Vertrag zur Auftragsverarbeitung (AVV datenschutzBR)

zwischen der

datenschutz nord GmbH

Konsul-Smidt-Str. 88, 28217 Bremen

als Lizenzgeber

(Auftragnehmer)

und dem

datenschutzBR Lizenznehmer

(Auftraggeber)

Präambel

Der Auftragnehmer stellt dem Auftraggeber die Software-Lösung datenschutzBR (nachfolgend Software) als sogenannte Software-as-a-Service (SaaS) auf Grundlage der Allgemeinen Lizenzbedingungen vom 09.09.2021 zur Verfügung. Da der Auftragnehmer in diesem Zusammenhang personenbezogene Daten im Auftrag und nach Weisung des Auftraggebers verarbeitet, schließen die Parteien den vorliegenden Vertrag zur Auftragsverarbeitung ab.

§ 1 Gegenstand und Dauer des Auftrags

(1) Der Auftragnehmer führt die in der **Anlage A.1** beschriebenen Dienstleistungen für den Auftraggeber durch. Gegenstand, Art und Zweck der Verarbeitung, die Art der Daten sowie die Kategorien betroffener Personen werden dort beschrieben.

(2) Dieser Vertrag tritt – solange keine anderweitigen Regelungen vereinbart wurden – mit Annahme des von dem Auftragnehmer unterbreiteten Angebotes über die Nutzung der Software, in Kraft und gilt, solange der Auftragnehmer für den Auftraggeber personenbezogene Daten verarbeitet.

§ 2 Weisungen des Auftraggebers

(1) Der Auftraggeber ist für die Einhaltung der gesetzlichen Bestimmungen des Datenschutzrechts, insbesondere für die Rechtmäßigkeit der Verarbeitung sowie für die Wahrung der Betroffenenrechte verantwortlich. Gesetzliche oder vertragliche Haftungsregelungen bleiben hiervon unberührt.

(2) Der Auftragnehmer verarbeitet die ihm zur Verfügung gestellten personenbezogenen Daten nur für in **Anlage A.1** aufgeführte Zwecke bzw. nur auf Grund dokumentierter Weisungen des Auftraggebers und im Rahmen der getroffenen Vereinbarungen, es sei denn, er ist nach Unionsrecht oder nach dem Recht eines Mitgliedstaats, dem er unterliegt, zur Verarbeitung verpflichtet. In einem solchen Fall teilt der Auftragnehmer dem Auftraggeber diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine Mitteilung nicht wegen eines wichtigen öffentlichen Interesses untersagt.

(3) Ist der Auftragnehmer der Ansicht, dass eine Weisung des Auftraggebers gegen datenschutzrechtliche Vorschriften verstößt, hat er den Auftraggeber unverzüglich darauf hinzuweisen.

§ 3 Technische und organisatorische Maßnahmen

(1) Der Auftragnehmer hat für die zu verarbeitenden Daten angemessene technische und organisatorische Sicherheitsmaßnahmen getroffen und diese in **Anlage A.2** dieses Vertrages dokumentiert. Die Sicherheitsmaßnahmen gewährleisten ein dem Risiko angemessenes Schutzniveau.

(2) Die getroffenen Maßnahmen können im Laufe der Zeit der technischen und organisatorischen Weiterentwicklung angepasst werden. Der Auftragnehmer darf entsprechende Anpassungen nur vornehmen, wenn diese mindestens das Sicherheitsniveau der bisherigen Maßnahmen erreichen. Soweit nichts anderes bestimmt ist, muss der Auftragnehmer dem Auftraggeber nur wesentliche Anpassungen mitteilen.

§ 4 Pflichten des Auftragnehmers

(1) Der Auftragnehmer bestätigt, dass ihm die einschlägigen datenschutzrechtlichen Vorschriften bekannt sind. Er gestaltet in seinem Verantwortungsbereich die innerbetriebliche Organisation so, dass er den besonderen Anforderungen des Datenschutzes gerecht wird.

