Vereinbarung zur Auftragsdatenverarbeitung Mitgliederverwaltung Nordbayerischer Musikbund

Stand: 12.06.2018

1) Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DS-GVO

1.1) Auftraggeber (Verantwortlicher i.S.v. Art. 4 Nr. 7 DS-GVO):

Verein _____

Vereinsnummer _____ (wenn bekannt)

Vorsitzender _____

Straße/Postfach _____

PLZ – Ort _____

Telefon _____

Email _____

(nachfolgend „Auftraggeber“ genannt)

1.2) Auftragnehmer (Auftragsverarbeiter):
Nordbayerischer Musikbund e.V. – An der Spielleite 12 – 97294 Unterpleichfeld
(nachfolgend „Auftragnehmer“ oder „NBMB“ genannt)

2) Gegenstand und Dauer der Vereinbarung

2.1) Gegenstand des Auftrages: Der Auftragnehmer verarbeitet im Rahmen der softwarebasierten Mitgliederverwaltung (Verbandsverwaltung) seiner Mitgliedsvereine – so auch für den Auftraggeber – personenbezogene Daten im Sinne von Art. 4 Nr. 2 und Art. 28 DS-GVO auf Grundlage dieses Vertrages.

Die vertraglich vereinbarte Dienstleistung wird ausschließlich in einem Mitgliedsstaat 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 (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

2.2) Dauer des Auftrages: Der Vertrag wird auf unbestimmte Zeit geschlossen.

3) Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen:

3.1) Art und Zweck der Verarbeitung
Der Auftraggeber übermittelt die gemäß Ziffer 3.2 personenbezogenen Daten an den NBMB und dieser verarbeitet diese zum Zwecke der jährlichen Mitgliedermeldung. Die Mitgliedermeldung erfolgt zum

Zwecke der Berechnung der Höhe der Beitragspflicht des Auftraggebers, der Ermittlung der Bemessungsgrundlage zur Abgabenpflicht an die Künstlersozialkasse im Rahmen der Ausgleichsvereinigung, der Höhe der zu zahlenden GEMA-Gebühren für eigene Veranstaltungen des Auftraggebers sowie der Inanspruchnahme der Versicherungsleistungen in der optionalen Unfall-, Haftpflicht-, D&O- und Vermögenschaden-Haftpflichtversicherung. Die Übermittlung durch den Auftraggeber und Verarbeitung durch den NBMB erfolgt ferner für die Inanspruchnahme verschiedener Serviceangeboten des NBMB durch den Auftraggeber, wie zum Beispiel der Teilnahme an Seminaren und Prüfungen des NBMB sowie die Durchführung von Ehrungen.

Die Verarbeitung durch den NBMB beinhaltet u.a. das Hosting der Online-Datenbank, die Durchführung von Datensicherungen sowie die anlassbezogene Auswertung der übermittelten Daten aus der Online-Datenbank. Die personenbezogenen Daten werden somit erhoben, erfasst, organisiert, geordnet, gespeichert, ausgelesen, abgefragt, abgeglichen sowie verwendet.

3.2) Art der personenbezogenen Daten
Folgenden Arten von personenbezogenen Daten werden verarbeitet:
a) Stammdaten:
Vor- und Nachname, Geburtsdatum, Geschlecht, Geburtsname, Instrument, Anschrift, „Musiker seit“, Ehepartner, Hochzeitsdatum

b) Kommunikationsdaten:
Telefon, Fax, 1. Email-Adresse, 2. Email-Adresse Facebook-Adresse

c) sonstige mitgliederbezogene Daten:
„GEMA frei“, „Führungszeugnis vorgelegt“, weitere personenbezogene Notizen (Kommentar)

c) Mitgliederhistorie:
Zeiten der Vereinsmitgliedschaften (Ein- und Austrittsdatum)
Mitgliedstatus (aktiv, passiv, fördernd, verstorben) mit Beiträgen (aktuell und historisch)
Orchesterzugehörigkeiten (aktuell und historisch)
Musikunterricht / Ausbildung (aktuell und historisch)
Verliehene Ehrungen und Ehrungstermine durch den NBMB
Vereinsfunktionen (aktuell und historisch)
Teilnahme an Vereinsveranstaltungen
Lehrgänge, Prüfungen und Qualifikationen einschl. Lehrgangs-/Prüfungsort, Fach/Instrument, Datum
Vereinsinterne Prüfungen und Ehrungen einschließlich Datum

