auswahl des Wach-, Reinigungs- und Betriebspersonals
- ▶ Einbruchschutz

Die Betriebsflächen der BNotK 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

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
- ▶ Einsatz von Firewalls und Intrusion Detection Systemen
- ▶ Einsatz von Anti-Viren-Software
- ▶ Regelmäßige Implementierung von Sicherheits-Updates

1.3. Zugriffskontrolle

Die BNotK stellt 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

1.5. Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)

Zu Testzwecken werden in den Testumgebungen Testdaten verwendet.

1.6. 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

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

2.1. Weitergabekontrolle

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

Weitere Maßnahmen:

- ▶ Verschlüsselter Transport
- ▶ Verschlüsselung von Datenträgern
- ▶ Datenschutzgerechte Datenträgerentsorgung
- ▶ Sichere Löschung von Informationen und Datenträgern

2.2. Eingabekontrolle

Bei der BNotK 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

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

3.1. Verfügbarkeitskontrolle

Die BNotK 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

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. Notfallpläne bilden den Rahmen bezüglich der entsprechenden Handlungsanweisungen für ausgewählte dokumentierte Notfallszenarien.

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 Datenschutzorganisation bei der BNotK besteht aus einer Datenschutzbeauftragten und einer Informationssicherheitsbeauftragten.

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 des Verantwortlichen zu verarbeiten.

Datenschutzvorfälle werden dokumentiert und 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 BNotK.

4.2. Sicherheits- und Risikomanagement

Die BNotK 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 BNotK 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.

Die technischen und organisatorischen Maßnahmen zum Datenschutz gemäß DS-GVO, Artikel 32, werden im Rahmen der Konformitätsprüfungen regelmäßig überprüft. Darüber hinaus finden bei internen Prozessaudits auch datenschutzrelevante Fragestellungen Berücksichtigung.

4.3. Audits und Sicherheitstests

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

4.4. Störungsmanagement

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

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

Durch datenschutzfreundliche Voreinstellungen („Privacy-by-Design and Privacy-by-Default“) wird dem Datenschutz bei der BNotK schon zu einem möglichst frühen Zeitpunkt Rechnung getragen, um eine unrechtmäßige Verarbeitung oder den Missbrauch von Daten präventiv zu verhindern. 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

Bei der BNotK erfolgt die Auftragsdatenverarbeitung 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 BNotK 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