(2) Der Auftragnehmer bietet hinreichende Garantien dafür, dass die geeigneten technischen und organisatorischen Maßnahmen durchgeführt werden, die gewährleisten, dass die Verarbeitung im Einklang mit den datenschutzrechtlichen Vorschriften und den Rechten der betroffenen Personen steht.

(3) Der Auftragnehmer sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeitenden mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet sind oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Er überwacht die Einhaltung der datenschutzrechtlichen Vorschriften.

(4) Der Auftragnehmer darf im Rahmen der Auftragsverarbeitung nur dann auf personenbezogene Daten des Auftraggebers zugreifen, wenn dies für die Durchführung der Auftragsverarbeitung zwingend erforderlich ist.

(5) Soweit gesetzlich vorgeschrieben, bestellt der Auftragnehmer einen Beauftragten für den Datenschutz und teilt dem Auftraggeber dessen Kontaktdaten im **Anlage A.1** unaufgefordert mit. Der Auftragnehmer informiert den Auftraggeber über den Wechsel des Datenschutzbeauftragten.

(6) Der Auftragnehmer darf die ihm zur Verfügung gestellten personenbezogenen Daten ausschließlich im Gebiet der Bundesrepublik Deutschland, in einem Mitgliedsstaat der Europäischen Union in einem oder innerhalb des Europäischen Wirtschaftsraums verarbeiten. Die Verarbeitung von personenbezogenen Daten in einem Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen gesetzlichen Voraussetzungen der DSGVO erfüllt sind.

(7) Der Auftragnehmer unterstützt den Auftraggeber mit geeigneten technischen und organisatorischen Maßnahmen, damit dieser seine bestehenden Pflichten gegenüber den betroffenen Personen erfüllen kann, z.B. die Information und Auskunft, die Berichtigung oder Löschung von Daten, die Einschränkung der Verarbeitung oder das Recht auf Datenübertragbarkeit und Widerspruch. Auskünfte an betroffene Personen oder Dritte darf der Auftragnehmer nur nach vorheriger Weisung des Auftraggebers erteilen. Soweit eine betroffene Person ihre Betroffenenrechte unmittelbar gegenüber dem Auftragnehmer geltend macht, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(8) Unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen unterstützt der Auftragnehmer bei der Durchführung einer Datenschutz-Folgenabschätzung sowie einer ggf. erforderlichen Konsultation der Aufsichtsbehörden.

(9) Ferner unterstützt der Auftragnehmer auf Anfrage bei der Prüfung von Datenschutzverletzungen und der Umsetzung etwaiger Melde- und Benachrichtigungspflichten.

§ 5 Berechtigung zur Begründung von Unterauftragsverhältnissen

(1) Der Auftragnehmer hat zum Zeitpunkt des Vertragsschlusses folgende Unterauftragnehmer beauftragt:

UNTERAUFTRAGNEHMER	VERARBEITUNGSSTANDORT	BESCHREIBUNG DER VERARBEITUNG
PLUTEX GmbH, Bremen	Bremen	Hosting, Managed Services

Die zum Zeitpunkt des Vertragsschlusses beauftragten Unterauftragnehmer gelten als genehmigt.

Weitere Unterauftragnehmer dürfen nur beauftragt werden, wenn der Auftragnehmer den Auftraggeber über die beabsichtigte informiert, damit der Auftraggeber Einwände gegen die Beauftragung erheben kann. Einwände

gegen weitere Beauftragungen dürfen nur aus wichtigem Grund erhoben werden.

(2) Ein Unterauftragsverhältnis liegt insbesondere vor, wenn der Auftragnehmer weitere Auftragnehmer in Teilen oder im Ganzen mit Leistungen beauftragt, auf die sich dieser Vertrag bezieht. Nicht als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die der Auftragnehmer bei Dritten als Nebenleistung zur Unterstützung bei der Auftragsdurchführung in Anspruch nimmt. Dazu zählen z.B. Telekommunikationsleistungen oder Reinigungskräfte. Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Schutzes und der Sicherheit der Daten des Auftraggebers auch bei fremd vergebenen Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen zu treffen sowie Kontrollmaßnahmen zu ergreifen.