d) Vertragsabrechungs- und Zahlungsdaten:
Zahlungsart (SEPA / Rechnung), Datum SEPA-Mandat
Bankverbindung / ggf. Verweis auf Referenzkonto
Ausleihe von Vereinsinstrumenten mit Datum der Ausleihe
Ausleihe von Vereinstrachten mit Datum der Ausleihe

3.3) Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DSGVO):
Folgende Kategorien von Personen werden verarbeitet:
Mitglieder des Auftraggebers

Hinweis zur Datenübermittlung / Datenverwendung durch den NBMB

Die unter 3.2 genannten personenbezogenen Daten werden an den NBMB übermittelt. Übermittelt heißt, dass die Daten in einer vom NBMB zur Verfügung gestellten Datenbank gespeichert werden. Der NBMB, jede dem NBMB unterstellte Person sowie alle Funktionäre des NBMB haben im Rahmen ihrer Tätigkeit nach 3.1) ausschließlich Zugriff auf folgende personenbezogenen Daten: Name, Vorname, Geburtsdatum, Geburtsname, Geschlecht, „Musiker seit", Instrument(e), Anschrift, Telefon, 1. Email-Adresse, Mitgliedsstatus (aktiv, passiv, ehemalig, verstorben), „GEMA frei", „in Ausbildung", Newsletter, vereins- und verbandsinterne Hinweise, Meldungen an den Verband, Prüfungen durch den Verband, Teilnahme an Lehrgängen und Seminaren, Ehrungen durch den Verband, Vereinsfunktionen.

4) Rechte und Pflichten sowie Weisungsbefugnisse des Auftraggebers

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 ff. DS-GVO ist allein der Auftraggeber verantwortlich. Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Auftraggeber und Auftragnehmer abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

Der Auftraggeber erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

Der Auftraggeber ist berechtigt, sich wie unter Ziffer 5 festgelegt vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen. Der Auftraggeber wird das Ergebnis in geeigneter Weise dokumentieren. Der Auftraggeber trägt die Verantwortung dafür, dass diese für die Risiken der zu verarbeiteten Daten ein angemessenes Schutzniveau bieten.

Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Beide Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen. Die vorstehende Verpflichtung gilt nicht für Informationen, die eine der Parteien nachweisbar von Dritten erhalten hat, ohne zur Geheimhaltung verpflichtet zu sein, oder die öffentlich bekannt sind.

5) Weisungsberechtigte des Auftraggebers, Weisungsempfänger des Auftragnehmers

5.1) Weisungsberechtigte Person des Auftraggebers:

Der erste Vorsitzende des Auftraggebers
Adresse siehe 1.1)

5.2) Weisungsempfänger beim Auftragnehmer ist:
Der Verbandsgeschäftsführer des NBMB.

Verbandsanschrift:
Nordbayerischer Musikbund e.V. · Geschäftsstelle
An der Spielleite 12 · 97294 Unterpleichfeld e.V.
Tel. 09367 / 988 689 0; Fax 09367 / 988 689 9
www.nbmb-online.de · geschaeftsstelle@nbmb.de