(3) Ein Zugriff auf Daten darf durch die Unterauftragnehmer erst dann erfolgen, wenn der Auftragnehmer durch einen Vertrag sicherstellt, dass die in diesem Vertrag vereinbarten Regelungen auch gegenüber dem Unterauftragnehmer gelten, wobei insbesondere hinreichende Garantien dafür geboten werden müssen, dass die geeigneten technischen und organisatorischen Maßnahmen so durchgeführt werden, dass die Verarbeitung entsprechend den datenschutzrechtlichen Vorschriften erfolgt.

§ 6 Kontrollrechte des Auftraggebers

(1) Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber oder eine von ihr beauftragte Person berechtigt ist, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen im erforderlichen Umfang zu kontrollieren, insbesondere durch die Einholung von Auskünften und Anforderung von relevanten Unterlagen, die Einsichtnahme in die Verarbeitungsprogramme oder durch Zutritt zu den Arbeitsräumen des Auftragnehmers.

(2) Kontrollen vor Ort sind mit angemessener Vorankündigung und unter Einhaltung von Betriebs- und Geschäftsgeheimnissen des Auftragnehmers sowie nach Möglichkeit ohne Störung des Betriebsablaufs durchzuführen. Für Kontrollen vor Ort kann der Auftragnehmer die ihm hierdurch entstehenden Aufwendungen gemäß den üblichen Stundensätzen des Auftragnehmers vom Auftraggeber ersetzt verlangen.

(3) Der Nachweis einer ordnungsgemäßen Verarbeitung kann auch durch geeignete und gültige Zertifikate zur IT-Sicherheit (z.B. IT-Grundschutz, ISO 27001) erbracht werden, sofern hierzu auch der jeweilige Gegenstand der Zertifizierung auf die Auftragsverarbeitung im konkreten Fall zutrifft. Die Vorlage eines relevanten Zertifikats ersetzt jedoch nicht die Pflicht des Auftragnehmers zur Dokumentation der Sicherheitsmaßnahmen im Sinne des § 3 dieses Vertrages.

§ 7 Mitzuteilende Verstöße

(1) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich über Störungen des Betriebsablaufs, die Gefahren für die Daten des Auftraggebers mit sich bringen, sowie bei Bekanntwerden von Datenschutzverletzungen im Zusammenhang mit den Daten des Auftraggebers. Gleiches gilt, wenn der

Auftragnehmer feststellt, dass die bei ihm getroffenen Sicherheitsmaßnahmen den gesetzlichen Anforderungen nicht genügen.

(2) Dem Auftragnehmer ist bekannt, dass der Auftraggeber verpflichtet ist, umfassend alle Verletzungen des Schutzes personenbezogener Daten zu dokumentieren und ggf. den Aufsichtsbehörden bzw. der betroffenen Person zu melden. Er wird bekanntgewordene Verletzungen unverzüglich an den Auftraggeber melden und hierbei zumindest folgende Informationen mitteilen:

(a) Beschreibung der Art der Verletzung, soweit möglich mit Angabe der Kategorien und der ungefähren Anzahl der betroffenen Personen und Datensätze,

(b) Name und Kontaktdaten von Kontaktpersonen für weitere Informationen

(c) Beschreibung der wahrscheinlichen Folgen der Verletzung sowie

(d) Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zu Behebung der Verletzung oder zur Abmilderung der sich daraus ergebenden nachteiligen Auswirkungen.

§ 8 Beendigung des Auftrags

(1) Nach Abschluss der Auftragsverarbeitung hat der Auftragnehmer alle personenbezogenen Daten nach Wahl des Auftraggebers entweder zu löschen oder an diesen zurückzugeben, soweit nicht eine gesetzliche Verpflichtung zur Speicherung der personenbezogenen Daten besteht.

(2) Der Auftraggeber kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn der Auftragnehmer einen schwerwiegenden Verstoß gegen die Bestimmungen dieses Vertrags oder gegen datenschutzrechtliche Bestimmungen begeht und dem Auftraggeber aufgrund dessen die Fortsetzung der Auftragsverarbeitung bis zum Ablauf der Kündigungsfrist oder bis zu der vereinbarten Beendigung des Auftrags nicht zugemutet werden kann.

(3) Der Auftragnehmer kann das Auftragsverhältnis ohne Einhaltung einer Frist kündigen, wenn der Auftraggeber auf die Erfüllung seiner Weisungen besteht, obwohl diese Weisungen gegen geltende rechtliche Anforderungen oder gegen diesen Vertrag verstoßen und der Auftragnehmer den Auftraggeber darüber in Kenntnis gesetzt hat.

§ 9 Schlussbestimmungen

(1) Sollte das Eigentum des Auftraggebers bei dem Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenzverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen. Ein Zurückbehaltungsrecht ist in Bezug auf Datenträger und Datenbestände des Auftraggebers ausgeschlossen.

(2) Die Vertragsbegründung, Vertragsänderungen und Nebenabreden sind schriftlich abzufassen, was auch in einem elektronischen Format erfolgen kann.

(3) Im Falle eines Widerspruchs zwischen den Regelungen dieses Vertrags und den Bestimmungen damit zusammenhängender Vereinbarungen, die zwischen den

Parteien bestehen oder später eingegangen oder geschlossen werden, haben die Regelungen dieses Vertrags Vorrang.

(4) Sollten einzelne Teile dieses Vertrags unwirksam sein, so berührt dies die Wirksamkeit des Vertrags im Übrigen nicht.

DocuSigned by:
Sven Venzke-Caprarese
8BEFA52F63554FD...

Sven Venzke-Caprarese

Geschäftsführer datenschutz nord GmbH

Anlage A.1

Auflistung der beauftragten Dienstleistungen

Gegenstand der Verarbeitung	Betrieb und Hosting von Software
Art und Zweck der Verarbeitung	Bereitstellung von Software zur Dokumentation datenschutzrelevanter Verfahren und Durchführung von Schulungen
Art der personenbezogenen Daten	E-Mail-Adressen der Nutzer mit dezidierten Zugängen zum System. In aller Regel keine darüberhinausgehenden personenbezogenen Daten, in Ausnahmefällen Anfragen von Betroffenen der Datenverarbeitung des Auftraggebers
Kategorien betroffener Personen	Mitarbeitende des Auftraggebers

Kontaktdaten der Datenschutzbeauftragten

Kontaktdaten der Datenschutz-beauftragten des Auftragnehmers	Joanna Maxine Stünkel, Konzerndatenschutzbeauftragte der DSN Holding GmbH, office@datenschutz-nord.de

Anlage A.2

Technische und organisatorische Maßnahmen

In dieser Anlage werden die technischen und organisatorischen Maßnahmen dokumentiert, die durch den Auftragnehmer zur ordnungsgemäßen Erfüllung der erbrachten Dienstleistung umgesetzt werden.

1. Maßnahmen zur Pseudonymisierung personenbezogener Daten

Personenbezogene Daten werden grundsätzlich pseudonymisiert, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert. Sofern zur Auslieferung von Inhalten IP-Adressen erforderlich sind, werden diese nicht gespeichert bzw. umgehend anonymisiert.

2. Maßnahmen zur Verschlüsselung personenbezogener Daten

datenschutzBR kann nur über eine Verbindung mit https-Verschlüsselung angesteuert werden. Administrative Zugriffe auf das Serversystem sind zudem nur aus dem Firmennetzwerk des Auftragnehmers möglich.