6) 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 Europäischen 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 verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Auftraggebers nicht erstellt:
Der Auftragnehmer sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. Er sichert zu, dass die für den Auftraggeber verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.
Der Auftragnehmer überprüft regelmäßig die auftrags- und datenschutzgerechte Durchführung dieses Vertrages, mindestens jedoch einmal halbjährlich. Die Prüfergebnisse sind zu dokumentieren und dem Auftraggeber auf Verlangen vorzulegen.
Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 ff. DS-GVO durch den Auftraggeber, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Auftraggebers hat der Auftragnehmer im notwendigen Umfang mitzuwirken und den Auftraggeber soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DS-GVO). Er hat dem Auftraggeber die dazu jeweils erforderlichen Angaben in geeigneter Weise mitzuteilen.
Der Auftragnehmer 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). Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber nach Überprüfung bestätigt oder geändert wird.
Der Auftragnehmer hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Auftraggeber dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragnehmers dem nicht entgegenstehen.
Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Weisung oder Zustimmung durch den Auftraggeber erteilen.
Die Verarbeitung von Daten im Auftrag des Auftraggebers erfolgt ausschließlich in den Betriebsstätten des Auftragnehmers und seiner Subunternehmern, als auch durch die Funktionäre des NBMB an deren jeweiligen Standort. Eine darüber hinausgehende Verarbeitung außerhalb vorbenannter Orte ist nur mit Zustimmung des Auftraggebers in Schriftform oder Textform (Fax/E-Mail) zulässig. Eine

Verarbeitung von Daten für den Auftraggeber in Privatwohnungen, die nicht die technischen und organisatorischen Schutzmaßnahmen gemäß Anhang 2 erfüllen ist nur mit Zustimmung des Auftraggebers in Schriftform oder Textform (Fax/E-Mail) im Einzelfall zulässig, wenn der Auftragnehmer und Wohnungsinhaber vor der Verarbeitung schriftlich versichern, dass der Auftraggeber Zugang zum Verarbeitungsort erhält.

Der Auftragnehmer bestätigt, dass ihm die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DS-GVO bekannt sind.

7) Qualitätssicherung durch den Auftragnehmer

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Vertrags gesetzliche Pflichten gemäß Art. 28 ff. DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 Buchst. b), 29, 32 Abs. 4 DS-GVO. 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, jede dem Auftragnehmer unterstellte Person sowie alle Funktionäre des Auftragnehmers, 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.

Die Umsetzung und Einhaltung aller für diese Auftragsverarbeitung erforderlichen technischen und organisatorischen Maßnahmen erfolgt gemäß Art. 28 Abs. 3 S. 2 Buchst. c), 32 DS-GVO. Der Auftragnehmer wird zu diesem Zweck insbesondere die in Anhang 2 geregelten technischen und organisatorischen Maßnahmen treffen.

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

Es erfolgt die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Vertrag 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.

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 im Rahmen dieses Vertrags ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

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.

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

Der Auftragnehmer ist zur Bestellung eines Datenschutzbeauftragten (Email: datenschutz@nbmb-online.de) verpflichtet.

8) Kontrollrechte des Auftraggebers

Der Auftragnehmer erklärt sich damit einverstanden, dass der Auftraggeber - grundsätzlich nach einer Vorankündigung von fünf (5) Werktagen - 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 den jeweils üblichen Geschäftszeiten 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).

Der Auftraggeber wird dabei Sorge dafür tragen, dass die Kontrollen nur im erforderlichen Umfang durchgeführt werden, um die Betriebsabläufe des Auftragnehmers durch die Kontrollen nicht unverhältnismäßig zu stören.

Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO 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.

Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch:

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren); oder
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

9) Mitteilungspflichten des Auftragnehmers bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

Der Auftragnehmer teilt dem Auftraggeber unverzüglich Störungen, Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen oder seiner Funktionäre sowie 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. Der Auftragnehmer 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 der Auftragnehmer nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

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

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 o. g. Kommunikationswege (Ziff. 4) mit Ausnahme der mündlichen Gestattung erfolgen muss. Der Auftraggeber darf seine Zustimmung nicht ohne wichtigen datenschutzrechtlichen Grund verweigern. 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.
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).
Der Auftragnehmer hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Auftraggeber und Auftragnehmer auch gegenüber Subunternehmern gelten. Der Auftragnehmer hat die Einhaltung dieser Pflichten regelmäßig zu kontrollieren. Das Ergebnis der Überprüfungen ist zu dokumentieren und dem Auftraggeber auf Verlangen zugänglich zu machen.
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. 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.
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). Dem Auftraggeber ist der Auftragsverarbeitungsvertrag auf Anfrage in Kopie zu übermitteln.
Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Subunternehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.
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.
Zurzeit sind für den Auftragnehmer die im Anhang 1 bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt. Mit deren Beauftragung erklärt sich der Auftraggeber einverstanden.