3. Gewährleistung der Vertraulichkeit

Das Hosting der Software, die Administration der Server und Datenbanksysteme erfolgt durch einen nach ISO/IEC 27001 & DIN ISO 9001 zertifizierten Hosting-Dienstleister, der dem Auftragnehmer hoch verfügbare und sichere Managed Server bereitstellt.

a) Zutrittskontrolle

Maßnahmen zur Zutrittskontrolle (sollen Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, verwehren):

aa) Rechenzentrum:

Die Eingangstür zum Rechenzentrum (besonders widerstandsfähig) ist mit einer elektronischen Schließanlage ausgestattet (Schlüsselkarte und PIN-Code). Zutritte werden personenbezogen protokolliert. Das Rechenzentrum ist fensterlos und verfügt über eine Einbruchmeldeanlage.

bb) Büroraume:

Sämtliche Eingangstüren zu den Büroräumen sind mit elektronischen Schließanlagen ausgestattet (RFID-Chips). Auch während der Geschäftszeiten sind alle Eingangstüren verschlossen und können nur per Klinke von innen oder mit einem passenden Schlüssel geöffnet werden. Außerhalb der Geschäftszeiten werden die Büroräume mit einer Einbruchmeldeanlage überwacht (Alarmaufschaltung bei einem Sicherheitsdienst). Besucher dürfen sich nur in Begleitung eines/einer Beschäftigten in den Büroetagen aufhalten.

b) Zugangskontrolle

Maßnahmen zur Zugangskontrolle (sollen verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können):

aa) Administrative Zugänge:

Administrative Zugänge zu datenschutzBR setzen die Eingabe eines Nutzernamens und eines Passworts voraus. Die Administratoren-Passwörter enthalten zwischen 11 und 20 Zeichen, bestehen aus großen und kleinen Buchstaben sowie Sonderzeichen und Ziffern. Serverseitig können administrative Tätigkeiten nur aus dem Unternehmensnetz des Auftragnehmers durchgeführt werden. Zudem werden für Zugriffe sog. Securitysticks nebst PIN verwendet.

bb) Client-Systeme:

Bei der Anmeldung am System werden Benutzername und Passwort abgefragt. Die verwendeten Passwörter müssen mindestens 8 Zeichen umfassen sowie aus großen und kleinen Buchstaben, Sonderzeichen und Ziffern bestehen.

c) Zugriffskontrolle

Maßnahmen zur Zugriffskontrolle (sollen gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können):

Zugriffsrechte werden streng nach dem Need-to-Know-Prinzip auf der Grundlage von Berechtigungskonzepten vergeben.

Die Authentisierung von Mitarbeitenden des Auftraggebers bei datenschutzBR erfolgt durch eine E-Mail-gestützte Multi-Faktor-Authentisierung.

d) Weitergabekontrolle

Maßnahmen zur Weitergabekontrolle (Sollen gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist):

datenschutzBR kann nur über eine Verbindung mit https-Verschlüsselung angesteuert werden. Das System unterstützt zudem Zugriffe per SSL/TLS 1.2 und 1.3.

Der temporäre Zugriff auf einzelne Web-Formulare kann per Deep-Link gewährt werden; dieser wird über eine ausreichend lange ID abgesichert, die nicht erraten werden kann.

e) Trennungsgebot

Maßnahmen zur Umsetzung des Trennungsgebots (Sollen gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können):

Durch eine logische Datentrennung ist sichergestellt, dass die Daten eines Auftraggebers getrennt von den Daten anderer Auftraggeber verarbeitet werden.

4. Gewährleistung der Integrität (Eingabekontrolle)

Maßnahmen zur Eingabekontrolle (sollen gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind):

Das Anlegen und Verändern eines Nutzerkontos wird systemseitig protokolliert.

5. Gewährleistung der Verfügbarkeit

a) Verfügbarkeitskontrolle

Maßnahmen zur Verfügbarkeitskontrolle (sollen gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind):

Der Datenbestand von datenschutzBR wird mehrfach täglich lokal und einmal täglich georedundant voll gesichert. Eine unterbrechungsfreie Stromversorgung verhindert, dass der Datenbestand bei einem plötzlichen Stromausfall Schaden nehmen kann. Das Rechenzentrum ist klimatisiert und verfügt über angemessene Brandschutzmaßnahmen. Sämtliche Systeme verfügen über einen aktuellen Virenschutz. Sicherheitsrelevante Softwareupdates werden unverzüglich installiert.

b) Auftragskontrolle

Maßnahmen zur Auftragskontrolle (sollen gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können):

Mit allen Auftragsverarbeitern bestehen Verträge nach Art. 28 DSGVO.

6. Gewährleistung der Belastbarkeit der Systeme

Es werden widerstandsfähige Systeme (Hard- und Software) eingesetzt, die im Hinblick auf die Speicher-, Zugriffs- und Leitungskapazitäten den zu erwartenden Beanspruchungen standhalten.

7. Regelmäßige Überprüfung der Maßnahmen

Die technischen und organisatorischen Maßnahmen werden laufend überprüft und im Bedarfsfall dem Stand der Technik angepasst.

DocuSign

Abschlusszertifikat

Umschlag-ID: 572811C620D642C5B2530B7B976A5F05
Betreff: Mit DocuSign signieren: AVV_BR_v1.pdf
Quellumschlag:
Dokumentenseiten: 10
Zertifikatsseiten: 1
Signatur mit Anleitung: Aktiviert
Umschlag-ID-Stempel: Aktiviert
Zeitzone: (UTC-08:00) Pacific Time (USA + Kanada)

Signaturen: 1
Initialen: 0

Status: Abgeschlossen

Umschlagersteller:
Sven Venzke-Caprarese
Konsul-Smidt-Str. 88
Bremen, Bremen 28217
svenzke-caprarese@datenschutz-nord.de
IP-Adresse: 82.198.219.177

Eintragsverfolgung

Status: Original
21.09.2021 07:40:26

Inhaber: Sven Venzke-Caprarese
svenzke-caprarese@datenschutz-nord.de

Standort: DocuSign

Unterzeichnerereignisse	Signatur	Zeitstempel
Sven Venzke-Caprarese svenzke-caprarese@datenschutz-nord.de Geschäftsführer datenschutz nord GmbH Sicherheitsstufe: E-Mail, Kontoauthentifizierung (keine)	DocuSigned by: Sven Venzke-Caprarese 8BEFA52F63554FD... Signaturübernahme: Vorgegebener Stil Mit IP-Adresse: 82.198.219.177	Gesendet: 21.09.2021 07:40:50 Eingesehen: 21.09.2021 07:40:56 Signiert: 21.09.2021 07:41:03

Vereinbarung bezüglich elektronischer Unterlagen und Signaturen:
Nicht über DocuSign möglich

Vor-Ort-Unterzeichner – Ereignisse	Signatur	Zeitstempel

Bearbeiterversandereignisse	Status	Zeitstempel

Beauftragtenversandereignisse	Status	Zeitstempel

Vermittlerversandereignisse	Status	Zeitstempel

Zertifizierter Versand - Ereignisse	Status	Zeitstempel

Kopienereignisse	Status	Zeitstempel

Zeugen-Ereignisse	Signatur	Zeitstempel

Notarereignisse	Signatur	Zeitstempel

Umschlagereignisse – Überblick	Status	Zeitstempel
Umschlag gesendet	Hash-codiert/verschlüsselt	21.09.2021 07:40:50
Zertifiziert zugestellt	Sicherheitsprüfung ausgeführt	21.09.2021 07:40:56
Signiervorgang abgeschlossen	Sicherheitsprüfung ausgeführt	21.09.2021 07:41:03
Abgeschlossen	Sicherheitsprüfung ausgeführt	21.09.2021 07:41:03

Zahlungen	Status	Zeitstempel