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

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.
Für die auftragsgemäße Verarbeitung personenbezogener Daten wird bei Bedarf, jedoch mindestens jährlich, eine Risikobewertung durchgeführt und dokumentiert, welche die Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten berücksichtigt.
Das im Anhang 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 beim Auftragnehmer dar.
Der Auftragnehmer 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 ist dem Auftraggeber auf Verlangen mitzuteilen.
Für die Sicherheit erhebliche Entscheidungen zur Organisation der Datenverarbeitung und zu den angewandten Verfahren sind zwischen Auftragnehmer und Auftraggeber abzustimmen.
Soweit die beim Auftragnehmer getroffenen Maßnahmen den Anforderungen des Auftraggebers nicht genügen, benachrichtigt er den Auftraggeber unverzüglich. Überschreiten die Anforderungen des Auftraggebers den üblichen Standard für die konkrete Auftragsverarbeitung, so hat der Auftraggeber die dem Auftragnehmer durch die Anhebung des Schutzniveaus entstehenden Mehrkosten zu erstatten.
Die Maßnahmen beim Auftragnehmer können im Laufe des Auftragsverhältnisses der technischen und organisatorischen Weiterentwicklung angepasst werden, dürfen aber die vereinbarten Standards nicht unterschreiten.
Wesentliche Änderungen muss der Auftragnehmer mit dem Auftraggeber in dokumentierter Form (schriftlich, elektronisch) abstimmen. Solche Abstimmungen sind für die Dauer dieses Vertrages aufzubewahren.

12) Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, Art. 28 Abs. 3 Satz 2 lit. g DS-GVO

Nach Beendigung des Auftrages hat der Auftragnehmer sämtliche in seinen Besitz sowie an Subunternehmen gelangte Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse Daten, die im Zusammenhang mit dem Auftragsverhältnis stehen, binnen einer Frist von 3 Monaten an den Auftraggeber auszuhändigen und die Datenträger des Auftragnehmers im Anschluss physisch zu löschen. Dies betrifft auch etwaige Datensicherungen beim Auftragnehmer. Die Löschung ist in geeigneter Weise zu dokumentieren. Test- und Ausschussmaterial ist unverzüglich zu vernichten oder physisch zu löschen. Der Auftraggeber hat das Recht, die vollständige und vertragsgemäße Rückgabe und Löschung der Daten beim Auftragnehmer zu kontrollieren.
Etwaige gesetzliche Aufbewahrungspflichten oder sonstige Pflichten zur Speicherung der Daten bleiben von vorbenannter Verpflichtung unberührt.

13) Haftung

Auf Art. 82 DS-GVO wird verwiesen.

14) Sonstiges

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

Für Nebenabreden ist grundsätzlich die Schriftform oder ein dokumentiertes elektronisches Format erforderlich.

Sollte das Eigentum oder die zu verarbeitenden personenbezogenen Daten des Auftraggebers beim Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung oder Beschlagnahme), durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu verständigen.

Die Einrede des Zurückbehaltungsrechts i. S. v. § 273 BGB wird hinsichtlich der für den Auftraggeber verarbeiteten Daten und der zugehörigen Datenträger ausgeschlossen.

Sollten einzelne Teile dieser Vereinbarung unwirksam sein, so berührt dies die Wirksamkeit der Vereinbarung im Übrigen nicht.

Es gilt das Recht der Bundesrepublik Deutschland unter Ausschluss des UN-Kaufrechts. Erfüllungsort und Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit diesem Vertrag ist der Sitz des Auftragnehmers.

Auftraggeber:	Auftragnehmer (NBMB): Unterpleichfeld, 12.06.2018
_____	_____
Ort, Datum – Unterschrift (ggf. Stempel)	Andreas Kleinhenz, *Verbandsgeschäftsführer NBMB*

Anlagen

Anhang 1 - Verzeichnis der Subunternehmer

Anhang 2 - Technische und organisatorische Maßnahmen (TOM) i.S.d. Art. 32 DSGVO